SUBSETS OF GROUPS EXHIBITING REGULARITY IN DIFFERENCES

by

Patrick G. Cesarz

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 Mathematical Sciences

Fall 2019

© 2019 Patrick G. Cesarz
All Rights Reserved

SUBSETS OF GROUPS EXHIBITING REGULARITY IN DIFFERENCES

by

Patrick G. Cesarz

Approved: _____
Louis Rossi, Ph.D.
Chair of the Department of Mathematical Sciences

Approved: _____
John Pelesko, Ph.D.
Dean of the College of Arts & Sciences

Approved: _____
Douglas J. Doren, Ph.D.
Interim Vice Provost for Graduate and Professional Education and
Dean of the Graduate College

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 S. Coulter, 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: _____

Felix 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: _____

Qing Xiang, 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: _____

Andrew Woldar, Ph.D.
Member of dissertation committee

ACKNOWLEDGEMENTS

It is said that it takes a village to raise a child. The same can be said of any student, not the least of which a doctoral student of mathematics. It is absurd to attempt a fully-comprehensive acknowledgement of all those who have led to the completion of this thesis, but I will now make such an attempt.

I thank my advisor, Dr. Robert S. Coulter, for his limitless patience and support. I have not been the easiest student to motivate over the past few years, and despite my best efforts at self-sabotage, Robert has never stopped supporting me and believing in me, especially when it would have been much easier to give up on me, as I have almost given up on myself too many times to count.

To my undergraduate mentor, Dr. Andrew Woldar, who very quickly saw in me the potential to be a mathematician, I give great thanks. The countless hours he spent in his office and over Skype instilling and fostering in me a love for mathematics will never be forgotten.

I am thankful for Dr. Felix Lazebnik, who was critically influential in my decision to attend the University of Delaware. I greatly appreciate Felix's personal concern for my learning and well-being during the first few years of my time at the University of Delaware and afterward.

Although Dr. Qing Xiang was working at the National Science Foundation during my first few years at the University of Delaware, he has allowed me to sit-in on many of the classes he has taught. Many techniques covered in those courses are used in this very thesis, so clearly, I owe a great deal of thanks to Qing.

Finally, I would like to thank Mrs. Loretta Minear and Mr. Curtis Minich. It was during middle school and high school that my love of mathematics and computer science was discovered and cultivated by these individuals.

TABLE OF CONTENTS

LIST OF TABLES

A COMMENT ON NOTATION

Before we start, a comment on notation is in order. This thesis contains a large variety of mathematical objects. In an attempt to help keep track of these objects, we have put in place some font-based notation. Specifically, unless there is a well-established precedent for notation (such as in the notation for the parameters of PDS and DS), we will use the following conventions:

- Fields are denoted as $\mathbb{F}, \mathbb{L}, \mathbb{R}$, and so forth.
- Groups are denoted as $\mathcal{G}, \mathcal{H}, \mathcal{N}$, and so forth.
- To talk of the non-identity elements of a group $\mathcal{G}$, we use $\mathcal{G}^\star$. This convention extends to the non-zero elements of a field, where we write $\mathbb{F}^\star$, for example.
- Subsets of algebraic objects which we are not assured as having structure are denoted as $\mathcal{S}, \mathcal{T}, \mathcal{J}$, and so forth.
- Elements of fields that we wish to highlight as being part of a basis we denote as **b, s**, and so forth.
- Greek letters are generally used to denote maps. There is one clear exception to this: When we talk of a character χ of a field $\mathbb{L}$, and we have a subfield $\mathbb{K}$ of $\mathbb{L}$, the restriction of χ to $\mathbb{K}$ is denoted by $\mathfrak{X}$. We do this mainly to avoid issues with subscripts.
- We use $\mathfrak{w}$ to denote a root of unity. On occasion, especially when dealing with character sums, we have to deal with complicated exponents of $\mathfrak{w}$. To improve readability, in parallel to the common notation exp, we introduce the notation $\mathfrak{w}\exp$ to mean $\mathfrak{w}\exp(x) = \mathfrak{w}^x$.

ABSTRACT

This thesis is primarily concerned with subsets of groups that exhibit a regularity of differences (if written additively). In it, both non-existence results and existence results shall be established, along with the development of a general construction technique for generalized difference sets. Chapter 1 contains an introduction to the objects being considered as well a brief background of character theory.

In Chapter 2 we prove certain integrality conditions regarding the parameters of PDS's. This leads to a particular nonexistence result.

Neo-difference sets have been used to study finite projective planes of Lenz-Barlotti type I.4. Although a nonexistence proof remains elusive, several results exist regarding conditions on orders of such projective planes. We generalize a group-ring equation used in proving one of these conditions in Chapter 3.

In Chapters 4-7, we outline a method of constructing infinite families of PDS's in finite fields and provide examples of three such constructions which come from the image sets of polynomials over said finite fields. These infinite families of PDS's are not new, however, and Chapter 8 establishes the equivalence of these recent constructions with Maiorana-McFarland bent functions and orthogonal arrays.

In Chapter 9, we provide examples of GDSs found in fields of characteristic 3 using the methods put forth in Chapter 4. Although no families of GDS's are found, there are some possibilities worth investigating.

Finally, we outline the publication status of our results. Those of Chapter 2 were subsumed by a more general result of De Winter etc., so has never been submitted to be published. The results of Chapter 3 was published in the article *A Wilbrink-like equation for neo-difference sets*. The results of Chapters 4 through 8 were published in the article *Image*

Sets with Regularity of Differences. The results of Chapter 9 remain unsubmitted as they are incomplete. We hope to establish an infinite class of GDS's that contain our work.

Chapter 1

INTRODUCTION

1.1 Sets exhibiting a regularity of differences

This thesis is primarily interested in sets exhibiting a regularity of differences. More specifically, we will be mostly considering the following sets.

Definition 1. *Let $\mathcal{S}, \mathcal{D}$ be two subsets of a group $\mathcal{G}$ of order v, written additively, but not necessarily Abelian. Set $|\mathcal{D}| = k$, and $|\mathcal{S}| = s$.*

(i) If there exist non-negative integers λ and μ such that every element of $\mathcal{S}^\star$ can be written in precisely λ ways as a difference in $\mathcal{D}$, while every element of $\mathcal{G}^\star \setminus \mathcal{S}$ can be written in precisely μ ways as a difference in $\mathcal{D}$, then $\mathcal{D}$ is a (v, s, k, λ, μ) generalized difference set (GDS) related to $\mathcal{S}$.

(ii) If $\mathcal{S} = \mathcal{D}$, then $\mathcal{D}$ is a (v, k, λ, μ) partial difference set (PDS).

(iii) If $\mathcal{S} = \mathcal{D}$ and $\lambda = \mu$, then $\mathcal{D}$ is a (v, k, λ) difference set (DS).

Although these objects are defined for any finite group, we will primarily be concerned with PDS's over Abelian groups. In particular, we investigate PDS's of the additive group of finite fields. For information regarding finite fields, see Lidl and Niederreiter [17] or Mullen and Panario [20].

While GDS appear to be a recent development, introduced in 2008 by Cao and Sun [5], DS and PDS have been studied for many years. There is a famous construction from 1933 due to Paley [21]: Let $\mathbb{F}_q$ denote the finite field of order q, with q odd, and let $\mathcal{D}$ be the set of all non-zero squares of $\mathbb{F}_q$. Then

- If $q \equiv 1 \bmod 4$, then $\mathcal{D}$ is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$-PDS in the additive group of $\mathbb{F}_q$.

⊡ If $q \equiv 3 \bmod 4$, then $\mathcal{D}$ is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$-DS in the additive group of $\mathbb{F}_q$. In this case, $\mathcal{D}$ is necessarily skew, that is, $\mathcal{D} \cap -\mathcal{D} = \emptyset$.

The DS examples of Paley are examples of what are known as *skew Hadamard* difference sets (SHDS), where the group $\mathcal{G}$ is equal to the disjoint union of $\mathcal{D}$, $-\mathcal{D}$, and $\{0\}$. For many years, these were the only known examples of SHDS, until 2006 when Ding and Yuan [9] constructed new examples using planar functions.

There are some famous (historical) names involved in the early years of the study of DS and PDS, such as Chowla [6], H.B. Mann [18], E. Lehmer [15], R.H. Bruck [4], and Marshall Hall Jr. [12]. Much of the early work was concerned with when the kth powers of $\mathbb{F}_p^\star$, p a prime, form a DS or PDS in the additive group of $\mathbb{F}_p$. In more recent times, the work of Ding and Yuan was put into a more general framework by Qiu *et al* [22], and the later chapters of this thesis are motivated, in part, by these classical results and the work of Qiu *et al*.

There is one further type of set exhibiting a regularity of differences that we shall be interested in. Neo-difference sets have defining properties that are similar to those of partial difference sets, though their applications are different.

Definition 2. *Let $n \in \mathbb{N}$, $\mathcal{X}$ be an Abelian group, $|\mathcal{X}| = n - 1$, $\mathcal{G} = \mathcal{X} \times \mathcal{X}$, and $\mathcal{D} \subset \mathcal{G}$. Let $\mathcal{U}_1 = \mathcal{X} \times \{1\}$, $\mathcal{U}_2 = \{1\} \times \mathcal{X}$, and $\mathcal{U}_3 = \{(x, x) \mid x \in \mathcal{X}\}$. If every element in $\mathcal{G} \setminus (\mathcal{U}_1 \cup \mathcal{U}_2 \cup \mathcal{U}_3)$ can be represented uniquely in the form $d_1 d_2^{-1}$ with $d_1, d_2 \in \mathcal{D}$ and no nonidentity element in $\mathcal{U}_1 \cup \mathcal{U}_2 \cup \mathcal{U}_3$ has such a representation, then $\mathcal{D}$ is a neo-difference set of order n.*

The existence of a neo-difference set of order n is equivalent to the existence of an order n projective plane of Lenz-Barlotti type I.3, I.4 or VII.2 – non-Abelian $\mathcal{G}$ corresponds to type I.3, while the Abelian case can be either I.4 or VII.2. The only known examples of a neo-difference set correspond to type VII.2, the Desarguesian plane. For Lenz-Barlotti types I.3 and I.4, several results exist putting restrictions on the possible orders of such planes, but whether they exist or not is still unknown. For background results on neo-difference sets, see the papers Hughes [13], Kantor [14], and Ghinelli and Jungnickel [10], [11]. For

information on projective planes and the Lenz-Barlotti classification system, see Dembowski [8]. The classification was originally derived by Lenz [16], with refinements by Barlotti [1].

We require one result concerning the behavior of differences in a particular SHDS in a finite field, $\mathbb{F}_q$, but we must first discuss notation regarding the group-ring $\mathbb{C}\mathcal{G}$. Recall that if $\mathcal{G}$ is written multiplicatively, then $\mathbb{C}\mathcal{G}$ consists of all formal sums $\sum_{g\in\mathcal{G}} a_g g$ with $a_g \in \mathbb{C}$ for all $g \in \mathcal{G}$. If we let $A = \sum_{g\in\mathcal{G}} a_g g$ and $B = \sum_{g\in\mathcal{G}} b_g g$, then we have the following definitions of addition and multiplication of group-ring elements:

$$A + B = \sum_{g\in\mathcal{G}} (a_g + b_g)g$$
$$AB = \sum_{g\in\mathcal{G}} \sum_{h\in\mathcal{G}} (a_g b_h)(gh).$$

Through a slight abuse of notation, if $\mathcal{S} \subseteq \mathcal{G}$, then we will also use the symbol $\mathcal{S}$ to denote the group-ring element $\sum_{s\in\mathcal{S}} s$. Also, for all $n \in \mathbb{Z}$, we define $\mathcal{S}^{(n)} = \sum_{s\in\mathcal{S}} s^n$. Finally, let $\varphi \in \mathrm{Aut}(\mathcal{G})$. Since φ is defined on $\mathcal{G}$, and $\mathcal{G}$ forms a basis for $\mathbb{C}\mathcal{G}$, we have that φ can be extended to a unique automorphism of $\mathbb{C}\mathcal{G}$, also denoted by φ. In other words, in the above notation, $\varphi(A) = \sum_{g\in\mathcal{G}} a_g \varphi(g)$.

In the case in which $\mathcal{G}$ is written additively, we make use of different notation. The elements of $\mathcal{G}$ will be denoted by x^g rather than g. By convention, the element x^0 will be denoted by 1. Since elements of $\mathbb{C}\mathcal{G}$ are linear combinations of elements of this form, we have that elements of $\mathbb{C}\mathcal{G}$ appear like functions of x. As such, function notation will be used when appropriate. For example, by letting $A(x) = \sum_{g\in\mathcal{G}} a_g x^g$ and $B(x) = \sum_{g\in\mathcal{G}} b_g x^g$, we have that the binary operations are defined as follows:

$$A(x) + B(x) = \sum_{g\in\mathcal{G}} (a_g + b_g)x^g$$
$$A(x)B(x) = \sum_{g\in\mathcal{G}} \sum_{h\in\mathcal{G}} (a_g b_h)x^{g+h}.$$

Note that with this notation, similarities between $\mathbb{C}\mathcal{G}$ and any polynomial ring are more-apparent. Instead of writing $\mathcal{S}^{(n)}$ as above, we write $\mathcal{S}(x^n)$. Also, if $\varphi \in \mathrm{Aut}(\mathcal{G})$, we write $A(x^\varphi)$ for $\varphi(A)$. In the special case in which $\mathcal{G}$ is $\left(\mathbb{F}_q, +\right)$, we have that the Frobenius automorphism maps any group-ring element $A(x)$ to $A(x^p)$.

Theorem 3. *Let $q \equiv 3 \bmod 4$, $\mathcal{N}$ denote the SHDS of nonsquares in the finite field $\mathbb{F}_q$, and $\mathcal{S} = \mathbb{F}_q^\star \setminus \mathcal{N}$, the SHDS of nonzero squares in $\mathbb{F}_q$. Then for all $n \in \mathcal{N}$, the set $\mathcal{N} - n$ contains $\frac{q-3}{4}$ nonsquares and $\frac{q-3}{4}$ nonzero squares. Also, for all $s \in \mathcal{S}$, the set $\mathcal{N} - s$, contains $\frac{q-3}{4}$ nonsquares and $\frac{q+1}{4}$ nonzero squares.*

Proof. We compute the group-ring element $\mathcal{N}(x)\,\mathbb{F}_q\left(x^{-1}\right)$ in two different ways. Note that for all $s \in \mathcal{S}$, we have that $\mathcal{N}(x^s) = \mathcal{N}(x)$. This is due to the fact that the squares of $\mathbb{F}_q^\star$ form a multiplicative subgroup of $\mathbb{F}_q^\star$. Using the fact that $\mathbb{F}_q(x) = \mathcal{S}(x) + \mathcal{N}(x) + 1$, we deduce the following.

$$\begin{aligned}\mathcal{N}(x)\,\mathbb{F}_q\left(x^{-1}\right) &= \mathcal{N}(x)\left(\mathcal{S}\left(x^{-1}\right) + \mathcal{N}\left(x^{-1}\right) + 1\right)\\ &= \mathcal{N}(x)\,\mathcal{S}\left(x^{-1}\right) + \mathcal{N}(x)\,\mathcal{N}\left(x^{-1}\right) + \mathcal{N}(x)\end{aligned}$$

by using the fact that $\mathcal{N}$ is a SHDS, we may continue to simplify this equation to obtain

$$\begin{aligned}\mathcal{N}(x)\,\mathbb{F}_q\left(x^{-1}\right) &= \mathcal{N}(x)\,\mathcal{S}\left(x^{-1}\right) + \frac{q+1}{4} + \frac{q-3}{4}\mathbb{F}_q(x) + \mathcal{N}(x)\\ &= \mathcal{N}(x)\,\mathcal{S}\left(x^{-1}\right) + \frac{q+1}{4} + \frac{q-3}{4}\left(\mathcal{S}(x) + \mathcal{N}(x) + 1\right) + \mathcal{N}(x)\\ &= \mathcal{N}(x)\,\mathcal{S}\left(x^{-1}\right) + \frac{q-1}{2} + \frac{q-3}{4}\mathcal{S}(x) + \frac{q+1}{4}\mathcal{N}(x).\end{aligned}$$

It is clear that $\mathbb{F}_q\left(x^{-1}\right) = \mathbb{F}_q(x)$, and since $|\mathcal{N}| = \frac{q-1}{2}$, we can conclude that

$$\mathcal{N}(x)\,\mathbb{F}_q\left(x^{-1}\right) = \frac{q-1}{2}\mathbb{F}_q(x).$$

By combining these equations and continuing to simplify, we obtain

$$\begin{aligned}\frac{q-1}{2}\mathbb{F}_q(x) &= \mathcal{N}(x)\,\mathcal{S}\left(x^{-1}\right) + \frac{q-1}{2} + \frac{q-3}{4}\mathcal{S}(x) + \frac{q+1}{4}\mathcal{N}(x)\\ \frac{q-1}{2}\left(\mathcal{S}(x) + \mathcal{N}(x) + 1\right) &= \mathcal{N}(x)\,\mathcal{S}\left(x^{-1}\right) + \frac{q-1}{2} + \frac{q-3}{4}\mathcal{S}(x) + \frac{q+1}{4}\mathcal{N}(x)\\ \mathcal{N}(x)\,\mathcal{S}\left(x^{-1}\right) &= \frac{q+1}{4}\mathcal{S}(x) + \frac{q-3}{4}\mathcal{N}(x).\end{aligned}$$

We now rewrite the term on the left-hand side of the above equation. Since the squares of $\mathbb{F}_q^\star$ form a group, we have $\mathcal{N}(x) = \mathcal{N}(x^s)$ for all nonzero squares s. Using this, we obtain

$$\begin{aligned}\mathcal{N}(x)\,\mathcal{S}\left(x^{-1}\right) &= \sum_{s\in\mathcal{S}} \mathcal{N}(x)\,x^{-s}\\ &= \sum_{s\in\mathcal{S}} \mathcal{N}(x^s)\,x^{-s}.\end{aligned}$$

We readily see that each term in the above sum can be obtained by taking the group-ring element $\mathcal{N}(x)$ and multiplying the exponents by a square of $\mathbb{F}_q^\star$. Thus, each term in this sum contains a constant number of terms from $\mathcal{S}$ and a constant number of terms from $\mathcal{N}$. We thus have

$$\sum_{s\in\mathcal{S}} \mathcal{N}(x^s)\, x^{-s} = \frac{q+1}{4}\mathcal{S}(x) + \frac{q-3}{4}\mathcal{N}(x).$$

There are $\frac{q-1}{2}$ terms on the left-hand side, and each nonzero square appears exactly $\frac{q+1}{4}$ times on the right-hand side. Since there are $\frac{q-1}{2}$ nonzero squares in $\mathbb{F}_q$, and each term on the left-hand side contains the same of number of nonzero squares, we conclude that each term on the left-hand side contains exactly $\frac{q+1}{4}$ unique nonzero squares. By a similar argument, we also have that each term on the left-hand side contains $\frac{q-3}{4}$ unique nonsquares.

By the definition of SHDS, we have the equation

$$\mathcal{N}(x)\,\mathcal{N}\left(x^{-1}\right) = \frac{q+1}{4} + \frac{q-3}{4}\mathbb{F}_q(x).$$

By expanding and simplifying, we obtain

$$\sum_{n\in\mathcal{N}} \mathcal{N}(x)\, x^{-n} = \frac{q-1}{2} + \frac{q-3}{4}\mathcal{S}(x) + \frac{q-3}{4}\mathcal{N}(x).$$

Now, let $n \in \mathcal{N}$ be fixed. Note that

$$\begin{aligned}\mathcal{N}(x) &= \mathcal{N}(x^s)\\ &= \sum_{s\in\mathcal{S}} x^{sn}.\end{aligned}$$

Using this, we now have

$$\sum_{s\in\mathcal{S}} \mathcal{N}(x^s)\, x^{-sn} = \frac{q-1}{2} + \frac{q-3}{4}\mathcal{S}(x) + \frac{q-3}{4}\mathcal{N}(x).$$

By using arguments similar to those employed in the first part of the proof, we have proven the theorem. □

1.2 Characters

It initially seems that GDS's have no inherent algebraic structure in that the definition of GDS is more combinatorial than it is algebraic. For Abelian groups, however, the use of

characters yields several results for these objects. We now define characters for finite Abelian groups.

Definition 4. *Let $\mathcal{G}$ be a finite Abelian group. Then a homomorphism $\chi : \mathcal{G} \to \mathbb{C}^*$ is a character of $\mathcal{G}$.*

Although characters can be defined to map to any field and not necessarily $\mathbb{C}$, we will only consider complex characters, and they will be referred to as simply characters unless otherwise noted.

Let the set of characters of $\mathcal{G}$ be denoted by $\hat{\mathcal{G}}$. Then $\hat{\mathcal{G}}$ is a group under pointwise-group multiplication. That is, if $\chi, \psi \in \hat{\mathcal{G}}$, and $g \in \mathcal{G}$, we define $(\chi\psi)(g) = \chi(g)\psi(g)$. One can easily check that this binary operation does, indeed, define a group. This group is called the dual group of $\mathcal{G}$. It can be verified that $\hat{\mathcal{G}} \cong \mathcal{G}$, though we do not make much use of this fact.

When $\mathcal{G}$ is taken to be the additive group of a finite field, then the dual group has much more structure. This is because finite fields have more structure than arbitrary finite groups. The presence of a multiplication in a finite field provides a succinct way of defining characters of the additive group of a finite field. Arbitrary Abelian groups do not have a second binary operation to rely on in representing their characters.

In order to see how additive characters over finite fields can be defined, we must first define the concept of trace.

Definition 5. *Let q be a power of a prime p, $m \in \mathbb{N}$, $\mathbb{F} = \mathbb{F}_q$, $\mathbb{K} = \mathbb{F}_{q^m}$. Then the trace of the field extension $\mathbb{K}/\mathbb{F}$ is the function $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}} : \mathbb{K} \to \mathbb{F}$ given by*

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(x) = \sum_{i=0}^{m-1} x^{q^i}.$$

It can be shown that $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}$, indeed, maps $\mathbb{K}$ to the subfield $\mathbb{F}$ and that $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}$ is an $\mathbb{F}$-linear functional on $\mathbb{K}$. In fact, if T is any $\mathbb{F}$-linear functional on $\mathbb{K}$, then there is a unique $a \in \mathbb{K}$ such that for all $x \in \mathbb{K}$, $T(x) = \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(ax)$.

With the trace now defined, we now have an alternate way to express additive characters of finite fields.

Definition 6. *Let q be a power of a prime p, $\mathbb{F} = \mathbb{F}_p$, $\mathbb{K} = \mathbb{F}_q$, and $t \in \mathbb{K}$. Let $\mathfrak{w}$ be a primitive p-th root of unity. Then define $\chi_t \in \hat{\mathbb{K}}$ by*

$$\chi_t(x) = \mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(tx)\right).$$

The fact that χ_t is a character follows from $\mathbb{F}$-linearity of $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}$. From the above definition, the following is clear.

Lemma 7. *With the above notation, we have $\chi_t(a) = \chi_1(ta) = \chi_{ta}(1)$.*

This fact will often be used implicitly in the proofs of the results in later chapters. Another useful property of the trace function is its transitive nature which we now make precise.

Theorem 8. *Let, $\mathbb{F}$, $\mathbb{K}$, $\mathbb{L}$ be three finite fields such that $\mathbb{F} \leq \mathbb{K} \leq \mathbb{L}$, then for all $x \in \mathbb{L}$, we have $\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(x) = \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x))$.*

Using this property, we can consider how characters on finite fields behave when restricted to a subfield.

Lemma 9. *Let $\chi_t \in \hat{\mathbb{L}}$, and let $\mathfrak{X} = \chi_t|_{\mathbb{K}}$. Then $\mathfrak{X} \in \hat{\mathbb{K}}$, and $\mathfrak{X} = \mathfrak{X}_{t'}$, where $t' = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t)$.*

Proof. Let $x \in \mathbb{K}$. We compute $\chi_t(x)$.

$$\begin{aligned}
\chi_t(x) &= \mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(tx)\right) \\
&= \mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(tx)\right) \\
&= \mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(x\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t))\right) \\
&= \mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(t'x)\right) \\
&= \mathfrak{X}'_{t'}(x).
\end{aligned}$$

Above we used transitivity of the trace function and $\mathbb{K}$-linearity of $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$. □

1.3 Orthogonality and its Consequences

The most important reason why characters are useful is because of the orthogonality relations. Here we state without proof one such relation as it relates to characters over finite fields.

Theorem 10. *Let $\mathcal{G}$ be an Abelian group with $|\mathcal{G}| = n$ and $x \in \mathcal{G}$. Then we have the following:*

$$\frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\chi(x) = \begin{cases} 1 & \text{if } x = 0, \\ 0 & \text{otherwise.} \end{cases}$$

For the special case in which $\mathcal{G}$ is a finite field, this becomes the following:

Corollary 11. *Let p be a prime, $n \in \mathbb{N}$, $q = p^n$, $\mathbb{F} = \mathbb{F}_q$, and $x \in \mathbb{F}$. Then we have the following:*

$$\frac{1}{q}\sum_{t\in\mathbb{F}}\chi_t(x) = \begin{cases} 1 & \text{if } a = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Thus far, we have defined the domain of characters to be a finite Abelian group. We can extend this definition so that characters can be evaluated on subsets of elements of finite Abelian groups. Namely, if $\mathcal{G}$ is a finite Abelian group and $\mathcal{S} \subseteq \mathcal{G}$, then for all $\chi \in \hat{\mathcal{G}}$, we define

$$\chi(\mathcal{S}) = \sum_{s\in\mathcal{S}}\chi(s). \tag{1.1}$$

In the following chapters equations involving character sums over subsets will frequently be used. As such, the following identities will be useful.

Theorem 12. *Let $\mathcal{G}$ be an Abelian group written additively with $|\mathcal{G}| = n$ and identity 0, and let $\mathcal{S} \subseteq \mathcal{G}$. The the following equation holds.*

$$\frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\chi(\mathcal{S}) = \begin{cases} 1 & \text{if } 0 \in \mathcal{S}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By using the definition of $\chi(\mathcal{S})$ and orthogonality, we have

$$\begin{aligned}\frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\chi(\mathcal{S}) &= \frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\sum_{s\in\mathcal{S}}\chi(s)\\ &= \frac{1}{n}\sum_{s\in\mathcal{S}}\sum_{\chi\in\hat{\mathcal{G}}}\chi(s).\end{aligned}$$

In the above summation, if $0 \notin \mathcal{S}$, then all terms in the innermost sum are 0. If $0 \in \mathcal{S}$, then all terms are 0 except for the term corresponding to $s = 0$, which is 1. This completes the proof. □

It should be noted that in most applications of this theorem, the group $\mathcal{G}$ is the additive group of a finite field, and $0 \notin \mathcal{S}$.

Another type of quantity that often appears involves the moduli of character sums. The next theorem provides a way to evaluate such sums.

Theorem 13. *Let $\mathcal{G}$ be an Abelian group written additively with $|\mathcal{G}| = n$, and let $\mathcal{S} \subseteq \mathcal{G}$. Then the following equation holds:*

$$\frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}|\chi(\mathcal{S})|^2 = |\mathcal{S}|\,.$$

Proof. Recall that if $z \in \mathbb{C}$, then $|z|^2 = z\bar{z}$. This fact allows us to rewrite the above summation as

$$\frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}|\chi(\mathcal{S})|^2 = \frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\chi(\mathcal{S})\overline{\chi(\mathcal{S})}.$$

We now expand the characters evaluated on $\mathcal{S}$ to obtain

$$\frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\chi(\mathcal{S})\overline{\chi(\mathcal{S})} = \frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\left(\sum_{s\in\mathcal{S}}\chi(s)\overline{\sum_{t\in\mathcal{S}}\chi(t)}\right).$$

Since complex conjugation respects addition we simplify to get

$$\frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\left(\sum_{s\in\mathcal{S}}\chi(s)\overline{\sum_{t\in\mathcal{S}}\chi(t)}\right) = \frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\left(\sum_{s\in\mathcal{S}}\chi(s)\sum_{t\in\mathcal{S}}\overline{\chi(t)}\right).$$

Since for all $z \in \mathbb{C}$ we have $\bar{z} = |z|^2 z^{-1}$, and since character values are all roots of unity, which have modulus 1, we conclude that $\overline{\chi(t)} = (\chi(t))^{-1}$ for all $t \in \mathcal{S}$. Using this, we now have

$$\frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}|\chi(\mathcal{S})|^2 = \frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\left(\sum_{s\in\mathcal{S}}\chi(s)\sum_{t\in\mathcal{S}}(\chi(t))^{-1}\right).$$

Because characters are group homomorphisms, it is clear that $(\chi(t))^{-1} = \chi(-t)$. By using this fact and rearranging terms, we obtain

$$\begin{aligned}\frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\left(\sum_{s\in\mathcal{S}}\chi(s)\sum_{t\in\mathcal{S}}(\chi(t))^{-1}\right) &= \frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\left(\sum_{s\in\mathcal{S}}\chi(s)\sum_{t\in\mathcal{S}}\chi(-t)\right)\\ &= \frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{S}}\chi(s-t)\\ &= \sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{S}}\left(\frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\chi(s-t)\right).\end{aligned}$$

The innermost sum is 0 whenever $s - t \neq 0$, that is, when $s \neq t$, and the innermost sum is 1 whenever $s = t$. Thus, the only nonzero terms of this sum occur when $s = t$. We therefore have

$$\begin{aligned}\sum_{s\in\mathcal{S}}\sum_{t\in\mathcal{S}}\left(\frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\chi(s-t)\right) &= \sum_{s\in\mathcal{S}}\left(\frac{1}{n}\sum_{\chi\in\hat{\mathcal{G}}}\chi(0)\right)\\ &= \sum_{s\in\mathcal{S}}1\\ &= |\mathcal{S}|.\end{aligned}$$

This completes the proof. □

Fix $\mathcal{D} \subseteq \mathbb{F}_q^\star$ with $\mathcal{D}$ nonempty. We will be interested in counting, for any $w \in \mathbb{F}_q^\star$, the number λ_w of ways in which we can write $w = d_1 - d_2$ with $d_i \in \mathcal{D}$. A classical technique for doing so follows from the orthogonality relations for characters. Indeed, we have

$$\begin{aligned}q\lambda_w &= \sum_{t\in\mathbb{F}_q}\sum_{d_1,d_2\in\mathcal{D}}\chi_t(w-(d_1-d_2))\\ &= \sum_{t\in\mathbb{F}_q}\chi_t(w)\sum_{d_1\in\mathcal{D}}\chi_t(d_1)\sum_{d_2\in\mathcal{D}}\overline{\chi_t(d_2)}\\ &= \sum_{t\in\mathbb{F}_q}\chi_t(w)\,|\chi_t(\mathcal{D})|^2,\end{aligned} \tag{1.2}$$

where $\chi_t(\mathcal{D})$ is understood to denote the partial sum of $\chi_t(d)$ as d ranges over all $\mathcal{D}$. We shall rely on this classical equation in our general approach to establishing whether a given set $\mathcal{D}$ is a GDS, PDS or DS, see Chapter 4.

Chapter 2

A NONEXISTENCE RESULT FOR CERTAIN PDS

Let $\mathcal{G}$ be an Abelian group written additively with $|\mathcal{G}| = v$, and let $\mathcal{D} \subseteq \mathcal{G}$. Also, let $\hat{\mathcal{G}}$ denote the dual group of $\mathcal{G}$. Then the following equation holds for all nonzero $w \in \mathcal{G}$:

$$\lambda_w = \frac{1}{v} \sum_{\chi \in \hat{\mathcal{G}}} \chi(w) \ |\chi(\mathcal{D})|^2 ,$$

where λ_w is the number of representation of w as differences of two elements of $\mathcal{D}$. In this chapter, we shall prove the following theorem.

Theorem 14. *Let $\mathcal{D}$ be a (v, k, λ, μ)-PDS contained in a finite Abelian group $\mathcal{G}$. Let $r, s \in \mathbb{Z}$ with $r \neq s$ and suppose $\chi(\mathcal{D}) \in \{r, s\}$ for each non-principal character χ of $\hat{\mathcal{G}}$. Then $\frac{v\lambda_w + s^2 - k^2}{r^2 - s^2}$ must be an integer for all $w \in \mathcal{G}^\star$.*

The motivation for this result stems from computation related to the method for constructing PDS outlined in Chapter 4. Specifically, through computation we obtained a (243,110,66,9,25)-GDS, which will be explored further in Chapter 9. These parameters are remarkably close to a strongly regular graph parameter, (243,66,9,21), which was listed in Brouwer's webpage as open. After initial attempts to manipulate the GDS into a PDS, the above theorem was established. While this proved that no Abelian (243,66,9,21)-PDS exists, our theorem was preceded by six months by a paper posted on arXiv, which proves a more general statement, see the paper of De Winter, Kamischke and Wang [7].

Now, suppose $\mathcal{D}$ is a (v, k, λ, μ)-PDS of $\mathcal{G}$. Then if $\lambda \neq \mu$, we have the following character sum for all $\chi \neq \chi_0$.

$$\chi(\mathcal{D}) = \frac{(\lambda - \mu) \pm \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}}{2}.$$

This is obtained by manipulating the group-ring equation for PDS's.

We now establish some facts regarding the uniformity of character values evaluated on a fixed group element.

Lemma 15. *Let $w \in \mathcal{G}$ be fixed and arbitrary, and let $|\mathcal{G}| = v$. Then for all $\chi \in \hat{\mathcal{G}}$, the values of $\chi(w)$ all lie in $\langle \mathfrak{w} \rangle$, where $\mathfrak{w}$ is a primitive d-th root of unity for some $d|v$. Moreover, as χ varies over $\hat{\mathcal{G}}$, each value in $\langle \mathfrak{w} \rangle$ is attained exactly $\frac{v}{d}$ times.*

Proof. Define the following function:

$$\Phi : \hat{\mathcal{G}} \to \mathbb{C}^\star$$
$$\chi \mapsto \chi(w).$$

It is routine to show that this is a group homomorphism. This means that $\mathrm{Im}(\Phi) \leq \mathbb{C}^\star$, so $\mathrm{Im}(\Phi) = \langle \mathfrak{w} \rangle$, where $\mathfrak{w}$ is a d-th root of unity for some natural number d. By the homomorphism theorems, we have that $d|v$, and $|\ker(\Phi)| = \frac{v}{d}$, and the proof is complete. □

We now proceed to prove Theorem 14. From (1.2), we have

$$v\lambda_w = \sum_{\chi \in \hat{\mathcal{G}}} \chi(w)|\chi(\mathcal{D})|^2.$$

We now examine the terms on the right-hand side. As χ ranges over all of $\hat{\mathcal{G}}$, $\chi(w)$ ranges over all d-th roots of unity uniformly, for some $d|n$. We also have that $|\chi(\mathcal{D})|^2 = r^2$ or s^2 for non-principal χ. Therefore, each term on the right-hand side can attain one of $2d$ possible values for non-principal χ. We now consider the frequencies with which these values are attained. In order to do this, we let $A_{ir} = \left|\{\chi \in \hat{\mathcal{G}} : \chi(w) = \mathfrak{w}^i \text{ and } \chi(\mathcal{D}) = r\}\right|$, and $A_{is} = \left|\{\chi \in \hat{\mathcal{G}} : \chi(w) = \mathfrak{w}^i \text{ and } \chi(\mathcal{D}) = s\}\right|$ for $i = 0, \ldots, d-1$. We can use 15 above to rewrite the sum on the right-hand side. Note that $A_{ir} + A_{is} = \frac{v}{d}$ for all $i \neq 0$, and $A_{0r} + A_{0s} = \frac{v}{d} - 1$. The

$i = 0$ case must be taken care of separately to account for the fact that $\chi_0(\mathcal{D}) = k$ and not r or s. We have

$$\begin{aligned}
\sum_{\chi \in \hat{\mathcal{G}}} \chi_(w)\ |\chi(\mathcal{D})|^2 &= \sum_{i=0}^{d-1} \left(r^2 A_{ir} \mathfrak{w}^i + s^2 A_{is} \mathfrak{w}^i \right) + |\chi_0(\mathcal{D})|^2 \\
&= r^2 A_{0r} + s^2 A_{0s} + \sum_{i=1}^{d-1} \left(r^2 A_{ir} \mathfrak{w}^i + s^2 A_{is} \mathfrak{w}^i \right) + k^2 \\
&= r^2 A_{0r} + s^2 \left(\frac{v}{d} - 1 - A_{0r} \right) + \sum_{i=1}^{d-1} \left(r^2 A_{ir} \mathfrak{w}^i + s^2 \left(\frac{v}{d} - A_{ir} \right) \mathfrak{w}^i \right) + k^2 \\
&= \sum_{i=0}^{d-1} \left((r^2 - s^2) A_{ir} \mathfrak{w}^i + s^2 \frac{v}{d} \mathfrak{w}^i \right) - s^2 + k^2.
\end{aligned}$$

Recall that the sum of the nth roots of unity is 0 for all $n > 1$. This causes the $s^2 \frac{v}{d} \mathfrak{w}^i$ term in the summation to vanish.

$$\begin{aligned}
\sum_{\chi \in \hat{\mathcal{G}}} \chi(w)\ |\chi(\mathcal{D})|^2 &= \sum_{i=0}^{d-1} \left((r^2 - s^2) A_{ir} \mathfrak{w}^i \right) - s^2 + k^2 \\
&= (r^2 - s^2) \sum_{i=0}^{d-1} A_{ir} \mathfrak{w}^i - s^2 + k^2.
\end{aligned}$$

Combining these equations yields the following:

$$\frac{v\lambda_w + s^2 - k^2}{r^2 - s^2} = \sum_{i=0}^{d-1} A_{ir} \mathfrak{w}^i.$$

Note that the right-hand side is clearly an algebraic integer and the the left-hand side is clearly a rational number. The only numbers that are both algebraic integers and rational numbers are the rational integers. Therefore, the left-hand side is an integer. This completes the proof of Theorem 14.

Chapter 3

NEO-DIFFERENCE SETS

Just as the definition of a PDS of $\mathcal{G}$ can be expressed in terms of the group-ring $\mathbb{Z}\mathcal{G}$, so too, can the definition of a neo-difference set of $\mathcal{G}$. With the same notation as in 2, let $\mathcal{N} = \mathcal{U}_1 + \mathcal{U}_2 + \mathcal{U}_3 \in \mathbb{Z}\mathcal{G}$. Then $\mathcal{D}$ is a neo-difference set of $\mathcal{G}$ if the following group-ring equation holds:

$$\mathcal{D}\mathcal{D}^{(-1)} = n + \mathcal{G} - \mathcal{N}. \tag{3.1}$$

In this chapter we shall establish the following generalization of a result of Ghinelli and Jungnickel [11], who established it for $p = 3$.

Theorem 16. *Let $\mathcal{G}$ be a finite Abelian group with neo-difference set $\mathcal{D}$ of order pm, with p and odd prime and $p \nmid m$. Then*

$$\mathcal{D}^{p-1} + (\mathcal{D}^{(-1)})^{p-1} = 1 - 2\mathcal{G} - \mathcal{N}$$

in $\mathbb{Z}_p\mathcal{G}$.

In the $p = 3$ case, this result was then used in [11] to prove that if n is the order of a projective plane of Lenz-Barlotti type I.4 and $3 \mid n$, then either $n = 3$ or $9 \mid n$. This proof relied on finding coefficients of group elements in the above equation. Since p is a small prime, these coefficients are relatively tractable. For greater primes, p, however, there are more terms to consider, and the process is much more difficult.

3.1 Results without restriction on n

The proof of Theorem 16 requires many computations. We now start with those computations that do not impose any conditions on n. The results in the following lemma are almost immediate.

Lemma 17. *Let $A, B \in \mathbb{Z}\mathcal{G}$. Then the following statements hold in $\mathbb{Z}\mathcal{G}$.*

(i) $(AB)^{(-1)} = A^{(-1)}B^{(-1)}$.

(ii) $(A + B)^{(-1)} = A^{(-1)} + B^{(-1)}$.

(iii) For any $k \in \mathbb{Z}$, $(A^{(-1)})^k = (A^k)^{(-1)}$.

For $A = \sum_{g\in\mathcal{G}} a_g g \in \mathbb{Z}\mathcal{G}$, define $[A] = \sum_{g\in\mathcal{G}} a_g$. From this we have

Lemma 18. *For $\mathcal{H} \leq \mathcal{G}$ and $A \in \mathbb{Z}\mathcal{H}$, $\mathcal{H}A = [A]\mathcal{H}$. In particular, $\mathcal{G}A = [A]\mathcal{G}$.*

Proof. This is clear from the fact that for all $h \in \mathcal{H}$, we have $h\mathcal{H} = \mathcal{H}$. Since A is a sum of integer multiples of elements of $\mathcal{H}$, the proof is complete. □

We now apply this lemma to obtain some useful identities.

Corollary 19. *The following statements hold in $\mathbb{Z}\mathcal{G}$.*

(i) $\mathcal{G}^2 = (n-1)^2\mathcal{G}$.

(ii) $\mathcal{G}\mathcal{N} = 3(n-1)\mathcal{G}$.

(iii) For any $\mathcal{H} \leq \mathcal{G}$ and any $A \in \mathbb{Z}\mathcal{G}$, we have $\mathcal{H}A = \mathcal{H}A^{(-1)}$.

(iv) $\mathcal{N}^2 = 6\mathcal{G} + (n-1)\mathcal{N}$.

Proof. (i) Note that $[\mathcal{G}] = (n-1)^2$.

(ii) Here, note that $[\mathcal{N}] = 3(n-1)$

(iii) Inverting elements of a group-ring element does not change the multi-set of coefficients. Thus, $[A] = [A^{(-1)}]$.

(iv) Since $\mathcal{N}$ is not a subgroup of $\mathcal{G}$, we expand $\mathcal{N}$ and compute, noting that $[\mathcal{U}_i] = n - 1$ for $i = 1, 2, 3$.

$$\begin{aligned}
\mathcal{N}^2 &= (\mathcal{U}_1 + \mathcal{U}_2 + \mathcal{U}_3)(\mathcal{U}_1 + \mathcal{U}_2 + \mathcal{U}_3) \\
&= \mathcal{U}_1^2 + \mathcal{U}_2^2 + \mathcal{U}_3^2 + 2\mathcal{U}_1\mathcal{U}_2 + 2\mathcal{U}_1\mathcal{U}_3 + 2\mathcal{U}_2\mathcal{U}_3 \\
&= (n-1)\mathcal{U}_1 + (n-1)\mathcal{U}_2 + (n-1)\mathcal{U}_3 + 2\mathcal{G} + 2\mathcal{G} + 2\mathcal{G} \\
&= (n-1)\mathcal{N} + 6\mathcal{G},
\end{aligned}$$

□

Lemma 20. *Let $k \in \mathbb{N}$. In $\mathbb{Z}\mathcal{G}$, we have*

$$\mathcal{N}\mathcal{D}^{2k} = \mathcal{N} - 3\mathcal{G}\sum_{i=0}^{2k-1}(2-n)^i.$$

Furthermore, if n is even, then

$$\mathcal{N}\mathcal{D}^{k} = (-1)^k\left(\mathcal{N} - 3\mathcal{G}\sum_{i=0}^{k-1}(2-n)^i\right).$$

Proof. We have

$$\begin{aligned}
\mathcal{N}\mathcal{D} &= \mathcal{D}\mathcal{U}_1 + \mathcal{D}\mathcal{U}_2 + \mathcal{D}\mathcal{U}_3 \\
&= (\mathcal{G} - \mathcal{U}_1) + (\mathcal{G} - \mathcal{U}_2) + (\mathcal{G} - \mathcal{U}_3(1,\theta)) \\
&= 3\mathcal{G} - \mathcal{U}_1 - \mathcal{U}_2 - \mathcal{U}_3(1,\theta),
\end{aligned}$$

and

$$\begin{aligned}
\mathcal{N}\mathcal{D}^2 &= 3\mathcal{D}\mathcal{G} - \mathcal{D}\mathcal{U}_1 - \mathcal{D}\mathcal{U}_2 - \mathcal{D}\mathcal{U}_3(1,\theta) \\
&= 3(n-2)\mathcal{G} - (\mathcal{G} - \mathcal{U}_1) - (\mathcal{G} - \mathcal{U}_2) - (1,\theta)(\mathcal{G} - \mathcal{U}_3(1,\theta)) \\
&= 3(n-2)\mathcal{G} - 3\mathcal{G} + (\mathcal{U}_1 + \mathcal{U}_2 + (1,\theta)^2\mathcal{U}_3) \\
&= 3(n-2)\mathcal{G} - 3\mathcal{G} + (\mathcal{U}_1 + \mathcal{U}_2 + \mathcal{U}_3) \\
&= 3(n-2)\mathcal{G} - 3\mathcal{G} + \mathcal{N},
\end{aligned}$$

where we have used $\theta^2 = 1$. Inducting on the identity for $\mathcal{N}\mathcal{D}^2$ now proves the first claim. If n is even, then $\theta = 1$ and we actually have $\mathcal{N}\mathcal{D} = 3\mathcal{G} - \mathcal{N}$. Now induction will yield the second claim. □

Lemma 21. *Let $k \in \mathbb{N}$. In $\mathbb{Z}\mathcal{G}$, we have*

$$\begin{aligned}&(n+\mathcal{G}-\mathcal{N})^k\\&\quad= n^k+\mathcal{G}\left(\sum_{i=0}^{k-1}(n-2)^{2i}n^{k-1-i}+(9-3n)\sum_{i=1}^{k-1}(n-2)^{2(k-1-i)}\left(\frac{n^i-1}{n-1}\right)\right)\\&\qquad-\mathcal{N}\left(\frac{n^k-1}{n-1}\right).\end{aligned}$$

Proof. Let $(n+\mathcal{G}-\mathcal{N})^k = a_k n + b_k\mathcal{G} - c_k\mathcal{N}$, where $a_k, b_k, c_k \in \mathbb{Z}$. We use the following recurrence:

$$\begin{aligned}a_k + b_k\mathcal{G} - c_k\mathcal{N} &= (n+\mathcal{G}-\mathcal{N})^k\\&= (n+\mathcal{G}-\mathcal{N})^{k-1}(n+\mathcal{G}-\mathcal{N})\\&= (a_{k-1}n + b_{k-1}\mathcal{G} - c_{k-1}\mathcal{N})(n+\mathcal{G}-\mathcal{N})\\&= a_{k-1}nn + b_{k-1}n\mathcal{G} - c_{k-1}n\mathcal{N}\\&\quad + a_{k-1}n\mathcal{G} + b_{k-1}\mathcal{G}^2 - c_{k-1}\mathcal{N}\mathcal{G}\\&\quad - a_{k-1}n\mathcal{N} - b_{k-1}\mathcal{N}\mathcal{G} + c_{k-1}\mathcal{N}^2\\&= (a_{k-1}n)n + b_{k-1}n\mathcal{G} - c_{k-1}n\mathcal{N}\\&\quad + a_{k-1}n\mathcal{G} + b_{k-1}(n-1)^2\mathcal{G} - c_{k-1}3(n-1)\mathcal{G}\\&\quad - a_{k-1}n\mathcal{N} - b_{k-1}3(n-1)\mathcal{G} + c_{k-1}((n-1)\mathcal{N} + 6\mathcal{G})\\&= (a_{k-1}n)n - \mathcal{N}(c_{k-1}n + a_{k-1}n - c_{k-1}(n-1))\\&\quad + \mathcal{G}(b_{k-1}n + a_{k-1}n + b_{k-1}(n-1)^2\\&\quad - c_{k-1}3(n-1) - b_{k-1}3(n-1) + 6c_{k-1}).\end{aligned}$$

So, with initial conditions $a_1 = b_1 = c_1 = 1$, we find

$$\begin{aligned}a_k &= a_{k-1}n,\\b_k &= a_{k-1}n + b_{k-1}(n-2)^2 + c_{k-1}(9-3n),\\c_k &= c_{k-1} + a_{k-1}n.\end{aligned}$$

Immediately, we have $a_k = n^{k-1}$. Substituting into the recurrence for c_k now yields

$$c_k = c_{k-1} + n^{k-1} = \frac{n^k-1}{n-1}.$$

Returning to b_k, we have the identity

$$b_k = n^{k-1} + b_{k-1}(n-2)^2 + (9-3n)\left(\frac{n^{k-1}-1}{n-1}\right),$$

from which an induction argument proves the claim. □

3.2 Results with restrictions on n

Following [11], central to our proof of Theorem 16 is the following result.

Lemma 22. *Suppose p is an odd prime dividing n. Then*

$$n(\mathcal{D}^{p-1} + (\mathcal{D}^{(-1)})^{p-1}) \equiv (n + \mathcal{G} - \mathcal{N})^p + (n + \mathcal{G} - \mathcal{N}) - 2\mathcal{G}\mathcal{D}^{p-1} + 2\mathcal{N}\mathcal{D}^{p-1} \bmod p^2. \quad (3.2)$$

Proof. As p divides n, Theorem 5.3 of [10] shows that $\mathcal{D}^{(p)} = \mathcal{D}$ in $\mathbb{Z}\mathcal{G}$. Since we also have $\mathcal{D}^p \equiv \mathcal{D}^{(p)} \bmod p$, there must exist some $A \in \mathbb{Z}\mathcal{G}$ satisfying $pA = \mathcal{D}^p - \mathcal{D}$. We also have $pA^{(-1)} = (\mathcal{D}^p)^{(-1)} - \mathcal{D}^{(-1)}$. Thus

$$\begin{aligned} 0 &\equiv (pA)(pA^{(-1)}) \bmod p^2 \\ &\equiv (\mathcal{D}\mathcal{D}^{(-1)})^p + \mathcal{D}\mathcal{D}^{(-1)} - \mathcal{D}(\mathcal{D}^{(-1)})^p - \mathcal{D}^p\mathcal{D}^{(-1)} \bmod p^2 \\ &\equiv (\mathcal{D}\mathcal{D}^{(-1)})^p + \mathcal{D}\mathcal{D}^{(-1)}(1 - (\mathcal{D}^{(-1)})^{p-1} - \mathcal{D}^{p-1}) \bmod p^2. \end{aligned}$$

As $\mathcal{D}$ is a neo-difference set, we have $\mathcal{D}\mathcal{D}^{(-1)} = n + \mathcal{G} - \mathcal{N}$, and by rearranging we find

$$\begin{aligned} &n(\mathcal{D}^{p-1} + (\mathcal{D}^{(-1)})^{p-1}) \\ &\quad\equiv (n + \mathcal{G} - \mathcal{N})^p + (n + \mathcal{G} - \mathcal{N}) - (\mathcal{G} - \mathcal{N})(\mathcal{D}^{p-1} + (\mathcal{D}^{(-1)})^{p-1}) \bmod p^2. \end{aligned}$$

By Corollary 19 (iii), $\mathcal{G}\mathcal{D}^{p-1} = \mathcal{G}(\mathcal{D}^{(-1)})^{p-1}$, while $\mathcal{N}\mathcal{D}^{p-1} = \mathcal{N}(\mathcal{D}^{(-1)})^{p-1}$ follows from Lemma 20. This establishes the claim. □

We now proceed to compute the parts of the equation of Lemma 22.

Lemma 23. *The following statements hold in $\mathbb{Z}\mathcal{G}$.*

(i) For any $k \in \mathbb{N}$, $\mathcal{G}\mathcal{D}^k = (n-2)^k\mathcal{G}$. In particular, if p is an odd prime dividing n, then

$$\mathcal{G}\mathcal{D}^{p-1} \equiv 2^{p-2}(2+n)\mathcal{G} \bmod p^2.$$

(ii) If p is an odd prime dividing n, then

$$\mathcal{N}\mathcal{D}^{p-1} \equiv \mathcal{N} + 3(1-2^{p-1})\mathcal{G} + 3n\mathcal{G}(1-2^{p-2}3) \bmod p^2.$$

Proof. The first claim is immediate from Lemma 18. For the remainder of (i) we have

$$\begin{aligned}
\mathcal{G}\mathcal{D}^{p-1} &= (n-2)^{p-1}\mathcal{G} \\
&\equiv \left((-2)^{p-1} + (p-1)n(-2)^{p-2}\right)\mathcal{G} \bmod p^2 \\
&\equiv (2^{p-1} + (-1)^{p-1}2^{p-2}n)\mathcal{G} \bmod p^2 \\
&\equiv 2^{p-2}(2+n)\mathcal{G} \bmod p^2,
\end{aligned}$$

as desired. Appealing to Lemma 20 yields

$$\begin{aligned}
\mathcal{N}\mathcal{D}^{p-1} &= \mathcal{N} - 3\mathcal{G}\sum_{i=0}^{p-2}(2-n)^i \\
&\equiv \mathcal{N} - 3\mathcal{G}\sum_{i=0}^{p-2}2^i + 3n\mathcal{G}\sum_{i=1}^{p-2}i2^{i-1} \bmod p^2 \\
&\equiv \mathcal{N} + 3(1-2^{p-1})\mathcal{G} + 3n\mathcal{G}\sum_{i=1}^{p-2}i2^{i-1} \bmod p^2,
\end{aligned}$$

where we have used $n^k \equiv 0 \bmod p^2$ for $k \geq 2$ extensively. The above sum is part of a well-known induction question for undergraduates satisfying

$$\sum_{i=1}^{k} i2^{i-1} = 1 + (k-1)2^k.$$

Applying the identity now yields the claimed result. □

The only part of (3.2) that requires some care to compute is the $(n + \mathcal{G} - \mathcal{N})^p$ component.

Lemma 24. *Suppose p is an odd prime dividing n. Then*

$$(n + \mathcal{G} - \mathcal{N})^p \equiv (4^p - 3)(1+2n)\mathcal{G} - (1+n)\mathcal{N} \bmod p^2.$$

Proof. It is easily seen that

$$\frac{n^p - 1}{n - 1} \equiv n + 1 \bmod p^2,$$

so the parts of $(n + \mathcal{G} - \mathcal{N})^p$ that we need to consider are the coefficients of $\mathcal{G}$ in Lemma 21.

Firstly,

$$\begin{aligned}
\sum_{i=0}^{p-1}(n-2)^{2i}n^{p-1-i} &\equiv (n-2)^{2(p-1)} + (n-2)^{2(p-2)}n \bmod p^2 \\
&\equiv (n-2)^{2(p-2)}\left(n^2 - 4n + 4 + n\right) \bmod p^2 \\
&\equiv (n^2 - 4n + 4)^{p-2}(4 - 3n) \bmod p^2 \\
&\equiv 4^{p-2}(4 - 3n)(1 - n)^{p-2} \bmod p^2 \\
&\equiv 4^{p-2}(4 - 3n)(1 + 2n) \bmod p^2 \\
&\equiv 4^{p-2}(4 + 5n) \bmod p^2.
\end{aligned}$$

Next, we have

$$\begin{aligned}
&(9 - 3n)\sum_{i=1}^{p-1}(n-2)^{2(p-1-i)}\left(\frac{n^i - 1}{n - 1}\right) \\
&\quad\equiv (9 - 3n)(n-2)^{2(p-2)} + (9 - 3n)(1 + n) \\
&\qquad + (9 - 3n)\sum_{i=2}^{p-2}(n-2)^{2(p-1-i)}(1 + n) \bmod p^2 \\
&\quad\equiv (9 - 3n)(n^2 - 4n + 4)^{p-2} + (9 + 6n) \\
&\qquad + (9 + 6n)\sum_{i=2}^{p-2}(n^2 - 4n + 4)^{p-1-i} \bmod p^2 \\
&\quad\equiv 4^{p-2}(9 - 3n)(1 - n)^{p-2} + (9 + 6n) \\
&\qquad + (9 + 6n)\sum_{i=2}^{p-2}4^{p-1-i}(1 - n)^{p-1-i} \bmod p^2 \\
&\quad\equiv 4^{p-2}(9 - 3n)(1 + 2n) + (9 + 6n) + (9 + 6n)\sum_{i=1}^{p-3}4^i(1 - n)^i \bmod p^2 \\
&\quad\equiv 4^{p-2}(9 + 15n) + (9 + 6n) + (9 + 6n)\sum_{i=1}^{p-3}4^i(1 - in) \bmod p^2
\end{aligned}$$

$$\equiv 4^{p-2}(9+15n)+(9+6n)+(9+6n)\sum_{i=1}^{p-3}4^i-9n\sum_{i=1}^{p-3}i4^i \bmod p^2$$

$$\equiv 4^{p-2}(9+15n)+(9+6n)+(3+2n)4(4^{p-3}-1)-9n\sum_{i=1}^{p-3}i4^i \bmod p^2$$

$$\equiv 4^{p-2}(12+17n)-(3+2n)-9n\sum_{i=1}^{p-3}i4^i \bmod p^2.$$

Noting that for all $k \geq 1$,

$$\sum_{i=1}^{k} i4^i = \frac{1}{3}k4^{k+1}+\frac{1}{9}(4-4^{k+1}),$$

we thus find that

$$(9-3n)\sum_{i=1}^{p-1}(n-2)^{2(p-1-i)}\left(\frac{n^i-1}{n-1}\right)$$

$$\equiv 4^{p-2}(12+17n)-(3+2n)-9n\sum_{i=1}^{p-3}i4^i \bmod p^2$$

$$\equiv 4^{p-2}(12+17n)-(3+2n)-3n(p-3)4^{p-2}-n(4-4^{p-2}) \bmod p^2$$

$$\equiv 4^{p-2}(12+17n)-(3+2n)+9n4^{p-2}-4n+n4^{p-2} \bmod p^2$$

$$\equiv 4^{p-2}(12+27n)-(3+6n) \bmod p^2.$$

Summing the respective parts and simplifying now yields the claim. □

3.3 Proof of Theorem 16

We are now in a position to prove Theorem 16. Suppose p is an odd prime and $n = pm$ with $p \nmid m$. We appeal to (3.2) and simplify:

$$\begin{aligned}
&n(D^{p-1}+(D^{(-1)})^{p-1}) \\
&\quad\equiv -(1+n)N + (4^p-3)(1+2n)G + n + G - N - 2\left(2^{p-2}(2+n)G\right) \\
&\qquad + 2\left(N + 3(1-2^{p-1})G + 3nG - 2^{p-2}9nG\right) \bmod p^2 \\
&\quad\equiv G(4^p - 3 + 2n4^p - 6n + 1 - 2^p - 2^{p-1}n + 6 - 2^p 3 + 6n - 2^{p-1}9n) \\
&\qquad + n - nN \bmod p^2 \\
&\quad\equiv n - nN + G(4^p + 4 - 4\cdot 2^p + n(2\cdot 4^p - 10\cdot 2^{p-1})) \bmod p^2 \\
&\quad\equiv n - nN + G((2^p-2)^2 + n(2\cdot 4^p - 5\cdot 2^p)) \bmod p^2 \\
&\quad\equiv n - nN + nG(2\cdot 4^p - 5\cdot 2^p) \bmod p^2.
\end{aligned}$$

As $p \nmid m$, we may cancel the multiple of n and work modulo p. This yields

$$\begin{aligned}
D^{p-1} + (D^{(-1)})^{p-1} &\equiv 1 - N + G(2\cdot 4^p - 5\cdot 2^p) \bmod p \\
&\equiv 1 - N + G(2\cdot 4 - 5\cdot 2) \bmod p \\
&\equiv 1 - 2G - N \bmod p,
\end{aligned}$$

which establishes Theorem 16.

While Theorem 16 gives an affirmative answer to the first part of Remark 2 of [11], there still remains the task of finding a suitable argument which generalizes the main theorem of [11] – i.e. to produce a general proof showing that if G is an Abelian neo-difference set of order pn, with p a prime, then $n = 1$ or $p|n$. The main stumbling block in doing so concerns obtaining suitably tight statements concerning D^{p-1} and $(D^{(-1)})^{p-1}$ modulo the prime p.

Chapter 4

PDS CONSTRUCTION SCHEME

We now move to outline a general approach for finding subsets with regularity of differences by using polynomials having regularity of images, though we only rely on the latter towards the end of the approach.

Let p be a prime, $e \in \mathbb{N}$, $v = p^e$, $a, b \in \mathbb{N}$ with $ab = v - 1$. Let $\mathbb{L} = \mathbb{F}_v$, with $\mathbb{L}^\star = \langle \mathfrak{g} \rangle$, and let $C = \langle \mathfrak{g}^a \rangle$. We first suppose the potential GDS $\mathcal{D}$ in $\mathbb{L}$ is a union of cosets of C. By doing this for infinitely many choices of e, we hope to obtain an infinite class of GDS's, PDS's, or DS's for finite fields of different orders. We now make some definitions regarding polynomials over $\mathbb{L}$ and their images.

Definition 25. *Let $f(X) \in \mathbb{L}[X]$, and let $z, r, s \in \mathbb{N}$. Denote by* $\mathrm{Im}(f)$ *the set* $\{f(x) : x \in \mathbb{F}_q\}$. *The polynomial $f(X)$ is* (r, s)-biregular *on $\mathbb{F}_q^\star$ if f has z roots in $\mathbb{F}_q$ and for any $y \in \mathrm{Im}(f) \setminus \{0\}$, the equation $f(x) = y$ has either r or s solutions $x \in \mathbb{F}_q$. The polynomial $f(X)$ is* r-regular *on $\mathbb{F}_q^\star$ if f is (r, r)-biregular. The polynomial $f(X)$ is* r-to-1 *on $\mathbb{F}_q$ if f is r-regular with $z = 1$.*

We then incorporate the general assumption that $\mathcal{D} = \mathrm{Im}(f) \setminus \{0\}$ for some r-regular polynomial f. What follows is a general approach for such classes of PDS's.

4.1 General Approach

Let $\mathcal{D} \subseteq \mathbb{L}$, $|\mathcal{D}| = k > 0$, such that $\mathcal{D} = \bigcup_{g \in \mathcal{I}} gC$ for some $\mathcal{I} \subseteq \mathbb{L}^\star$. In other words, $\mathcal{D}$ is a union of cosets of C in $\mathbb{L}^\star$. Finally, let $w \in \mathbb{L}$. In order to determine whether $\mathcal{D}$ is a PDS, we must count the number λ_w of times w can be represented as the difference of elements of $\mathcal{D}$. We have from (1.2) that

$$\lambda_w = \frac{1}{v} \sum_{t \in \mathbb{L}} \chi_t(w) \, |\chi_t(\mathcal{D})|^2 .$$

We now wish to rewrite this sum in terms of the group C. To this end, we first isolate from the sum the term corresponding to $t = 0$. In this term, $\chi_t = \chi_0$, the principal character. Since $\chi_0(x) = 1$ for all $x \in \mathbb{L}$ and $|\mathcal{D}| = k$, we obtain

$$\begin{aligned} v\lambda_w &= k^2 + \sum_{t \in \mathbb{L}^\star} \chi_t(w)\ |\chi_t(\mathcal{D})|^2 \\ &= k^2 + \sum_{t \in \mathbb{L}^\star} \chi_1(tw)\ |\chi_1(t\mathcal{D})|^2, \end{aligned} \tag{4.1}$$

where in the last step we have used the identity $\chi_t(w) = \chi_1(tw)$ for all $t, w \in \mathbb{L}$.

Next, let $\mathcal{T} = \{g_0, g_1, \ldots, g_{a-1}\}$ be a transversal of C in $\mathbb{L}^\star$. Thus, $\mathbb{L}^\star = \cup_{i=0}^{a-1} g_i C$, and every $t \in \mathbb{L}^\star$ can be written uniquely as $t = g_i c$ with $i \in \mathbb{Z}_a$, and $c \in C$. Because of this representation, the above sum can be written to range over all possible values of i and c instead of values of t:

$$v\lambda_w - k^2 = \sum_{i=0}^{a-1} \sum_{c \in C} \chi_1(g_i c w)\ |\chi_1(g_i c \mathcal{D})|^2$$

Since $\mathcal{D}$ is a union of cosets of C, we have that $c\mathcal{D} = \mathcal{D}$ for all $c \in C$. Using this fact allows us to further simplify the sum to

$$\begin{aligned} v\lambda_w - k^2 &= \sum_{i=0}^{a-1} \sum_{c \in C} \chi_1(g_i c w)\ |\chi_1(g_i \mathcal{D})|^2 \\ &= \sum_{i=0}^{a-1} |\chi_1(g_i \mathcal{D})|^2 \left(\sum_{c \in C} \chi_1(g_i c w) \right) \\ &= \sum_{i=0}^{a-1} |\chi_1(g_i \mathcal{D})|^2\ \chi_1(g_i w C). \end{aligned}$$

We now let $w = g_w c_w$, with $g_w \in \mathcal{T}$ and $c_w \in C$. Proceeding in a similar way as above, substituting and using the fact $cC = C$ holds for all $c \in C$, we obtain

$$v\lambda_w - k^2 = \sum_{i=0}^{a-1} |\chi_1(g_i \mathcal{D})|^2\ \chi_1(g_i g_w C). \tag{4.2}$$

Note that (4.2) is independent of the value of c_w. This means that λ_w depends solely on which coset of C contains w.

In the special case where $g_i = \mathfrak{g}^i$ for $i \in \mathbb{Z}_a$, we introduce additional notation. In order to do this, let $w = \mathfrak{g}^m c_w$. If we define $\mathbb{X}_j = \chi_1(\mathfrak{g}^j C)$ and $\mathbb{Y}_j = \chi_1(\mathfrak{g}^j \mathcal{D})$ for all $j \in \mathbb{Z}_a$, then

$$v\lambda_w - k^2 = \sum_{i=0}^{a-1} \left|\chi_1(\mathfrak{g}^i \mathcal{D})\right|^2 \chi_1(\mathfrak{g}^i \mathfrak{g}^m C) \tag{4.3}$$

$$= \sum_{i=0}^{a-1} |\,\mathbb{Y}_i\,|^2\ \mathbb{X}_{m+i}. \tag{4.4}$$

By the above formula, it is evident that the values of $\mathbb{X}_i$ need to be calculated for all i, as do the values of $\mathbb{Y}_i$. It is in computing these values that different classes require different methods of calculation, though there are some commonalities. Since $\mathcal{D}$ is a union of cosets of C, $\mathbb{Y}_i$ is a sum of $\mathbb{X}_j$-terms for various j. Depending on the various cases, additional structure in $\mathcal{D}$ may help in determining what $\mathbb{X}_j$ terms are in this sum. Finally, the interaction of the $\mathbb{Y}_i$ terms with the $\mathbb{X}_{m+i}$ terms must be such that the sum in the above equation can attain at most two values, and these values depend solely on w's membership in $\mathcal{D}$.

Let $f \in \mathbb{L}[X]$ such that $\left|f^{-1}(0)\right| = z$ and for all $y \in \mathbb{L}^\star$, $\left|f^{-1}(y)\right| = 0$ or r. In other words, f is r-regular on $\mathbb{F}_v^\star$ with z zeros. Set $\mathcal{D} = \mathrm{Im}(f) \setminus \{0\}$. Let $\mathbb{W}_t(f) = \sum_{x\in\mathbb{L}} \chi_t(f(x))$, called the *Weil sum* with argument $f(X)$. Due to the behavior of f, we immediately have

$$\mathbb{W}_t(f) = r\chi_t(\mathcal{D}) + z. \tag{4.5}$$

Rewritten, this is

$$\chi_t(\mathcal{D}) = \frac{1}{r}\left(\mathbb{W}_t(f) - z\right).$$

As a result, the computation of λ_w is directly connected to determining the Weil sum $\mathbb{W}_t(f)$, which is no longer a partial sum but a full character sum over $\mathbb{F}_v$. Specifically, we have

$$v\lambda_w - k^2 = \frac{1}{r^2} \sum_{i=0}^{a-1} \left|\,\mathbb{W}_{\mathfrak{g}^i}(f) - z\,\right|^2 \mathbb{X}_{m+i}. \tag{4.6}$$

It is often the case that partial sums are more intricate than Weil sums, especially when the polynomial involved generally behaves in a distinctive way. Given that the polynomial f is assumed to be r-regular, it is reasonable to have expectations that Weil sums involving f could be evaluated. As shall be seen, in practice these expectations are borne out.

Chapter 5

CLASS I

5.1 Class I

We now employ the construction scheme previously mentioned to obtain an infinite family of PDS's. For this class, we work in fields of characteristic 2. So with the notation established in Chapter 4, let $p = 2$, $e = 2n$ with $n \in \mathbb{N}$. Set $q = p^n$, so that $\mathbb{L} = \mathbb{F}_{q^2}$. Let $a = q - 1$, so $b = q + 1$. It will also help to define intermediate fields; we let $\mathbb{K} = \mathbb{F}_q$ and $\mathbb{F} = \mathbb{F}_2$. Also, let $\mathcal{H}_1 = \{y^2 - y : y \in \mathbb{K}\}$ be the subgroup of $(\mathbb{L}, +)$ containing all elements of $\mathbb{K}$ with absolute trace equal to 0. Note that this is a hyperplane of the $\mathbb{F}$-vector space $\mathbb{K}$, and that all hyperplanes of $\mathbb{K}$ can be expressed uniquely in the form $g\mathcal{H}_1$, with $g \in \mathbb{K}^\star$.

Now let $f(X) = X^2(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(X) + 1) \in \mathbb{L}[X]$ and $\mathcal{D} = \mathrm{Im}(f) \setminus \{0\}$. We will prove that $\mathcal{D}$ is a PDS.

Theorem 26. *Let $p = 2$ and $q = p^n$ with $n \in \mathbb{N}$. Set $a = q - 1$ and $b = q + 1$. Let $\mathbb{K} = \mathbb{F}_q$ and $\mathbb{L} = \mathbb{F}_{q^2}$. Define $f \in \mathbb{L}[X]$ by $f(X) = X^2(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(X) + 1)$. Let $\mathcal{D} = \mathrm{Im}(f) \setminus \{0\}$. Then $\mathcal{D}$ is a $(q^2, \frac{1}{2}(q+1)(q-2), \frac{1}{4}(q+2)(q-1), \frac{1}{4}q(q-2))$-PDS.*

We first show that f is regular.

Theorem 27. *With the above notation, $f(X)$ is 2-regular with $q + 2$ roots.*

Proof. First, the set of roots of $f(X)$ over $\mathbb{L}$ consists of 0 and the $q + 1$ distinct elements of norm 1, so we need only deal with the regularity claim. To this end, suppose $f(x) = f(y) \neq 0$ for $x, y \in \mathbb{L}$. This means that $x^2(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + 1) = y^2(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(y) + 1)$, and $xy \neq 0$. By rearranging terms we obtain

$$\left(\frac{y}{x}\right)^2 = \frac{\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + 1}{\mathrm{N}_{\mathbb{L}/\mathbb{K}}(y) + 1}.$$

It is clear that the right-hand side is an element of $\mathbb{K}^\star$, so $(\frac{y}{x})^2 \in \mathbb{K}^\star$. As $\mathbb{L}$ is characteristic 2, we also have $\frac{y}{x} \in \mathbb{K}^\star$. Let $y = ax$ with $a \in \mathbb{K}^\star$. We then have

$$x^2(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + 1) = (ax)^2(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(ax) + 1).$$

Since $\mathrm{N}_{\mathbb{L}/\mathbb{K}}$ is multiplicative and $a \in \mathbb{K}^\star$ we obtain

$$x^2(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + 1) = a^2x^2(a^2\,\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + 1).$$

By assumption, $x \neq 0$, so we may divide both sides by x^2 to get

$$\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + 1 = a^2(a^2\,\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + 1)$$

The above is a quadratic equation in a^2. We now rearrange terms to conclude

$$\begin{aligned} \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)a^4 + a^2 + (1 + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)) &= 0 \\ a^4 + (\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x))^{-1}a^2 + (1 + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x))(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x))^{-1} &= 0 \end{aligned}$$

From this equation, we conclude $a = 1$ or $(1 + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x))(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x))^{-1}$. Since

$$(1 + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x))(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x))^{-1} \neq 1,$$

we have that a^2, and hence a, attains exactly two values, and the proof is complete. □

Lemma 28. *As multiplicative groups,* $\mathbb{L}^\star \cong \mathbb{K}^\star \times C$.

Proof. Note that $\left|\mathbb{K}^\star\right| = q - 1$ and $|C| = q + 1$. Since $\mathbb{L}^\star$ is cyclic, we have that $\left|\mathbb{K}^\star \cap C\right| = \gcd(\left|\mathbb{K}^\star\right|, |C|) = 1$. We also have

$$\begin{aligned} \left|\mathbb{K}^\star C\right| &= \frac{\left|\mathbb{K}^\star\right| |C|}{|\mathbb{K}^\star \cap C|} \\ &= \frac{(q-1)(q+1)}{1} \\ &= q^2 - 1 \\ &= \left|\mathbb{L}^\star\right|. \end{aligned}$$

This means that $\mathbb{L}^\star = \mathbb{K}^\star C$. Since $\mathbb{L}^\star$ is Abelian, it is clear that both $\mathbb{K}^\star$ and C are normal in $\mathbb{L}^\star$, and the proof is complete. □

Application of (4.6) with Lemma 28 now gives

$$4(v\lambda_w - k^2) = \sum_{g\in\mathbb{K}^\star} \left|\mathsf{W}_g(f) - q - 2\right|^2 \chi_g(g_w C), \tag{5.1}$$

where $w = g_w c_w$ for some $g_w \in \mathbb{K}^\star$ and $c_w \in C$. We now evaluate $\mathsf{W}_g(f)$ with $g \in \mathbb{K}^\star$ with $g \in \mathbb{K}^\star$. By definition,

$$\begin{aligned}\mathsf{W}_g(f) &= \sum_{x\in\mathbb{L}} \chi_g\left(x^2(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)+1)\right)\\ &= 1 + \sum_{x\in\mathbb{L}^\star} \chi_g\left(x^2(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)+1)\right).\end{aligned}$$

Through Lemma 28 again, by letting $x = yc$ with $y \in \mathbb{K}^\star$ and $c \in C$, we obtain

$$\mathsf{W}_g(f) = 1 + \sum_{c\in C}\sum_{y\in\mathbb{K}^\star} \chi_g\left((yc)^2\left(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(yc)-1\right)\right).$$

Since $\mathrm{N}_{\mathbb{L}/\mathbb{K}}$ is multiplicative and $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(c) = 1$, this equation simplifies to

$$\begin{aligned}\mathsf{W}_g(f) &= 1 + \sum_{c\in C}\sum_{y\in\mathbb{K}^\star} \chi_g\left(y^2c^2(y^2-1)\right)\\ &= 1 + \sum_{c\in C}\sum_{y\in\mathbb{K}^\star} \chi_g\left(c^2y^4 - c^2y^2\right)\\ &= 1 + \sum_{c\in C}\sum_{y\in\mathbb{K}^\star} \chi_{gc^2}\left(y^4 - y^2\right).\end{aligned}$$

Since $y^4 - y^2 \in \mathbb{K}$, we may restrict χ_{gc^2} to $\mathbb{K}$. This becomes the character $\mathfrak{X}_r$, where $r = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(gc^2)$. With this restriction, the equation now becomes

$$\mathsf{W}_g(f) = 1 + \sum_{c\in C}\sum_{y\in\mathbb{K}^\star} \mathfrak{X}_r(y^4 - y^2).$$

Since $\mathfrak{X}_r$ is a homomorphism and its values are real numbers, we obtain

$$\mathsf{W}_g(f) = 1 + \sum_{c\in C}\sum_{y\in\mathbb{K}^\star} \mathfrak{X}_r(y^4)\mathfrak{X}_r(y^2).$$

Note that $\mathfrak{X}_r$ is the principal character on $\mathbb{K}$ if and only if $r = 0$. By definition, this occurs if and only if $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(gc^2) = 0$. Since $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ is $\mathbb{K}$-linear, we have $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(gc^2) = g\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c^2)$ and so this is equivalent to $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c^2) = 0$. Since $|\mathbb{L} : \mathbb{K}| = 2$, we have $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c^2) = 0$ if and only

if $c^2 \in \mathbb{K}^\star$. Since we also have that $c^2 \in C$ and $\mathbb{K}^\star \cap C = \{1\}$, we conclude that $\mathfrak{X}_r$ is the principal character on $\mathbb{K}$ if and only if $c = 1$. For $c \in C^\star$, $\mathfrak{X}_r$ will be non-principal. We isolate the terms in which $c = 1$ from the sum to obtain

$$\mathbb{W}_g(f) = q + \sum_{c \in C^\star} \sum_{y \in \mathbb{K}^\star} \mathfrak{X}_r(y^4)\mathfrak{X}_r(y^2).$$

The character values in the above sum are ± 1. In order to evaluate the sum, we must determine those values of y for which $\mathfrak{X}_r(y^4) = \mathfrak{X}_r(y^2) = 1$. Note that as y ranges over all of $\mathbb{K}^\star$, so too do y^2 and y^4, so both $\mathfrak{X}_r(y^4)$ and $\mathfrak{X}_r(y^2)$ attain the value 1 for exactly $\frac{1}{2}q - 1$ values of y and the value -1 for exactly $\frac{1}{2}q$ values of y.

We need an additional lemma.

Lemma 29. *The trace function* $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ *is* 2*-to-*1 *on* $C^\star$. *In other words, for all* $y \in \mathbb{K}$, $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c) = y$ *has either no solution or exactly two solutions for* $c \in C^\star$.

Proof. By definition of trace, we have

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c) = c + c^q,$$

and multiplying both sides by c, we obtain

$$c\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c) = c^2 + c^{q+1}.$$

But by definition of norm, $c^{q+1} = \mathrm{N}_{\mathbb{L}/\mathbb{K}}(c) = 1$. Thus,

$$c\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c) = c^2 + 1.$$

Now suppose $y \in \mathbb{K}$ with $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c) = y$ for some $c \in C^\star$. We wish to find all $x \in C^\star$ such that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = y$. We have

$$\begin{aligned} xy &= x\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) \\ &= x^2 + 1, \end{aligned}$$

so that $x^2 + yx + 1 = 0$. This quadratic has at most two roots, and by assumption $x = c$ is a root. It is also clear that $x = c^{-1}$ is also a root. These are distinct since otherwise $c^2 = 1$, which would mean $c = 1$, a contradiction. Therefore, $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c^{-1}) = y$, and the proof is complete. □

Theorem 30. *With the above notation,*

$$\mathsf{W}_g(f) = \begin{cases} 0 & \text{if } \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(gc^2) \neq 1 \text{ for all } c \in C^\star, \\ 2q & \text{otherwise.} \end{cases}$$

Proof. In general, for any $x \in \mathbb{K}$, we have $\mathfrak{X}_r(x) = 1$ if and only if $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(rx) = 0$. This is true precisely when $rx \in \mathcal{H}_1$, or equivalently, $x \in r^{-1}\mathcal{H}_1$.

Let $\mathcal{G} = \mathrm{Gal}(\mathbb{K}/\mathbb{F}) = \langle\sigma\rangle$, where $x^\sigma = x^2$ for all $x \in \mathbb{K}$. Since $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(x^\sigma) = \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(x)$ for all $x \in \mathbb{K}$, we conclude that $\mathcal{H}_1^\sigma = \mathcal{H}_1$. From this, we can also conclude that $(x\mathcal{H}_1)^\sigma = x^\sigma\mathcal{H}_1 = x^2\mathcal{H}_1$. As a consequence, $(x\mathcal{H}_1)^\sigma = x\mathcal{H}_1$ if and only if $x^2 = x$, which occurs precisely when $x = 1$.

Let $\mathcal{U} = r^{-1}\mathcal{H}_1$. We have that $\mathfrak{X}_r(y^4) = \mathfrak{X}_r(y^2) = 1$ if and only if $y^4, y^2 \in \mathcal{U}$. It is clear that $y^2 \in \mathcal{U}$ if and only if $(y^2)^\sigma \in \mathcal{U}^\sigma$. This is equivalent to $y^4 \in \mathcal{U}^\sigma$. Therefore, $\mathfrak{X}_r(y^4) = \mathfrak{X}_r(y^2) = 1$ if and only if $y^4 \in \mathcal{U} \cap \mathcal{U}^\sigma$.

We now wish to determine $|\mathcal{U} \cap \mathcal{U}^\sigma|$ for all hyperplanes $\mathcal{U}$ of $\mathbb{K}$. If $\mathcal{U} = \mathcal{U}^\sigma$, then clearly $|\mathcal{U} \cap \mathcal{U}^\sigma| = \frac{1}{2}q$. From elementary linear algebra, we know

$$\dim(\mathcal{U} + \mathcal{U}^\sigma) = \dim(\mathcal{U}) + \dim(\mathcal{U}^\sigma) - \dim(\mathcal{U} \cap \mathcal{U}^\sigma).$$

If $\mathcal{U} \neq \mathcal{U}^\sigma$, then $\mathcal{U}+\mathcal{U}^\sigma = \mathbb{K}$. This implies $\dim(\mathcal{U}\cap\mathcal{U}^\sigma) = n-2$, which means $|\mathcal{U} \cap \mathcal{U}^\sigma| = \frac{1}{4}q$.

From above, we have $\mathcal{U} = \mathcal{U}^\sigma$ if and only if $r = 1$. Since $r = g\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c^2)$, we have that this occurs if and only if $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c^2) = g^{-1}$. We have from Lemma 29 that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}|_{C^\star}$ is 2-to-1, so this equation has a solution for exactly $\frac{1}{2}q$ values of g. In other words, for a fixed $g \in \mathbb{K}^\star$, there are either two values or no values of $c \in C^\star$ such that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(gc^2) = 1$.

First, suppose there does not exist a $c \in C^\star$ such that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(gc^2) = 1$. Then $\mathfrak{X}_r(y^4) =$

$\mathfrak{X}_r(y^2) = 1$ for exactly $\frac{1}{4}q - 1$ values of $y \in \mathbb{K}^\star$ for all $c \in C^\star$, which means

$$\begin{aligned}
\mathsf{W}_g(f) &= q + \sum_{c\in C^\star}\sum_{y\in\mathbb{K}^\star} \mathfrak{X}_r(y^4)\mathfrak{X}_r(y^2) \\
&= q + \sum_{c\in C^\star}\left(\left(\frac{1}{4}q - 1\right)(1)(1) + \frac{1}{4}q(1)(-1) + \frac{1}{4}q(-1)(1) + \frac{1}{4}q(-1)(-1)\right) \\
&= q + \sum_{c\in C^\star}(-1) \\
&= 0.
\end{aligned}$$

Finally, suppose that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(g(c_1)^2) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(g(c_2)^2) = 1$. Then

$$\begin{aligned}
\mathsf{W}_g(f) &= q + \sum_{c\in C^\star}\sum_{y\in\mathbb{K}^\star} \mathfrak{X}_r(y^4)\mathfrak{X}_r(y^2) \\
&= q + 2\left(\left(\frac{1}{2}q - 1\right)(1)(1) + \frac{1}{2}q(-1)(-1)\right) \\
&\quad + \sum_{c\in C^\star\setminus\{c_1,c_2\}}\left(\left(\frac{1}{4}q - 1\right)(1)(1) + \frac{1}{4}q(1)(-1) + \frac{1}{4}q(-1)(1) + \frac{1}{4}q(-1)(-1)\right) \\
&= q + 2q - 2 + \sum_{c\in C^\star\setminus\{c_1,c_2\}}(-1) \\
&= 3q - 2 - (q-2) \\
&= 2q.
\end{aligned}$$

The proof is complete. □

We now partition $\mathbb{K}^\star$ into two sets. Let

$$\begin{aligned}
\mathcal{R} &= \{g \in \mathbb{K}^\star \,:\, \mathsf{W}_g(f) = 0\}, \text{ and} \\
\mathcal{S} &= \{g \in \mathbb{K}^\star \,:\, \mathsf{W}_g(f) = 2q\}.
\end{aligned}$$

With these sets defined, from (5.1) we now have

$$\begin{aligned}
4(v\lambda_w - k^2) &= \sum_{g\in\mathbb{K}^\star} \left|\, \mathsf{W}_g(f) - q - 2 \,\right|^2 \chi_g(g_w C) \\
&= \sum_{g\in\mathcal{R}} |\, 0 - q - 2\,|^2 \chi_g(g_w C) + \sum_{g\in\mathcal{S}} |\, 2q - q - 2\,|^2 \chi_g(g_w C) \\
&= \sum_{g\in\mathcal{R}} (q+2)^2 \chi_g(g_w C) + \sum_{g\in\mathcal{S}} (q-2)^2 \chi_g(g_w C).
\end{aligned}$$

By expanding the squared terms and combining like terms, we obtain

$$\begin{aligned}
4(v\lambda_w - k^2) &= \sum_{g\in\mathcal{R}}(q^2+4q+4)\chi_g(g_wC) + \sum_{g\in\mathcal{S}}(q^2-4q+4)\chi_g(g_wC) \\
&= (q^2+4)\sum_{g\in\mathbb{K}^\star}\chi_g(g_wC) + 4q\left(\sum_{g\in\mathcal{R}}\chi_g(g_wC) - \sum_{g\in\mathcal{S}}\chi_g(g_wC)\right) \\
&= -(q^2+4) + 4q\left(\sum_{g\in\mathcal{R}}\chi_g(g_wC) - \sum_{g\in\mathcal{S}}\chi_g(g_wC)\right),
\end{aligned}$$

where the last step follows from orthogonality. We now rewrite the character sums by letting c range over C to obtain

$$4(v\lambda_w - k^2) = -(q^2+4) + 4q\left(\sum_{g\in\mathcal{R}}\sum_{c\in C}\chi_g(g_wc) - \sum_{g\in\mathcal{S}}\sum_{c\in C}\chi_g(g_wc)\right). \tag{5.2}$$

Motivated by 5.2, we define the following sets:

$$\begin{aligned}
\mathcal{R}_0 &= \{(g,c)\in\mathcal{R}\times C \,:\, \chi_g(g_wc) = 1\}, \\
\mathcal{R}_1 &= \{(g,c)\in\mathcal{R}\times C \,:\, \chi_g(g_wc) = -1\}, \\
\mathcal{S}_0 &= \{(g,c)\in\mathcal{S}\times C \,:\, \chi_g(g_wc) = 1\}, \\
\mathcal{S}_1 &= \{(g,c)\in\mathcal{S}\times C \,:\, \chi_g(g_wc) = -1\},
\end{aligned}$$

and set $r_i = |\mathcal{R}_i|$, $s_i = |\mathcal{S}_i|$, $i = 1, 2$. With these sets and values defined, we now have

$$4(v\lambda_w - k^2) = (q^2+4) + 4q(r_0 - r_1 + s_0 - s_1) \tag{5.3}$$

We now derive relations among the sizes of these four sets. This will allow us to rewrite 5.3 so that fewer quantities must be computed.

Lemma 31. *For the sets defined above, $r_0 + s_0 = \frac{1}{2}q^2 - 1$, and $r_1 + s_1 = \frac{1}{2}q^2$.*

Proof. By the orthogonality relations, $-1 = \sum_{t\in\mathbb{L}^\star}\chi_1(g_wt)$. Since the values of characters of $\mathbb{L}$ are from the set $\{1,-1\}$, this happens if and only if $\chi_1(g_wt) = 1$ for $\frac{1}{2}q^2 - 1$ values of t and $\chi_1(g_wt) = -1$ for $\frac{1}{2}q^2$ values of t. □

This lemma establishes that χ_1 is almost equidistributive on $\mathbb{L}^\star$. This is because $\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}$ is equidistributive on $\mathbb{L}$, which leads to χ_1 being equidistributive on $\mathbb{L}$. The next result follows immediately from the observation that $\mathcal{S}\times C = \mathcal{S}_0 \cup \mathcal{S}_1$.

Lemma 32. *For the sets defined above,* $s_0 + s_1 = \frac{1}{2}q^2 + \frac{1}{2}q$.

In summary, we have the following:

$$\begin{aligned} s_1 &= \frac{1}{2}q^2 + \frac{1}{2}q - s_0, \\ r_0 &= \frac{1}{2}q^2 - 1 - s_0, \\ r_1 &= r_0 - \frac{1}{2}q. \end{aligned}$$

We now make these substitutions in (5.3) and simplify, obtaining

$$v\lambda_w - k^2 + \frac{1}{4}q^2 + 1 = q(q^2 + q - 1 - 4s_0). \tag{5.4}$$

Therefore, we only have to compute s_0.

Recall that for all $x \in \mathbb{L}$, $\chi_1(x) = (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(x)}$. Thus, $\chi_1(g_w c) = 1$ if and only if $\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(g_w c) = 0$. Since $\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}$ is a nonzero $\mathbb{F}$-linear transformation, its kernel is a proper subgroup of $\mathbb{L}$. Let $\mathcal{H}_2 = \{x \in \mathbb{L} : \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(x) = 0\}$ be this kernel. Then as additive groups, $|\mathbb{L} : \mathcal{H}_2| = 2$.

Lemma 33. *As additive groups,* $\mathbb{K} \leq \mathcal{H}_2$, *and* $|\mathcal{H}_2 : \mathbb{K}| = \frac{1}{2}q$.

Proof. Suppose $x \in \mathbb{K}$. Then $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = x + x^q = x + x = 0$. The transitivity of trace now yields

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(x) = \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x)) = \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(0) = 0.$$

Therefore, $x \in \mathcal{H}_2$, and the proof is complete. □

We now partition $\mathcal{H}_2$ into cosets of $\mathbb{K}$. Let $\{t_1, t_2, \ldots, t_{q/2}\}$ be a transversal of $\mathbb{K}$ in $\mathcal{H}_2$. That is, choose $t_1, t_2, \ldots, t_{q/2}$ such that

$$\mathcal{H}_2 = \bigcup_{i=1}^{q/2} (\mathbb{K} + t_i).$$

One more lemma is required for us to determine s_0.

Lemma 34. *Let* $g \in \mathbb{K}$. *Then there exists* $i \in \mathbb{N}$ *with* $i \leq \frac{q}{2}$ *such that* $g = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t_i)$ *if and only if* $g \in \mathcal{H}_1$.

Proof. Note that if $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t_i) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t_j)$, then by the $\mathbb{K}$-linearity of $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$, we have $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t_i - t_j) = 0$. This means that $t_i - t_j \in \mathbb{K}$, implying $\mathbb{K} + t_i = \mathbb{K} + t_j$. We conclude $t_i = t_j$. This means that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t_i)$ attains $\frac{q}{2}$ different values as i ranges from 1 to $\frac{q}{2}$.

We now compute $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t_i))$. By the transitivity of trace, $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t_i)) = \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(t_i)$. But by definition, $\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(t_i) = 0$. Since $|\mathcal{H}_1| = \frac{q}{2}$, we conclude that

$$\mathcal{H}_1 = \left\{ \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t_i) \,:\, i = 1, \ldots, \frac{q}{2} \right\}.$$

From this, the statement is clear. □

With this lemma established, we may finally compute s_0.

Theorem 35. *With s_0 defined as above,*

$$s_0 = \begin{cases} \frac{1}{4}q^2 + \frac{1}{2}q & \text{if } w \in \mathcal{D}, \\ \frac{1}{4}q^2 & \text{if } w \notin \mathcal{D}. \end{cases}$$

Proof. An element $g \in \mathbb{K}^\star$ satisfies $g \in \mathcal{S}$ if and only if $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(gu) = 1$ for some $u \in C$. So $(g, c) \in \mathcal{S}_0$ if and only if $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(gu) = 1$ for some $u \in C$ and $\chi_1(gg_w c) = 1$, i.e. $gg_w c \in \mathcal{H}_2$, which is to say $gg_w c = m + t_l$ for some $m \in \mathbb{K}$ and some $1 \le l \le \frac{1}{2}q$. By rearranging terms, we deduce $(g, c) \in \mathcal{S}_0$ if and only if $g = (m + t_l)(g_w c)^{-1}$ and $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(gu) = 1$ for some $u \in C$. By substitution, we obtain

$$1 = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}\left(\frac{(m + t_l)u}{g_w c} \right). \tag{5.5}$$

Let $y = uc^{-1}$. Then (5.5) becomes

$$1 = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}\left(\frac{m + t_l}{g_w} y \right).$$

For fixed t_l and $y \neq 1$, we may solve uniquely for m, and the pair (g, c). Moreover, $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(gcy) = 1$, so that $(g, c) \in \mathcal{S}_0$. However, by Lemma 29, two distinct choices of y must produce the same pair (g, c). As y has q possible values and there are $\frac{1}{2}q$ choices for t_l, with the double counting involved, we obtain $\frac{1}{4}q^2$ different elements of $\mathcal{S}_0$.

What remains to be considered is the case $y = 1$. In this case (5.5) becomes

$$g_w = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t_l). \tag{5.6}$$

This relates to Lemma 34, and as we now show is dependent on w's membership in $\mathcal{D}$. Suppose $w \in \mathcal{D}$, so that $w = f(x)$ for some x. We thus have $f(x) = g_w c_w$. Note that $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(w) = g_w$. We have

$$\begin{aligned} g_w = \mathrm{N}_{\mathbb{L}/\mathbb{K}}(w) &= \mathrm{N}_{\mathbb{L}/\mathbb{K}}(f(x)) \\ &= \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x^2(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + 1)) \\ &= \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)^2 \, \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + 1) \\ &= \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)^2(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + 1)^2 \\ &= \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)^2(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)^2 + 1) \\ &= \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)^4 - \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)^2 \in \mathcal{H}_1. \end{aligned}$$

Thus this final case hinges on whether or not $w \in \mathcal{D}$.

There is at most one value of l that satisfies (5.6), for suppose $g_w = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t_l) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t_j)$. Then $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t_l - t_j) = 0$, so $t_l - t_j \in \mathbb{K}$, and as t_l and t_j are coset representatives, we conclude $t_l = t_j$. Clearly, if $w \notin \mathcal{D}$, $\mathcal{S}_0$ contains no further elements. If $w \in \mathcal{D}$, then we must have a unique choice of t_l. Fix a $g \in \mathcal{S}$. Then for $(g, c) \in \mathcal{S}_0$, $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(gc) = 1$ is now forced. By Lemma 29, an additional choice $u \in C$ for which $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(gu) = 1$ also exists. However, this second choice would not satisfy the $y = 1$ hypothesis, so the pair $(g, c) \in \mathcal{S}_0$ is uniquely determined by the choice of $g \in \mathcal{S}$. Hence, for $w \in \mathcal{D}$, there are an additional $|\mathcal{S}| = \frac{1}{2}q$ elements of $\mathcal{S}_0$, and we are done. □

With s_0 determined, we may finally compute the values of λ_w, and complete the proof of Theorem 26. For ease of notation, let $\epsilon = \frac{1}{2}q$ if $w \in \mathcal{D}$ and 0 otherwise. Then we may write $s_0 = \frac{1}{4}q^2 + \epsilon$ and the equation (5.4) becomes

$$\begin{aligned} v\lambda_w - k^2 + \frac{1}{4}q^2 + 1 &= q(q^2 + q - 1 - 4s_0) \\ &= q\left(q^2 + q - 1 - 4\left(\frac{1}{4}q^2 + \epsilon\right)\right) \\ &= q(q - 1 - 4\epsilon) \\ &= q^2 - q - 4q\epsilon. \end{aligned}$$

We now make the substitutions $v = q^2$ and $k = \frac{1}{2}(q-2)(q+1)$ in order to rewrite the left-hand side:

$$\begin{aligned} v\lambda_w - k^2 + \frac{1}{4}q^2 + 1 &= q^2\lambda_w - \left(\frac{1}{2}(q-2)(q+1)\right)^2 + \frac{1}{4}q^2 + 1 \\ &= q^2\lambda_w - \left(\frac{1}{4}q^4 - \frac{1}{2}q^3 - \frac{3}{4}q^2 + q + 1\right) + \frac{1}{4}q^2 + 1 \\ &= q^2\lambda_w - \frac{1}{4}q^4 + \frac{1}{2}q^3 + q^2 - q. \end{aligned}$$

Combining these results and solving for λ_w yields the equation

$$\begin{aligned} q^2\lambda_w - \frac{1}{4}q^4 + \frac{1}{2}q^3 + q^2 - q &= q^2 - q - 4q\epsilon \\ \Leftrightarrow q^2\lambda_w &= \frac{1}{4}q^4 - \frac{1}{2}q^3 - 4q\epsilon \\ \Leftrightarrow \lambda_w &= \frac{1}{4}q^2 - \frac{1}{2}q - \frac{4}{q}\epsilon. \end{aligned}$$

Substituting the appropriate value of ϵ now produces

$$\lambda_w = \begin{cases} \frac{1}{4}q^2 - \frac{1}{2}q - 2 & \text{if } w \in \mathcal{D}, \\ \frac{1}{4}q^2 - \frac{1}{2}q & \text{if } w \notin \mathcal{D}. \end{cases}$$

These are the claimed parameters, and Theorem 26 is established.

Chapter 6

CLASS II

6.1 Class II

We now use the same construction scheme with a different polynomial. After the biregularity of the new polynomial is established, this proof is vastly different from the proof of Theorem 26.

Theorem 36. *Let $p = 2$ and $q = p^n$ with $n \in \mathbb{N}$. Set $a = q - 1$ and $b = q + 1$. Let $\mathbb{K} = \mathbb{F}_q$ and $\mathbb{L} = \mathbb{F}_{q^2}$. Define $f \in \mathbb{L}[X]$ by $f(X) = X^b + X$. Then $f(X)$ is $(2, 1)$-biregular. More specifically, for all $y \in \mathbb{L}$, $\left|f^{-1}(y)\right| = 0$ or 2 if $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(y) \neq 1$, and $\left|f^{-1}(y)\right| = 1$ if $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(y) = 1$.*

Proof. We note that for all $x \in \mathbb{L}$, $f(x) = \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + x$. Suppose $f(x) = f(y)$. This means that

$$y + x = \mathrm{N}_{\mathbb{L}/\mathbb{K}}(y) + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x).$$

Since $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(y) + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) \in \mathbb{K}$, we have that $y + x \in \mathbb{K}$. Let $y + x = w \in \mathbb{K}$ so that $y = x + w$. We now have the equation

$$w = \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x + w) + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x).$$

We now compute $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x + w)$:

$$\begin{aligned}
\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x + w) &= (x + w)(x + w)^q \\
&= (x + w)(x^q + w) \\
&= x^{q+1} + wx + wx^q + w^2 \\
&= \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + w\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) + w^2.
\end{aligned}$$

Substituting this back into the original equation gives us

$$\begin{aligned}
w &= \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) + w\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) + w^2 + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) \\
&= w\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) + w^2,
\end{aligned}$$

so that $w^2 + (\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) + 1)w = w(w + 1 + \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x)) = 0$. Hence $w = 0$ or $w = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) + 1$. Since $y = x + w$, this means that $y = x$ or $y = x + \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) + 1$. These possibilities are distinct unless $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = 1$. In other words, the two possible values of y are distinct unless $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = 1$. □

As in Class I, let $p = 2$, $e = 2n$ with $n \in \mathbb{N}$. Let $q = p^n$, so that $\mathbb{L} = \mathbb{F}_{q^2}$. Let $a = q - 1$, so that $b = q + 1$. We again define the intermediate fields $\mathbb{K} = \mathbb{F}_q$ and $\mathbb{F} = \mathbb{F}_2$. Also, let $\mathbf{s} \in \mathbb{L}$ be a fixed element such that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathbf{s}) = 1$. This means that $\{1, \mathbf{s}\}$ forms a $\mathbb{K}$-basis for $\mathbb{L}$.

Let $f \in \mathbb{L}[X]$ with $f(X) = X^b + X$, and set $\mathcal{D} = \mathrm{Im}(f) \setminus \{0\}$. As shown in Theorem 36, this polynomial is $(2, 1)$-biregular. Because of this, we have the following variant of (4.5) to deal with:

$$\mathsf{W}_t(f) = 2\chi_t(\mathcal{D}) - \chi_t(\mathbb{K} + \mathbf{s}) + 2. \tag{6.1}$$

Solving for $\chi_t(\mathcal{D})$ yields

$$\chi_t(\mathcal{D}) = \frac{1}{2}\left(\mathsf{W}_t(f) + \chi_t(\mathbb{K} + \mathbf{s}) - 2\right).$$

Our version of (4.1) is

$$\begin{aligned} v\lambda_w - k^2 &= \sum_{t \in \mathbb{L}^\star} |\chi_t(\mathcal{D})|^2 \chi_t(w) \\ &= \sum_{t \in \mathbb{L}^\star} \left| \frac{1}{2}\left(\mathsf{W}_t(f) + \chi_t(\mathbb{K} + \mathbf{s}) - 2\right) \right|^2 \chi_t(w) \\ &= \frac{1}{4} \sum_{t \in \mathbb{L}^\star} |\mathsf{W}_t(f) + \chi_t(\mathbb{K} + \mathbf{s}) - 2|^2 \chi_t(w). \end{aligned} \tag{6.2}$$

We now evaluate $\chi_t(\mathbb{K} + \mathbf{s})$.

Theorem 37. *With the notation above,*

$$\chi_t(\mathbb{K} + \boldsymbol{s}) = \begin{cases} q\,\chi_t(\boldsymbol{s}) & \text{if } t \in \mathbb{K}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By definition,

$$\chi_t(\mathbb{K} + \mathbf{s}) = \sum_{x \in \mathbb{K}} \chi_t(x + \mathbf{s}).$$

Since χ_t is an additive character, we obtain

$$\begin{aligned}\sum_{x\in\mathbb{K}}\chi_t(x+\mathbf{s}) &= \sum_{x\in\mathbb{K}}\chi_t(x)\chi_t(\mathbf{s})\\ &= \chi_t(\mathbf{s})\sum_{x\in\mathbb{K}}\chi_t(x).\end{aligned}$$

As in Class I, we can restrict the character χ_t to $\mathbb{K}$ to obtain the character $\mathfrak{X}_r$ in $\widehat{\mathbb{K}}$, where $r = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t)$. Using this restriction gives us

$$\begin{aligned}\chi_t(\mathbf{s})\sum_{x\in\mathbb{K}}\chi_t(x) &= \chi_t(\mathbf{s})\sum_{x\in\mathbb{K}}\mathfrak{X}_r(x)\\ &= \chi_t(\mathbf{s})\,\mathfrak{X}_r(\mathbb{K}).\end{aligned}$$

From the orthogonality relations we know that

$$\mathfrak{X}_r(\mathbb{K}) = \begin{cases} q & \text{if } r = 0,\\ 0 & \text{otherwise.}\end{cases}$$

We also know that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t) = 0$ if and only if $t \in \mathbb{K}$, and this establishes the statement. □

This equality will be useful in partitioning the equation for λ_w into smaller, more manageable parts.

We now rewrite f in terms of linearized polynomials. If we let $x = u + v\mathbf{s}$ with $u, v \in \mathbb{K}$, then we can express $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)$ in terms of u, v, and $\mathbf{s}$:

$$\begin{aligned}\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) &= \mathrm{N}_{\mathbb{L}/\mathbb{K}}(u+v\mathbf{s})\\ &= (u+v\mathbf{s})(u+v\mathbf{s})^q\\ &= (u+v\mathbf{s})(u+v\mathbf{s}^q)\\ &= u^2 + uv\mathbf{s} + uv\mathbf{s}^q + v^2\mathbf{s}^{q+1}.\end{aligned}$$

By definition, $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s}) = \mathbf{s}^{q+1}$, and $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathbf{s}) = \mathbf{s} + \mathbf{s}^q = 1$. We therefore have

$$\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) = u^2 + uv + v^2\,\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s}).$$

By calculating $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(u + v\mathbf{s})$, we may now rewrite $f(x)$ in terms of u, v, and $\mathbf{s}$:

$$\begin{aligned} f(x) &= f(u + v\mathbf{s}) \\ &= \mathrm{N}_{\mathbb{L}/\mathbb{K}}(u + v\mathbf{s}) + (u + v\mathbf{s}) \\ &= u^2 + uv + v^2\,\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s}) + u + v\mathbf{s} \\ &= \left(u^2 + (v+1)u\right) + \left(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s})v^2 + v\mathbf{s}\right). \end{aligned}$$

For the degree 2 extension $\mathbb{L}/\mathbb{K}$, $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)$ can be rewritten in terms of $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x)$ in a convenient way. Indeed, for all $x \in \mathbb{L}$, we have

$$x\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = x^2 + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x).$$

This means that

$$\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s}) = \mathbf{s}\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathbf{s}) - \mathbf{s}^2 = \mathbf{s} - \mathbf{s}^2,$$

and substituting this into the equation for $f(x)$ gives us

$$f(x) = \left(u^2 + (v+1)u\right) + \left((\mathbf{s}^2 + \mathbf{s})v^2 + v\mathbf{s}\right).$$

Set $\hbar(X) = (\mathbf{s}^2 + \mathbf{s})X^2 + \mathbf{s}X \in \mathbb{L}[X]$.

Lemma 38. *With $\hbar$ defined as above, $\hbar$ is a 2-polynomial. Let $\phi : \mathbb{L} \to \mathbb{L}$ be the evaluation map of $\hbar$ on $\mathbb{L}$. Then $\phi|_{\mathbb{K}}$ is a group homomorphism from $\mathbb{K}$ into $\mathbb{L}$. Moreover, $|\ker(\phi)| = 2$, and $|\ker(\phi|_{\mathbb{K}})| = 1$.*

Proof. That $\hbar$ is a 2-polynomial is clear, and this is equivalent to ϕ being a group homomorphism on $\mathbb{L}$, which implies the claim regarding the restriction of ϕ to $\mathbb{K}$.

Factoring $\hbar$ shows $\ker(\phi) = \{0, (1 + \mathbf{s})^{-1}\}$, and since $1 + \mathbf{s} \in \mathbb{L} \setminus \mathbb{K}$, the remaining claims are established. □

Now

$$f(u + v\mathbf{s}) = \left(u^2 + (v+1)u\right) + \hbar(v).$$

Note that the first part of $f(u + v\mathbf{s})$, that is, $u^2 + (v + 1)u$, is a 2-polynomial in u for all fixed $v \in \mathbb{K}$. We now use this rewritten form of $f(x)$ to evaluate $\mathbb{W}_t(f)$. By letting $x = u + v\mathbf{s}$ with $u, v \in \mathbb{K}$, we may write

$$\begin{aligned}
\mathbb{W}_t(f) &= \sum_{x\in\mathbb{L}} \chi_t(f(x)) \\
&= \sum_{u\in\mathbb{K}} \sum_{v\in\mathbb{K}} \chi_t(f(u + v\mathbf{s})) \\
&= \sum_{u\in\mathbb{K}} \sum_{v\in\mathbb{K}} \chi_t\left(\left(u^2 + (v + 1)u\right) + h(v)\right) \\
&= \sum_{u\in\mathbb{K}} \sum_{v\in\mathbb{K}} \chi_t\left(u^2 + (v + 1)u\right)\chi_t\left(h(v)\right) \\
&= \sum_{v\in\mathbb{K}} \chi_t\left(h(v)\right) \sum_{u\in\mathbb{K}} \chi_t\left(u^2 + (v + 1)u\right).
\end{aligned}$$

We now evaluate the inner sum. Since the mapping $u \mapsto u^2 + (v + 1)u$ is a group homomorphism defined on $\mathbb{K}$, its image is an $\mathbb{F}$-subspace of $\mathbb{K}$. This also means that the image is a subgroup of the additive group of $\mathbb{K}$. Let $\mathcal{H}_v$ denote this group. In order to compute $|\mathcal{H}_v|$, we compute the order of this mapping's kernel, which is straightforward. We have

$$|\mathbb{K} : \mathcal{H}_v| = \begin{cases} 1 & \text{if } v = 1, \\ 2 & \text{otherwise.} \end{cases}$$

Note that $\mathcal{H}_1 = \mathbb{K}$. By restricting the character χ_t to $\mathbb{K}$, we obtain a character of $\mathbb{K}$, which we'll denote $\mathfrak{X}_r$, where $r = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t)$. We thus have

$$\sum_{u\in\mathbb{K}} \chi_t\left(u^2 + (v + 1)u\right) = \sum_{u\in\mathbb{K}} \mathfrak{X}_r\left(u^2 + (v + 1)u\right).$$

Lemma 39. *With the notation above,*

$$\sum_{u\in\mathbb{K}} \chi_t\left(u^2 + (v + 1)u\right) = \begin{cases} 2\chi_t(\mathcal{H}_v) & \text{if } v \neq 1, \\ \chi_t(\mathbb{K}) & \text{if } v = 1. \end{cases}$$

Proof. Note that as u ranges over $\mathbb{K}$, the expression $u^2 + (v + 1)u$ ranges over $\mathcal{H}_v$ twice except for when $v = 1$. □

We next prove that distinct values of v give rise to distinct subgroups $\mathcal{H}_v$.

Lemma 40. *Let $v, w \in \mathbb{K}$. Then $\mathcal{H}_v = \mathcal{H}_w$ if and only if $v = w$.*

Proof. Suppose $\mathcal{H}_v = \mathcal{H}_w$. Note that since $|\mathcal{H}_v| = q$ if and only if $v = 1$, we may assume that $v \neq 1$ and $w \neq 1$. By the way in which $\mathcal{H}_v$ and $\mathcal{H}_w$ were defined, we have that for all $y \in \mathbb{K}$, $y^2 + (v+1)y \in \mathcal{H}_v$ and $y^2 + (w+1)y \in \mathcal{H}_w$. Since $\mathcal{H}_v = \mathcal{H}_w$, we also have that $y^2 + (w+1)y \in \mathcal{H}_v$. Since $\mathcal{H}_v$ is a subgroup of $\mathbb{K}$, we have that

$$\left(y^2 + (v+1)y\right) - \left(y^2 + (w+1)y\right) \in \mathcal{H}_v,$$

so that $(v+w)y \in \mathcal{H}_v$. This holds for all $y \in \mathbb{K}$. If $v \neq w$, then this would imply $\mathbb{K} \leq \mathcal{H}_v$, a contradiction. Therefore, the proof is complete. □

Recall that every index 2 subgroup of $\mathbb{K}$ is the kernel of a unique character in $\widehat{\mathbb{K}}$. By the previous lemma, the set of index 2 subgroups of $\mathbb{K}$ is precisely $\{\mathcal{H}_v : (v \in \mathbb{K}) \wedge (v \neq 1)\}$. Thus, for all $r \in \mathbb{K}^\star$, there exists a unique $v_r \in \mathbb{K}$ such that

$$\sum_{u \in \mathbb{K}} \mathfrak{X}_r\left(u^2 + (v+1)u\right) = \begin{cases} q & \text{if } v = v_r, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\mathcal{H} = \hbar(\mathbb{K})$. Then we have the following theorem.

Theorem 41. *With $\mathsf{W}_t(f)$ defined as above,*

$$\mathsf{W}_t(f) = \begin{cases} q\chi_t(\mathcal{H}) & \text{if } t \in \mathbb{K}, \\ q\chi_t\left(\hbar(v_r)\right) & \text{otherwise.} \end{cases}$$

Proof. From before,

$$\mathsf{W}_t(f) = \sum_{v \in \mathbb{K}} \left(\chi_t(\hbar(v)) \sum_{u \in \mathbb{K}} \mathfrak{X}_r\left(u^2 + (v+1)u\right) \right).$$

We now consider two cases. First, suppose $t \in \mathbb{K}$. Then $r = 0$, and by the orthogonality of characters, the innermost sum is q. This means

$$\begin{aligned} \mathsf{W}_t(f) &= \sum_{v \in \mathbb{K}} q\chi_t(\hbar(v)) \\ &= q\chi_t(\mathcal{H}). \end{aligned}$$

Now, suppose $t \notin \mathbb{K}$. Then $r \neq 0$, but there exists a unique $v_r \in \mathbb{K}$ such that $\ker(\mathfrak{X}_r) = \mathcal{H}_{v_r}$. Therefore, the innermost sum is 0 unless $v = v_r$, in which case the innermost sum is q. Therefore, $\mathbb{W}_t(f) = q\chi_t(\hbar(v_r))$ in this case. □

With $\mathbb{W}_t(f)$ rewritten, we return to (6.2) and obtain

$$4(v\lambda_w - k^2) = \sum_{t \in \mathbb{K}^\star} \left(q\chi_t(\mathcal{H}) + q\chi_t(v) - 2\right)^2 \chi_t(w) + \sum_{t \in \mathbb{L} \setminus \mathbb{K}} \left(q\chi_t(\hbar(v_r)) - 2\right)^2 \chi_t(w). \tag{6.3}$$

We now require a lemma relating $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ and $\hbar(x)$.

Lemma 42. *For all $v \in \mathbb{K}$, we have $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\hbar(v)) = v$.*

Proof. Note that $\hbar(v) = (\mathbf{s}^2 + \mathbf{s})v^2 + v\mathbf{s}$. By using the $\mathbb{K}$-linearity of $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$, we obtain

$$\begin{aligned}\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\hbar(v)) &= \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}\left((\mathbf{s}^2 + \mathbf{s})v^2 + v\mathbf{s}\right) \\ &= v^2\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathbf{s}^2) + \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathbf{s})\right) + v\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathbf{s}).\end{aligned}$$

Recall that $\mathbf{s} \in \mathbb{L}$ was chosen such that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathbf{s}) = 1$. Also note that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(u^2) = \left(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(u)\right)^2$ for all $u \in \mathbb{L}$. From this we conclude

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\hbar(v)) = v^2\left(1^2 + 1\right) + (1)v = v.$$

□

This lemma is useful in computing $\chi_t(\hbar(v))$ when $t \in \mathbb{K}$.

Lemma 43. *If $t \in \mathbb{K}$, then $\chi_t(\hbar(v)) = \mathfrak{X}_t(v)$.*

Proof. Let $\mathfrak{w} = -1$, the primitive second root of unity. By definition,

$$\chi_t(\hbar(v)) = \mathfrak{w}^{\exp\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(t\hbar(v))\right)}.$$

We now use transitivity of trace and the $\mathbb{K}$-linearity of $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ to obtain

$$\begin{aligned}\chi_t(\hbar(v)) &= \mathfrak{w}^{\exp\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(t\hbar(v))\right)\right)} \\ &= \mathfrak{w}^{\exp\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}\left(t\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\hbar(v))\right)\right)}.\end{aligned}$$

By the last lemma, we have

$$\chi_t\left(\hbar(v)\right) = \mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(tv)\right).$$

By definition, the right-hand side is $\mathfrak{X}_t(v)$. Therefore we have

$$\chi_t\left(\hbar(v)\right) = \mathfrak{X}_t(v).$$

□

We may now compute $\chi_t(\mathcal{H})$. By definition, we have

$$\chi_t(\mathcal{H}) = \sum_{v\in\mathbb{K}} \chi_t\left(\hbar(v)\right),$$

and by the last lemma

$$\chi_t(\mathcal{H}) = \sum_{v\in\mathbb{K}} \mathfrak{X}_t(v).$$

The orthogonality relations now show

Lemma 44. *Let $t \in \mathbb{K}$. Then*

$$\chi_t(\mathcal{H}) = \begin{cases} q & \text{if } t = 0, \\ 0 & \text{otherwise.} \end{cases}$$

With these character sums computed, we may again rewrite the equation for λ_w, last given in (6.3). First, note that $\chi_t(\mathcal{H}) = 0$ for all $t \in \mathbb{K}^\star$. Hence

$$\begin{aligned} 4(v\lambda_w - k^2) &= \sum_{t\in\mathbb{K}^\star} \left(q\chi_t(\mathcal{H}) + q\chi_t(v) - 2\right)^2 \chi_t(w) + \sum_{t\in\mathbb{L}\setminus\mathbb{K}} \left(q\chi_t\left(\hbar(v_r)\right) - 2\right)^2 \chi_t(w) \\ &= \sum_{t\in\mathbb{K}^\star} \left(q\chi_t(\mathbf{s}) - 2\right)^2 \chi_t(w) + \sum_{t\in\mathbb{L}\setminus\mathbb{K}} \left(q\chi_t\left(\hbar(v_r)\right) - 2\right)^2 \chi_t(w). \end{aligned}$$

We now expand the squared terms to obtain

$$\begin{aligned} 4(v\lambda_w - k^2) = &\sum_{t\in\mathbb{K}^\star} \left(q^2\left(\chi_t(\mathbf{s})\right)^2 - 4q\chi_t(\mathbf{s}) + 4\right)\chi_t(w) \\ &+ \sum_{t\in\mathbb{L}\setminus\mathbb{K}} \left(q^2\left(\chi_t\left(\hbar(v_r)\right)\right)^2 - 4q\chi_t\left(\hbar(v_r)\right) + 4\right)\chi_t(w). \end{aligned}$$

Note that $\chi_t(x) = \pm 1$ for all $x \in \mathbb{L}$, and so $\chi_t(x)^2 = 1$ for all $x \in \mathbb{L}$. Using this fact, we can simplify the above to obtain

$$4(v\lambda_w - k^2) = \sum_{t\in\mathbb{K}^\star} \left(q^2 - 4q\chi_t(\mathbf{s}) + 4\right)\chi_t(w) + \sum_{t\in\mathbb{L}\setminus\mathbb{K}} \left(q^2 - 4q\chi_t\left(\hbar(v_r)\right) + 4\right)\chi_t(w).$$

We now rearrange and combine like terms:

$$\begin{aligned} 4(v\lambda_w - k^2) &= (q^2+4)\sum_{t\in\mathbb{K}^\star}\chi_t(w) - 4q\sum_{t\in\mathbb{K}^\star}\chi_t(\mathbf{s})\chi_t(w) \\ &\quad + (q^2+4)\sum_{t\in\mathbb{L}\setminus\mathbb{K}}\chi_t(w) - 4q\sum_{t\in\mathbb{L}\setminus\mathbb{K}}\chi_t\left(\hbar(v_r)\right)\chi_t(w) \\ &= (q^2+4)\sum_{t\in\mathbb{L}^\star}\chi_t(w) - 4q\left(\sum_{t\in\mathbb{K}^\star}\chi_t(\mathbf{s}+w) + \sum_{t\in\mathbb{L}\setminus\mathbb{K}}\chi_t\left(\hbar(v_r)+w\right)\right). \end{aligned}$$

From the orthogonality relations, we know $\sum_{t\in\mathbb{L}^\star}\chi_t(w) = -1$. Thus, we arrive at

$$4(v\lambda_w - k^2) = -(q^2+4) - 4q\left(\sum_{t\in\mathbb{K}^\star}\chi_t(\mathbf{s}+w) + \sum_{t\in\mathbb{L}\setminus\mathbb{K}}\chi_t\left(\hbar(v_r)+w\right)\right). \tag{6.4}$$

We next evaluate the two character sums in this equation.

Lemma 45. *With the notation above,*

$$\sum_{t\in\mathbb{K}^\star}\chi_t(\boldsymbol{s}+w) = \begin{cases} q-1 & \textit{if } \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) = 1, \\ -1 & \textit{otherwise.} \end{cases}$$

Proof. We first rewrite $\chi_t(\mathbf{s}+w)$ as $\chi_{\mathbf{s}+w}(t)$. Since t ranges through $\mathbb{K}^\star$, we restrict the character $\chi_{\mathbf{s}+w}$ to obtain the character $\mathfrak{X}_z \in \widehat{\mathbb{K}}$, where $z = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathbf{s}+w)$. The character sum now becomes

$$\sum_{t\in\mathbb{K}^\star}\chi_t(\mathbf{s}+w) = \sum_{t\in\mathbb{K}^\star}\mathfrak{X}_z(t).$$

By the orthogonality relations we obtain

$$\sum_{t\in\mathbb{K}^\star}\mathfrak{X}_z(t) = \begin{cases} q-1 & \text{if } z = 0, \\ -1 & \text{if } z \neq 0. \end{cases} \tag{6.5}$$

Note that $z = 0$ if and only if $\mathbf{s}+w \in \mathbb{K}$. This occurs if and only if $w \in \mathbb{K}+\mathbf{s}$. But $\mathbb{K}+\mathbf{s} = \{x \in \mathbb{L} : \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = 1\}$, which establishes the result. □

Moving to the second sum, we first write t as $t = c + d\mathbf{s}$ with $c, d \in \mathbb{K}$, $d \neq 0$, and letting c and d range. Note that under this substitution, $r = d$. We have

$$\begin{aligned}\sum_{t\in\mathbb{L}\setminus\mathbb{K}} \chi_t\left(\hbar(v_r) + w\right) &= \sum_{d\in\mathbb{K}^\star}\left(\sum_{c\in\mathbb{K}} \chi_{c+d\mathbf{s}}\left(\hbar(v_r) + w\right)\right) \\ &= \sum_{d\in\mathbb{K}^\star}\left(\sum_{c\in\mathbb{K}} \chi_c\left(\hbar(v_d) + w\right)\chi_{d\mathbf{s}}\left(\hbar(v_d) + w\right)\right).\end{aligned}$$

Since the second character in the above product is independent of c, we may factor it out, resulting in

$$\sum_{t\in\mathbb{L}\setminus\mathbb{K}} \chi_t\left(\hbar(v_d) + w\right) = \sum_{d\in\mathbb{K}^\star}\left(\chi_{d\mathbf{s}}\left(\hbar(v_d) + w\right)\sum_{c\in\mathbb{K}} \chi_c\left(\hbar(v_d) + w\right)\right). \tag{6.6}$$

We now compute the innermost character sum.

Lemma 46. *With the notation above,*

$$\sum_{c\in\mathbb{K}} \chi_c\left(\hbar(v_d) + w\right) = \begin{cases} q & \text{if } \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) = v_d, \\ 0 & \text{otherwise.}\end{cases}$$

Proof. Note that $\chi_c\left(\hbar(v_d) + w\right) = \chi_{\hbar(v_d)+w}(c)$. By using this and restricting the resulting character $\mathfrak{X}_j$ to $\mathbb{K}$, with $j = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\hbar(v_d) + w)$, we obtain

$$\begin{aligned}\sum_{c\in\mathbb{K}} \chi_c\left(\hbar(v_d) + w\right) &= \sum_{c\in\mathbb{K}} \chi_{\hbar(v_d)+w}(c) \\ &= \sum_{c\in\mathbb{K}} \mathfrak{X}_j(c) \\ &= \begin{cases} q & \text{if } j = 0, \\ 0 & \text{otherwise.}\end{cases}\end{aligned}$$

We have that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}\left(\hbar(v_d)\right) = v_d$, and so

$$\begin{aligned}\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}\left(\hbar(v_d) + w\right) &= \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}\left(\hbar(v_d)\right) + \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) \\ &= v_d + \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w).\end{aligned}$$

This means $j = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}\left(\hbar(v_d) + w\right) = 0$ if and only if $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) = v_d$. □

Since $v_d \neq 0$ for any d, we have that if $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) = 1$, then

$$\sum_{t \in \mathbb{L}\setminus\mathbb{K}} \chi_t\left(\hbar(v_r) + w\right) = 0.$$

At this point, we may compute λ_w in the case where $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) = 1$. Note that we have $v = q^2$ and $k = \frac{1}{2}(q-1)(q+2)$, so that

$$\begin{aligned} 4v\left(\lambda_w - k^2\right) &= 4q^2\lambda_w - 4\left(\frac{1}{2}(q-1)(q+2)\right)^2 \\ &= 4q^2\lambda_w - (q^4 + 2q^3 - 3q^2 - 4q + 4) \end{aligned}$$

Therefore, when $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) = 1$, we obtain from (6.4), (6.6) and the above calculations the identity

$$\begin{aligned} 4q^2\lambda_w - (q^4 + 2q^3 - 3q^2 - 4q + 4) &= -(q^2+4) - 4q\left(\sum_{t \in \mathbb{K}^\star} \chi_t(\mathbf{s} + w) + \sum_{t \in \mathbb{L}\setminus\mathbb{K}} \chi_t\left(\hbar(v_r) + w\right)\right) \\ &= -(q^2+4) - 4q(q - 1 + 0) \\ &= -5q^2 + 4q - 4. \end{aligned}$$

From here, we solve for λ_w to obtain

$$\lambda_w = \frac{1}{4}q^2 + \frac{1}{2}q - 2. \tag{6.7}$$

It remains to deal with the case where $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) \neq 1$. If $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) \neq 1$, then there exists a unique $d \in \mathbb{K}$ such that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) = v_d$. For this unique d, we have

$$\begin{aligned} \sum_{t \in \mathbb{L}\setminus\mathbb{K}} \chi_t\left(\hbar(v_d) + w\right) &= \sum_{d \in \mathbb{K}^\star}\left(\chi_{d\mathbf{s}}\left(\hbar(v_d) + w\right) \sum_{c \in \mathbb{K}} \chi_c\left(\hbar(v_d) + w\right)\right) \\ &= q \sum_{d \in \mathbb{K}^\star} \chi_{d\mathbf{s}}\left(\hbar(v_d) + w\right). \end{aligned}$$

We now compute this character sum.

Lemma 47. *With the notation above,*

$$\sum_{t \in \mathbb{L}\setminus\mathbb{K}} \chi_t\left(\hbar(v_d) + w\right) = q\,\mathfrak{X}_d\left(\hbar(v_d) + w\right).$$

Proof. We first apply the definition of a character to $\chi_{d\mathbf{s}}(\hbar(v_d)+w)$ to obtain

$$\chi_{d\mathbf{s}}(\hbar(v_d)+w) = \mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(d\mathbf{s}(\hbar(v_d)+w))\right).$$

By using transitivity of trace, this becomes

$$\chi_{d\mathbf{s}}(\hbar(v_d)+w) = \mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(d\mathbf{s}(\hbar(v_d)+w)))\right).$$

By the $\mathbb{K}$-linearity of $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$, and since $\hbar(v_d)+w \in \mathbb{K}$ we obtain

$$\begin{aligned}\chi_{d\mathbf{s}}(\hbar(v_d)+w) &= \mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(d(\hbar(v_d)+w)\,\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathbf{s}))\right)\\ &= \mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(d(\hbar(v_d)+w))\right).\end{aligned}$$

The above quantity can now be viewed as a character of $\mathbb{K}$. By definition,

$$\mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(d(\hbar(v_d)+w))\right) = \mathfrak{X}_d(\hbar(v_d)+w).$$

Therefore, we finally obtain

$$\sum_{t\in\mathbb{L}\setminus\mathbb{K}} \chi_t(\hbar(v_d)+w) = q\,\mathfrak{X}_d(\hbar(v_d)+w).$$

□

We have one more character to evaluate after we simplify:

$$\begin{aligned}4q^2\lambda_w - (q^4+2q^3-3q^2-4q+4) &= -(q^2+4) - 4q(-1+q\mathfrak{X}_d(\hbar(v_d)+w))\\ \Leftrightarrow 4q^2\lambda_w &= (q^4+2q^3-3q^2-4q+4) - q^2 - 4 + 4q - 4q^2\mathfrak{X}_d(\hbar(v_d)+w)\\ \Leftrightarrow 4q^2\lambda_w &= q^4+2q^3-4q^2-4q^2\mathfrak{X}_d(\hbar(v_d)+w)\\ \Leftrightarrow \lambda_w &= \frac{1}{4}q^2+\frac{1}{2}q-1-\mathfrak{X}_d(\hbar(v_d)+w).\end{aligned}$$

Once we compute $\mathfrak{X}_d(\hbar(v_d)+w)$, we will have established that $\mathcal{D}$ is a PDS.

Lemma 48. *With the notation above,*

$$\mathfrak{X}_d(\hbar(v_d)+w) = \begin{cases}1 & \text{if } w\in\mathcal{D} \text{ and } \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w)\neq 1,\\ -1 & \text{if } w\notin\mathcal{D} \text{ and } w\neq 0.\end{cases}$$

Proof. Recall that if $w \in \mathcal{D}$ and $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) \neq 1$, then there exists a unique $d \in \mathbb{K}$ such that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) = v_d$. For this d, we have $w - \hbar(v_d) \in \mathbb{K}$. Therefore, there exists a unique $a_w \in \mathbb{K}$ such that $w = a_w + \hbar(v_d)$. This means

$$w = a_w + \left((-\mathbf{s}^2 + \mathbf{s})v_d^2 + \mathbf{s}v_d\right).$$

Hence, if $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) \neq 1$, then $w \in \mathcal{D}$ if and only if $a_w \in \mathcal{H}_{v_d}$. We now compute $\mathfrak{X}_d\left(\hbar(v_d) + w\right)$. We have

$$\begin{aligned}\chi_d\left(\hbar(v_d) + w\right) &= \mathfrak{X}_d(a_w) \\ &= \begin{cases} 1 & \text{if } a_w \in \mathcal{H}_{v_d}, \\ -1 & \text{otherwise.} \end{cases}\end{aligned}$$

This is equivalent to the statement in the lemma. □

We have now all but established the following theorem.

Theorem 49. *With the notation above, $\mathcal{D}$ is a $\left(q^2, \frac{1}{2}(q-1)(q+2), \frac{1}{4}q^2 + \frac{1}{2}q - 2, \frac{1}{4}q^2 + \frac{1}{2}q\right)$-PDS.*

Proof. Note that if $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) = 1$, then $w \in \mathcal{D}$. In this case, we have concluded $\lambda_w = \frac{1}{4}q^2 + \frac{1}{2}q - 2$. For the case in which $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(w) \neq 1$, we have also derived the equation

$$\lambda_w = \frac{1}{4}q^2 + \frac{1}{2}q - 1 - \mathfrak{X}_d\left(\hbar(v_d) + w\right).$$

By the last lemma, we finally have

$$\lambda_w = \begin{cases} \frac{1}{4}q^2 + \frac{1}{2}q - 2 & \text{if } w \in \mathcal{D}, \\ \frac{1}{4}q^2 + \frac{1}{2}q & \text{if } w \notin \mathcal{D} \text{ and } w \neq 0. \end{cases}$$

□

Chapter 7

CLASS III

In Chapter 6, we formed the PDS $\mathcal{D}$ by taking the union of particular multiplicative cosets of a subfield (with 0 removed). As it turns out if $[\mathbb{L} : \mathbb{K}] = 2$, any union of cosets of $\mathbb{K}$ in $\mathbb{L}$ can be taken to be a PDS. This construction applies to any finite field of any characteristic, not just 2 as in the previous classes.

Let p be a prime number, $n \in \mathbb{N}$, $q = p^n$, $a = q - 1$, $b = q + 1$. Let $\mathbb{L} = \mathbb{F}_{q^2}$ with $\mathbb{L}^\star = \langle \mathfrak{g} \rangle$, and let $\mathbb{K} = \mathbb{F}_q$. Finally, let $C = \mathbb{K}^\star$, and let $\mathcal{J}$ be a nonempty subset of $\mathbb{Z}_a \cong \mathbb{L}^\star / C$ with $|\mathcal{J}| = m$, and define

$$\mathcal{D} = \bigcup_{j \in \mathcal{J}} \mathfrak{g}^j C.$$

In this chapter we prove the following:

Theorem 50. *With the notation above, $\mathcal{D}$ is a $\left(q^2, m(q-1), q + m(m-3), m(m-1)\right)$-PDS.*

Since $C = \mathbb{K}^\star$, we may exploit the extra structure in C inherited from all of $\mathbb{K}$. Recall the formula for counting difference representations.

$$v\lambda_w = \sum_{i=0}^{a-1} \left|\chi_1(\mathfrak{g}^i \mathcal{D})\right|^2 \chi_1(\mathfrak{g}^{m+i} C).$$

By substituting the expression for $\mathcal{D}$, we obtain

$$v\lambda_w = \sum_{i=0}^{a-1} \left|\sum_{j \in \mathcal{J}} \chi_1(\mathfrak{g}^{i+j} C)\right|^2 \chi_1(\mathfrak{g}^{m+i} C).$$

Since $C = \mathbb{K}^\star$, by letting $t' = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\mathfrak{g}^{i+j})$, we have

$$\begin{aligned}\chi_1(\mathfrak{g}^{i+j}C) &= \chi_{\mathfrak{g}^{i+j}}(C)\\ &= \mathfrak{X}_{t'}(C)\\ &= \begin{cases} q-1 \text{ if } t'=0,\\ -1 \text{ otherwise.}\end{cases}\end{aligned}$$

Let $\mathcal{U} = \ker(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}})$. Then $\mathcal{U}$ is a $\mathbb{K}$-vector subspace of $\mathbb{L}$. Since $\dim_{\mathbb{K}}(\mathbb{L}) = 2$ and $\mathrm{rank}(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}})) = 1$, we have that $\dim_{\mathbb{K}}(\mathcal{U}) = 1$. Therefore, $\mathcal{U} = s^*\mathbb{K}^\star$ for some $s^* \in \mathbb{L}^\star$. Without loss of generality, we may take $s^* = \mathfrak{g}^{i^*}$ with $i^* \in \mathbb{Z}_a$. We therefore have the following:

Theorem 51. *With the notation above, we have*

$$\chi_1(\mathfrak{g}^i\mathcal{D}) = \begin{cases} q-m \text{ if } i+j=i^* \text{ for some } i,j\in\mathbb{Z}_a,\\ -m \text{ otherwise.}\end{cases}$$

Proof. We begin by expanding the character sum in question to character sums of cosets of C.

$$\chi_1(\mathfrak{g}^i\mathcal{D}) = \sum_{j\in\mathcal{J}}\chi_1(\mathfrak{g}^{i+j}C).$$

Note that as j ranges over $\mathcal{J}$, all elements of the form $i + j$ are distinct elements of $\mathbb{Z}_a$. Therefore, all terms in the above sum are evaluated over distinct cosets of C, which are 1-dimensional $\mathbb{K}$ - subspaces of $\mathbb{L}$ with 0 removed. For a fixed i, there is at most one value of $j \in \mathcal{J}$ such that $i + j = i^*$. If there is no such j, then all terms of this sum are -1, and there are m such terms, so the sum equals $-m$. If there exists such a j, then one term of the sum is $q - 1$, and the other $m - 1$ terms are -1, thus establishing the claim. □

With the possible values of $\chi_1(\mathfrak{g}^i\mathcal{D})$ computed, we must now compute the frequency with which $\chi_1(\mathfrak{g}^i\mathcal{D})$ attains these values.

Theorem 52. *The character sum $\chi_1(\mathfrak{g}^i\mathcal{D})$ attains the value $q - m$ for m values of $i \in \mathbb{Z}_a$ and the value $-m$ for $q + 1 - m$ values of $i \in \mathbb{Z}_a$.*

Proof. Recall that by the orthogonality relations of characters, we have

$$-1 = \sum_{l=0}^{a-1} \chi_1(\mathfrak{g}^l C).$$

By writing the character sum $\chi_1(\mathfrak{g}^i \mathcal{D})$ in terms of character sums of cosets of C, we obtain

$$\chi_1(\mathfrak{g}^i \mathcal{D}) = \sum_{j \in \mathcal{J}} \chi_1(\mathfrak{g}^{i+j} C).$$

By summing this equation over all $i \in \mathbb{Z}_a$ and using orthogonality, we conclude

$$\begin{aligned}
\sum_{i=0}^{a-1} \chi_1(\mathfrak{g}^i \mathcal{D}) &= \sum_{i=0}^{a-1} \sum_{j \in \mathcal{J}} \chi_1(\mathfrak{g}^{i+j} C) \\
&= \sum_{j \in \mathcal{J}} \sum_{i=0}^{a-1} \chi_1(\mathfrak{g}^{i+j} C) \\
&= \sum_{j \in \mathcal{J}} -1 \\
&= -m.
\end{aligned}$$

Let A denote the number of values of $i \in \mathbb{Z}_a$ for which $\chi_1(\mathfrak{g}^i \mathcal{D}) = q - m$. Then the number of values of $i \in \mathbb{Z}_a$ for which $\chi_1(\mathfrak{g}^i \mathcal{D}) = -m$ is $q + 1 - A$. From this, we conclude

$$\begin{aligned}
-m &= A(q - m) + (q + 1 - A)(-m) \\
-m &= Aq - m - mq \\
A &= m.
\end{aligned}$$

The result follows. □

We know that $\chi_1(\mathfrak{g}^{i+m} C)$ can attain one of two possible values, namely, $q - 1$ and -1. We must now consider how these character sums relate to the sums $\chi_1(\mathfrak{g}^i \mathcal{D})$, which also can attain one of two possible values.

Theorem 53. *With the above notation, $\mathcal{D}$ is a $(q^2, mb, q + m(m-3), m(m-1))$-PDS.*

Proof. There is a unique $i \in \mathbb{Z}_a$ such that $i + m = i^*$, namely, $i^* - m$. We can thus simplify the equation used to compute λ_w in the following way:

$$\begin{aligned} v\lambda_w - k^2 &= |\chi_1(\mathfrak{g}^{i^*-r}\mathcal{D})\chi_1(\mathfrak{g}^{i^*}C) + \sum_{i \neq i^*-r} |\chi_1(\mathfrak{g}^i\mathcal{D})\chi_1(\mathfrak{g}^iC) \\ &= (q-1)\left|\chi_1(\mathfrak{g}^{i^*-r}\mathcal{D})\right|^2 - \sum_{i \neq i^*-r} \left|\chi_1(\mathfrak{g}^i\mathcal{D})\right|^2 \\ &= q\left|\chi_1(\mathfrak{g}^{i^*-r}\mathcal{D})\right|^2 - \sum_{i=0}^{a-1} \left|\chi_1(\mathfrak{g}^i\mathcal{D})\right|^2 \end{aligned}$$

The last equation above was obtained by using (13). By substituting this value and the values $v = q^2$, and $k = mb$, we obtain

$$\begin{aligned} q^2\lambda_w - (mb)^2 &= q\left|\chi_1(\mathfrak{g}^{i^*-r}\mathcal{D})\right|^2 - mq^2 + m^2b \\ q^2\lambda_w &= q\left|\chi_1(\mathfrak{g}^{i^*-r}\mathcal{D})\right|^2 + mq^2 + m^2b + m^2b^2 \\ &= q\left|\chi_1(\mathfrak{g}^{i^*-r}\mathcal{D})\right|^2 - mq^2 + m^2b(b+1) \\ &= q\left|\chi_1(\mathfrak{g}^{i^*-r}\mathcal{D})\right|^2 - mq^2 + m^2q(q-1) \\ &= q\left|\chi_1(\mathfrak{g}^{i^*-r}\mathcal{D})\right|^2 - mq^2 + m^2q^2 - m^2q \\ \lambda_w &= \frac{1}{q}\left(\left|\chi_1(\mathfrak{g}^{i^*-r}\mathcal{D})\right|^2 - m^2\right) + m^2 - m. \end{aligned}$$

The above sum can attain one of two values. These correspond to the cases in which $\chi_1(\mathfrak{g}^{i^*-r}\mathcal{D})$ equals $q - m$ or $-m$. We know that $\chi_1(\mathfrak{g}^{i^*-r}\mathcal{D}) = q - m$ if and only if there exists $j \in \mathcal{J}$ such that $i^* - r + j = i^*$. This occurs if and only if $r \in \mathcal{J}$. The condition that $m \in \mathcal{J}$ is equivalent to the condition that $w \in \mathcal{D}$. We therefore conclude that λ_w depends solely on w's membership in $\mathcal{D}$. In other words, $\mathcal{D}$ is a PDS. We now need only compute its parameters.

In order to compute λ, we first assume $w \in \mathcal{D}$. This means $\chi_1(\mathfrak{g}^{i^*-m}\mathcal{D}) = q - m$. By

substitution we obtain

$$\begin{aligned}\lambda &= \frac{1}{q}\Big((q-m)^2 - m^2\Big) + m^2 - m \\ &= \frac{1}{q}(q^2 - 2qm) + m^2 - m \\ &= q + m(m+3).\end{aligned}$$

We now assume $w \notin \mathcal{D}$ in order to compute μ.

$$\begin{aligned}mu &= \frac{1}{q}\Big((-m)^2 - m^2\Big) + m^2 - m \\ &= m^2 - m \\ &= m(m-1).\end{aligned}$$

□

In general, when $\left|\mathbb{F}_q^\star : C\right| = a$ and there exists an $i \in \mathbb{N}$ such that $p^i \equiv -1 \mod a$, we are said to be in the semiprimitive case. In [3], it is shown that for any choice of $\mathcal{J}$, the corresponding set $\mathcal{D}$ is a PDS in the semiprimitive case. Note that in class III, $a = q+1$, and $p^n \equiv -1 \mod a$, so we are in the semiprimitive case.

It should be noted that in [2], it is proven that the semiprimitive case is equivalent to case in which $\chi_1(\mathrm{g}^i C)$ attains the same value for all i except one.

Chapter 8

EQUIVALENCES FOR CLASSES I, II, AND III

8.1 Introduction

We now relate the notion of difference sets to that of bent functions. This relation can only be made, however, in the case in which the field in question has characteristic 2.

In order to define what a bent function is, we must first introduce the notions of Boolean functions, Hamming weight, and Hamming distance.

Definition 54. *A* Boolean function *is a function* $h : \mathbb{F}_2^n \to \mathbb{F}_2$. *The* support *of* h *is the set* $supp(h) = \{x \in \mathbb{F}_2^n \mid f(x) \neq 0\}$.

There is an intuitive way to define weights for Boolean functions which naturally gives rise to a notion of distance between two Boolean functions.

Definition 55. *Let* h *be a Boolean function on* $\mathbb{F}_2^n$. *Then the* Hamming weight *of* h *is* $w_H(h) = |\{x \in (\mathbb{F}_2)^n \mid h(x) \neq 0\}|$. *If* k *is another Boolean function on* $\mathbb{F}_2^n$, *then the* Hamming distance *between* h *and* k *is* $d_H(h, k) = |\{x \mid h(x) \neq k(x)\}|$.

We use this Hamming distance in the definition of a bent function. First, we must define a particular class of Boolean functions.

Definition 56. *Let* h *be a Boolean function on* $\mathbb{F}_2^n$ *with* $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$. *If* $h(x) = a_0 + a_1x_1 + a_2x_2 + \cdots + a_nx_n$ *with* $a_1, \ldots, a_n \in \mathbb{F}_2$, *then* h *is an* affine function.

Let A_n denote the set of all affine functions on $\mathbb{F}_2^n$. For an arbitrary Boolean function, h, we would like to measure in some sense how far h is from being an affine function. With the use of Hamming distance, we can make this measurement precise.

Definition 57. *Let h be a Boolean function on $\mathbb{F}_2^n$. Then the* nonlinearity *of h is $nl(h) = \min_{l \in A_n} d_H(h, l)$.*

It is known that if h is a Boolean function on $\mathbb{F}_2^{2n}$, then $nl(h) \leq 2^{2n-1} - 2^{n-1}$. We are finally in a position to define bent functions.

Definition 58. *Let h be a Boolean function on $\mathbb{F}_2^{2n}$. Then h is a* bent function *if $nl(h) = 2^{2n-1} - 2^{n-1}$.*

Loosely speaking, bent functions are as far from being affine or "straight" as possible, hence the name. There are many equivalent formulations of bent functions. One such formulation can be stated in terms of difference sets.

Theorem 59. *Let h be a Boolean function on $\mathbb{F}_2^{2n}$. Then h is a bent function if $supp(h)$ is a nontrivial difference set.*

Since the complement of a PDS is also a PDS, we also have that the nonzero roots of a bent function form a (v, k, λ, μ)-PDS with $\mu - \lambda = 2$.

8.2 Maiorana–McFarland Bent Functions, and Classes I and II

Since $\mathbb{F}_2^{2n}$ can be identified with $\mathbb{F}_2^n \times \mathbb{F}_2^n$ in a natural way, we may consider bent functions on $\mathbb{F}_2^{2n}$ as bivariate functions on $\mathbb{F}_2^n$. With this alternate form, an infinite family of bent functions can be expressed. For this, let "$\cdot$" denote the standard dot product in $\mathbb{F}_2^n$, and let $\mathrm{Sym}(\mathbb{F}_2^n)$ denote the symmetric group on $\mathbb{F}_2^n$.

Theorem 60. *Let $n \in \mathbb{N}$, $\pi \in Sym(\mathbb{F}_2^n)$, $k : \mathbb{F}_2^n \to \mathbb{F}_2$. Then the bivariate function on $\mathbb{F}_2^n$, $h(x, y) = x \cdot \pi(y) + k(y)$, is a bent function.*

This class of bent functions is called the Maiorana-McFarland class. In this chapter we prove the following.

Theorem 61. *The PDS's of classes I and II are equivalent to complements of DS's arising from Maiorana-McFarland bent functions.*

Let $\mathbb{F} = \mathbb{F}_2$. When we regard the fields $\mathbb{K}$ and $\mathbb{L}$ as $\mathbb{F}$-vector spaces, we shall express them as $\mathbb{F}^n$ and $\mathbb{F}^{2n}$, respectively. Thus, if a PDS in $\mathbb{F}^n \times \mathbb{F}^n$ is found, then it gives rise to a corresponding PDS in $\mathbb{L}$.

Let $T(x, y) = \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(xy)$. Then T is clearly bilinear over $\mathbb{F}$. Since q is even, there exists a self-dual basis $\{e_1, \ldots, e_n\}$ of $\mathbb{K}/\mathbb{F}$. This was proven by Seroussi and Lempel in [23]. By definition, this means that $T(e_i, e_j) = \delta_{ij}$. Let $\overline{e_1}, \ldots, \overline{e_n}$ be the standard basis of $\mathbb{F}^n$, and let $\varphi : \mathbb{K} \to \mathbb{F}^n$ be the linear transformation given by $\varphi(e_i) = \overline{e_i}$ for $i = 1, \ldots, n$, and extending by $\mathbb{F}$-linearity. Denote $\varphi(v) = \overline{v}$. Since $T(e_i, e_j) = \overline{e_i} \cdot \overline{e_j} = \delta_{ij}$, the dot product contained in the definition of the Maiorana-McFarland class is closely related to the field structure of $\mathbb{K}$.

8.3 Class I

Recall that in class I, $D = \mathcal{H}_1 C \backslash \{0\}$. D is also the set of nonzero roots of $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x))$. Let $\{1, \mathbf{b}\}$ be a basis for $\mathbb{K}/\mathbb{F}$, and let $x + y\mathbf{b} \in \mathbb{L}$ with $x, y \in \mathbb{K}$. We now relate the value of $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x + y\mathbf{b}))$ with computations in $\mathbb{F}^n$ corresponding to elements of $\mathbb{K}$.

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x + y\mathbf{b})) &= \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(x^2 + xy + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{b})y^2) \\
&= \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(x + xy) + \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{b})y^2) \\
&= \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(x(y + 1)) + \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{b})y^2) \\
&= \overline{x} \cdot \overline{y + 1} + \overline{\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{b})} \cdot \overline{y^2}.
\end{aligned}$$

Here we use bar notation to denote elements of the vector space $\mathbb{F}_2^n$. Let $\pi(\overline{y}) = \overline{y + 1}$, and let $k(y) = \overline{\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{b})} \cdot \overline{y^2}$. Then we finally arrive at the following:

Lemma 62. *Let $x + y\boldsymbol{b} \in \mathbb{L}$ with $x, y \in \mathbb{K}$. Then*

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x + y\boldsymbol{b})) = \overline{x} \cdot \pi(\overline{y}) + k(\overline{y}).$$

This proves (61) for class I.

8.4 Class II

Recall that $\mathcal{D} = \{u^2 + uv + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s})v^2 - u - vs \mid u, v \in \mathbb{K}\} \setminus \{0\}$. Let $\{e_1, \ldots, e_n\}$ be a self-dual basis of the extension $\mathbb{K}/\mathbb{F}$, and let $\{\overline{e_1}, \ldots, \overline{e_n}\}$ be the standard basis of $\mathbb{F}^n$ over $\mathbb{F}$.

Rewrite $\mathcal{D}$ as $\mathcal{D} = \{(u^2 + (v-1)u) + (\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s})v^2 - \mathbf{s}v) \mid u, v \in \mathbb{K}\}$. Note that for fixed v, $u^2 + (v-1)u$ is a 2-polynomial in u. This means that the image of this polynomial is an F-subspace of of $\mathbb{K}$. Since this polynomial is quadratic in u, the corresponding subspace is either all of $\mathbb{K}$ (when $v = 1$), or is index two in $\mathbb{K}$. In other words, these subgroups are hyperplanes in $\mathbb{K}$.

Let $\mathcal{H}_v = im(u^2 + (v-1)u)$. By the previous remarks made in the proof of 49, all $\mathcal{H}_\gamma$ are distinct for distinct γ. Since every hyperplane of $\mathbb{K}$ is the kernel of some linear functional on $\mathbb{K}$ and every linear functional is of the form $T_\gamma(x) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\gamma x)$, we conclude that for each hyperplane $\mathcal{H}_v$, $v \neq 1$, there exists $v \in \mathbb{K}$ such that $\ker(T_v) = \mathcal{H}_v$. In other words, $\mathcal{H}_v = \{c \in \mathbb{K} \mid T(c, v)\} = 0$. Note that $T(c, v) = 0$ in $\mathbb{K}$ if and only if $\overline{c} \cdot \overline{v} = 0$ in $\mathbb{F}^n$. This means that $\overline{\mathcal{H}_v} = \langle \overline{v} \rangle^\perp$.

We are now in a position to test for when an arbitrary element of $\mathbb{L}$, $x + y\mathbf{s}$, $x, y \in \mathbb{K}$ is an element of D. If $x + y\mathbf{s} \in D$, then there exists $u, v \in \mathbb{K}$ such that $x + y\mathbf{s} = u^2 + (v-1)u + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s})v^2 - v\mathbf{s}$. Since $\{1, \mathbf{s}\}$ is a $\mathbb{K}$-basis of $\mathbb{L}$, we have $x + y\mathbf{s} \in D$ if and only if there exists $u, v \in \mathbb{K}$ such that the following hold:

$$x = u^2 + (v-1)u + \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s})v^2$$

$$y = -v$$

Thus, the v in question is easily determined from the given element. Using the fact that the condition for x contains the aforementioned 2-polynomial, the condition can be rewritten as

$$x - \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s})y^2 \in \mathcal{H}_y$$

When passing from $\mathbb{K}$ to $\mathbb{F}^n$, this condition is equivalent to

$$\overline{x - \mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s})y^2} \cdot \overline{v_y} = 0$$

Written another way, this is

$$\overline{x} \cdot \overline{v_y} + \overline{\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s})y^2} \cdot \overline{v_y} = 0$$

Letting $\pi(\overline{y}) = \overline{v_y}$ and $k(\overline{y}) = \overline{\mathrm{N}_{\mathbb{L}/\mathbb{K}}(\mathbf{s})y^2} \cdot \overline{v_y}$, we see that Class II is the complement of a difference set coming from a bent function from the Maiorana-McFarland class. Therefore, (61) is proven for class II.

8.5 Orthogonal Arrays and Class III

Class III consists of PDS's in finite fields of any prime characteristic, not just 2. As the Maiorana-McFarland class of bent functions is defined only over fields of characteristic 2, class III cannot possibly arise from bent functions in the same way that classes I and II do. Class III PDS's, however, arise naturally from the combinatorial objects known as orthogonal arrays.

Definition 63. *Let $\mathcal{X}$ be a set with $|\mathcal{X}| = v$. Then a t-(v, m, λ)* orthogonal array *is a $\lambda v^t \times m$ array such that for every t-subset of the columns of the array, each t-tuple of elements of $\mathcal{X}$ appears λ times.*

We will primarily be concerned with the case in which $t = 2$ and $\lambda = 1$. In this case, a 2-$(v, m, 1)$ orthogonal array is a $v^2 \times m$ array such that for every pair of columns, each ordered pair in $\mathcal{X} \times \mathcal{X}$ appears exactly once.

From the last chapter, we may view $\mathbb{L}$ as a two-dimensional $\mathbb{K}$-vector space with K-basis $\{1, \mathbf{s}\}$. Using the notation from Chapter 7, let $|\mathcal{I}| = m$, and let A be a $q^2 \times m$ array with rows indexed by $\mathbb{K}^2$ and columns indexed by $\mathcal{I}$. Let $\pi : \mathbb{L} \to \mathbb{K}$ be the $\mathbb{K}$-linear functional given by $\pi(a + b\mathbf{s}) = b$ for all $a, b \in \mathbb{K}$. It is clear that $\ker(\pi) = \mathbb{K}$. Let the $((a, b), i)$-th entry of A be $\pi(g^i(a + b\mathbf{s}))$. With the entries of A defined, we have the following:

Theorem 64. *With the notation above, A is a 2-$(q, m, 1)$ orthogonal array.*

Proof. In order to show that A is an orthogonal array, we must show that for any $i, j \in \mathcal{I}$, $i \neq j$, each ordered pair $(x, y) \in \mathbb{K}^2$ appears exactly once in the i-th and j-th column of A. Suppose (x, y) appears at least twice in the i-th and j-th column and the (a, b)-th and (c, d)-th row with $(a, b) \neq (c, d)$. This leads to the following equations.

$$\pi(g^i(a + b\mathbf{s})) = x,$$
$$\pi(g^i(c + d\mathbf{s})) = x,$$
$$\pi(g^j(a + b\mathbf{s})) = y,$$
$$\pi(g^j(c + d\mathbf{s})) = y.$$

From the first two equations, we obtain

$$0 = \pi(g^i(a + b\mathbf{s} - c - d\mathbf{s})),$$
$$0 = \pi(g^i(a - c + (b - d)\mathbf{s})).$$

Therefore, we have $g^i(a - c + (b - d)\mathbf{s}) \in \mathbb{K}$. By a similar argument,

$$0 = \pi(g^j(a - c + (b - d)\mathbf{s}))$$

And so $g^j(a - c + (b - d)\mathbf{s}) \in \mathbb{K}$. If $a - c + (b - d)\mathbf{s} \neq 0$, then we divide these two elements of $\mathbb{K}$ to conclude that $g^{i-j} \in \mathbb{K}^*$. This occurs if and only if $i = j$, a contradiction. Therefore, we have $a - c + (b - d)\mathbf{s} = 0$. Since $\{1, \mathbf{s}\}$ is a $\mathbb{K}$-basis of $\mathbb{L}$, we have that $a - c = 0$, and $b - d = 0$, which means $(a, b) = (c, d)$, a contradiction. We thus have that (x, y) appears at most once in the i-th and j-th column of A. A simple counting argument then yields that (x, y) appears exactly once in the i-th and j-th column of A. □

Chapter 9

AN ATTEMPT AT A FURTHER CONSTRUCTION

9.1 Introduction

Through computation we have observed GDS's in $\mathbb{F}_{3^5}$ and $\mathbb{F}_{3^{11}}$ that are composed of cosets of particular subgroups of their multiplicative subgroups. We have attempted to generalize their construction to form an infinite class of such GDS's. The theory we develop here is based on our analysis of the two computed examples. To that end, we first find conditions that certain parameters must satisfy in order to generate this class.

Let $p = 3$, and let u and e be prime numbers such that $e \equiv 5 \mod 6$ and $u = 2e + 1 \equiv 11 \mod 12$. Let $q = 3^e$, and let $\mathbb{L} = \mathbb{F}_q$ with $\mathbb{L}^\star = \langle \mathfrak{g} \rangle$. Let $\mathcal{H} = \mathrm{Gal}\left(\mathbb{L}/\mathbb{F}_p\right) = \langle \sigma \rangle$, where $\sigma(x) = x^3$ for all $x \in \mathbb{L}$. Let $a = 2u$, and let $q - 1 = ab$. Let $C = \langle \mathfrak{g}^a \rangle \leq \mathbb{L}^\star$, thus $|C| = b$ and $|\mathbb{L}^\star : C| = a$. We wish to construct a GDS, $\mathcal{D}$, that is a union of cosets of C that is invariant under $\mathcal{H}$, that is, $\psi(\mathcal{D}) = \mathcal{D}$ for all $\psi \in \mathcal{H}$.

Note that each element in $\mathbb{L}/C$ can be uniquely expressed in the form $\mathfrak{g}^i C$ with $0 \leq i < a$. Also note that C char $\mathbb{L}^\star$, that is, $\psi(C) = C$ for all $\psi \in \mathcal{H}$. Because of this, an action of $\mathcal{H}$ can be defined on $\mathbb{L}/C$ by way of $\psi\left(\mathfrak{g}^i C\right) = \psi\left(\mathfrak{g}^i\right) C$ for all $\psi \in \mathcal{H}$. One can easily verify that this definition satisfies the axioms of a group action. In order to simplify notation, we can also define $\mathcal{H}$ to act on $\mathbb{Z}_a$. To do this, let $\psi \in \mathcal{H}$, and let $i \in \mathbb{Z}_a$. Then if $\psi\left(\mathfrak{g}^i C\right) = \mathfrak{g}^j C$, define $\psi(i) = j$.

Recall that $\mathcal{H}$ is generated by the Frobenius automorphism σ, where $\sigma(u) = u^p$ for all $u \in \mathbb{L}$ and that $|\mathcal{H}| = e$. This means that $\sigma(i) = 3 \cdot i$ for all $i \in \mathbb{Z}_a$. Using this fact, the orbits of $\mathcal{H}$ acting on $\mathbb{Z}_a$ can be easily computed.

Theorem 65. *Let $\mathcal{H}$ act on $\mathbb{Z}_a$ as defined above. Then this action has* 2 *fixed points and* 4 *orbits of length e.*

Proof. We will use the Orbit-Stabilizer theorem to compute the orbit sizes in $\mathbb{Z}_a$. It is clear that 0 is a fixed point of $\mathcal{H}$. Let $i \in \mathbb{Z}_a^*$. We now wish to find all $\psi \in \mathcal{H}$ such that $\psi(i) = i$. Since $\mathcal{H} = \langle\sigma\rangle$, it suffices to find all $j \in \mathbb{Z}$ such that $0 \leq j < e$ and $\sigma^j(i) = i$. It is clear that $j = 0$ is always a solution to this equation, so we now assume that $j \neq 0$. Note that $\sigma^j(i) = 3^j i$. Thus i is a fixed point of σ^j if and only if $3^j i \equiv i \mod a$, or $\left(3^j - 1\right) i \equiv 0 \mod a$. This occurs precisely when $a \mid \left(3^j - 1\right) i$. We may now introduce $\gcd(a, i)$ into this divisibility relation:

$$\frac{a}{\gcd(a,i)} \left| \left(3^j - 1\right) \frac{i}{\gcd(a,i)}. \right.$$

Since the fractions above are coprime natural numbers, we now have the following:

$$\frac{a}{\gcd(a,i)} \left| 3^j - 1. \right.$$

By definition, $a \left| 3^e - 1 \right.$, so $\frac{a}{\gcd(a,i)} \left| 3^e - 1 \right.$ as well. This means that

$$\frac{a}{\gcd(a,i)} \left| \gcd\left(3^j - 1, 3^e - 1\right) \right.$$

It is well-known that for all prime numbers p, $\gcd\left(p^a - 1, p^b - 1\right) = p^{\gcd(a,b)} - 1$. Since e is prime and $0 \leq j < e$, we conclude that $\gcd(j, e) = 1$. This means that

$$\begin{aligned} \gcd\left(3^j - 1, 3^e - 1\right) &= 3^{\gcd(j,e)} - 1 \\ &= 3^1 - 1 \\ &= 2. \end{aligned}$$

Consequently,

$$\frac{a}{\gcd(a,i)} \left| 2. \right.$$

So $\frac{a}{\gcd(a,i)} = 1$ or 2, meaning $\gcd(a, i) = a$ or $\frac{a}{2}$. Since $0 < i < a$, we have that $1 < \gcd(a, i) < a$. We conclude that $i = \frac{a}{2}$. In this case, there are no restrictions on a. This means that $\frac{a}{2} \in \mathbb{Z}_a$ is a fixed point of $\mathcal{H}$. In other words, $\frac{a}{2}$ is in an orbit of size 1.

For all other values of i, the only element of $\mathcal{H}$ that fixes i is the identity automorphism. That is, $|\mathcal{H}_i| = 1$. By Orbit-Stabilizer theorem, we have that $|i^{\mathcal{H}}| = |\mathcal{H} : \mathcal{H}_i| = \frac{|\mathcal{H}|}{1} = |\mathcal{H}| = e = \frac{u-1}{2}$.

In summary, when $\mathcal{H}$ acts on $\mathbb{Z}_a$, there are 2 fixed points: 0 and $\frac{a}{2}$. The remaining $a-2$ elements are contained in orbits of size $\frac{u-1}{2}$. Since $a = 2u$, we have that $a-2 = 2(u-1)$. From here, it is clear that there are 4 orbits of length $\frac{u-1}{2}$, and the proof is complete. □

We now wish to find algebraic properties of cosets in $\mathbb{L}^\star/C$ that remain constant on all cosets in the same orbit in the action of $\mathcal{H}$ on $\mathbb{L}^\star/C$. In this way we can attribute properties to these orbits that would otherwise be attributed to individual elements of $\mathbb{Z}_a$ or individual cosets in $\mathbb{L}^\star/C$.

Lemma 66. *For all $i \in \mathbb{Z}_a$ and $\psi \in \mathcal{H}$, we have $\chi_1\left(\psi\left(\mathfrak{g}^i C\right)\right) = \chi_1\left(\mathfrak{g}^i C\right)$.*

Proof. It suffices to prove that the lemma holds for $\psi = \sigma$ since $\mathcal{H} = \langle\sigma\rangle$. That is, we must show that for all $i \in \mathbb{Z}_a$, we have $\chi_1\left(\mathfrak{g}^{3i} C\right) = \chi_1\left(\mathfrak{g}^i C\right)$.

We first expand the sum $\chi_1\left(\mathfrak{g}^i C\right)$ and apply the definition of the character χ_1 to obtain

$$\begin{aligned}\chi_1\left(\mathfrak{g}^i C\right) &= \sum_{c\in C} \chi_1\left(\mathfrak{g}^i c\right) \\ &= \sum_{c\in C} \mathfrak{wexp}\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{g}^i c\right)\right).\end{aligned}$$

Since $\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(x^3\right) = \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(x)$ for all $x \in \mathbb{L}$, we have

$$\sum_{c\in C} \mathfrak{wexp}\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{g}^i c\right)\right) = \sum_{c\in C} \mathfrak{wexp}\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{g}^{3i} c^3\right)\right).$$

As c ranges over all of C, so too does c^3. Thus we obtain

$$\begin{aligned}\sum_{c\in C} \mathfrak{wexp}\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{g}^{3i} c^3\right)\right) &= \sum_{c\in C} \mathfrak{wexp}\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{g}^{3i} c\right)\right) \\ &= \chi_1\left(\mathfrak{g}^{3i} C\right) \\ &= \chi_1\left(\sigma\left(\mathfrak{g}^i C\right)\right).\end{aligned}$$

Thus the result is proved. □

We now relate the values of $\chi_1\left(\mathfrak{g}^i C\right)$ and $\chi_1\left(-\mathfrak{g}^i C\right)$.

Lemma 67. *For all $i \in \mathbb{Z}_a$, we have $\chi_1\left(-\mathfrak{g}^i C\right) = \chi_1\left(\mathfrak{g}^{i+u} C\right) = \overline{\chi_1\left(\mathfrak{g}^i C\right)}$.*

Proof. Note that $-1 = \mathfrak{g}^{(q-1)/2} = \mathfrak{g}^{bu}$. Since $q - 1 \equiv 2 \mod 4$ and a is even, we have that b is odd, so let $b = 2l + 1$, $l \in \mathbb{N}$. We then obtain

$$\begin{aligned} bu &= (2l+1)u \\ &= 2ul + u \\ &= al + u. \end{aligned}$$

Since $C = \langle \mathfrak{g}^a \rangle$, we conclude $-1C = \mathfrak{g}^u C$. This means $-\mathfrak{g}^i C = \mathfrak{g}^{i+u} C$, and so $\chi_1\left(-\mathfrak{g}^i C\right) = \chi_1\left(\mathfrak{g}^{i+u} C\right)$. Next, we compute $\chi_1\left(-\mathfrak{g}^i C\right)$ by expanding the sum and using $\mathbb{F}$-linearity of $\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}$:

$$\begin{aligned} \chi_1\left(-\mathfrak{g}^i C\right) &= \sum_{c \in C} \chi_1\left(-\mathfrak{g}^i c\right) \\ &= \sum_{c \in C} \mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(-\mathfrak{g}^i c\right)\right) \\ &= \sum_{c \in C} \mathfrak{w}\exp\left(-\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{g}^i c\right)\right) \\ &= \sum_{c \in C} \overline{\mathfrak{w}\exp\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{g}^i c\right)\right)} \\ &= \overline{\chi_1\left(\mathfrak{g}^i C\right)}. \end{aligned}$$

This completes the proof. □

Since $a = 2u$ and u is odd, by the Chinese Remainder Theorem, we have that $\mathbb{Z}_a \cong \mathbb{Z}_2 \times \mathbb{Z}_u$. This isomorphism is given by $\Phi : j \mapsto (j \bmod 2, j \bmod u)$ for all $j \in \mathbb{Z}_a$. This isomorphism allows us to define an action of $\mathcal{H}$ on $\mathbb{Z}_a \cong \mathbb{Z}_2 \times \mathbb{Z}_u$ by letting $\psi(i, j) = \Phi(\psi(\Phi^{-1}(i, j)))$. This new action is permutation-isomorphic to the action of $\mathcal{H}$ on $\mathbb{Z}_a$. As such, this action has six orbits consisting of two fixed elements and four orbits of size e. We now characterize these orbits.

Theorem 68. *The orbits of $\mathcal{H}$ acting on $\mathbb{Z}_2 \times \mathbb{Z}_u$ consists of the following six sets:*

$$\{(0,0)\}$$

$$\{(1,0)\}$$

$$\{(0,s) : s \in \square_u^*\}$$

$$\{(1,s) : s \in \square_u^*\}$$

$$\{(0,n) : n \in \boxslash_u\}$$

$$\{(1,n) : n \in \boxslash_u\}$$

Moreover, the size of each of the last four orbits is e.

Proof. Note that for all $(i,j) \in \mathbb{Z}_2 \times \mathbb{Z}_u$, we have $\sigma(i,j) = (3i, 3j)$. Since $|\mathcal{H}| = e$ is prime, we conclude that orbits of this action have sizes either 1 or e, which correspond to the cases in which the order of stabilizers of elements in the orbits are e or 1, respectively. In order to compute $\mathcal{H}_{(i,j)}$, we need only check if $\sigma(i,j) = (i,j)$.

First, we find that $\sigma(0,0) = (3 \cdot 0, 3 \cdot 0) = (0,0)$. Therefore, $|\mathcal{H}_{(0,0)}| = e$, and it follows that $(0,0)$ is a fixed element of this action, so its orbit size is 1. Similarly, $\sigma(1,0) = (3 \cdot 1, 3 \cdot 0) = (1,0)$, so $(1,0)$ is also a fixed point of this action.

Next, we observe that since $u \equiv 11$ modulo 12, we conclude that $u \equiv 2 \bmod 3$, and $u \equiv 3 \bmod 4$. Using these congruences and the laws of quadratic reciprocity, we compute

$$\begin{aligned}\left(\frac{3}{u}\right) &= -\left(\frac{u}{3}\right) \\ &= -\left(\frac{2}{3}\right) \\ &= -(-1) \\ &= 1.\end{aligned}$$

We conclude that 3 is a quadratic residue modulo u. Since $u \mid q - 1 = 3^e - 1$, we have that $3^e \equiv 1$ modulo u. Since e is prime, we conclude that $o(3) = e \mod u$. Because $e = \frac{u-1}{2}$, we know that 3 generates the subgroup of non-zero squares in $\mathbb{Z}_u$. Using this fact, we can now classify the remaining four orbits. By definition, for all $(i,j) \in \mathbb{Z}_2 \times \mathbb{Z}_u$, we have that

$\sigma(i, j) = (i, 3j)$. If $j \neq 0$, then $(i, j) \neq (i, 3j)$, for otherwise we would have that $j \equiv 3j$ modulo u, which would imply that $u|2j$, meaning $j = 0$, a contradiction. Therefore, if $j \neq 0$, then the element (i, j) is in an orbit of size e. Noting that the first coordinate of elements in $\mathbb{Z}_2 \times \mathbb{Z}_u$ is fixed by σ, we deduce that the first coordinates of elements in the same orbit are equal. Since 3 is a non-zero square modulo u, we may also conclude that the second coordinates of the elements in a size-e orbit are either all squares or all nonsquares modulo u. Thus the theorem is proven. □

With these orbits established, we immediately have the following corollary.

Corollary 69. *Let $\mathcal{O}_{(x,y)}$ be the orbit containing (x, y) in the action of $\mathcal{H}$ on $\mathbb{Z}_2 \times \mathbb{Z}_u$. Then the totality of orbits is as follows.*

$$\begin{aligned}
\mathcal{O}_{(0,0)} &= \{0\}, \\
\mathcal{O}_{(1,0)} &= \{u\}, \\
\mathcal{O}_{(0,s)} &= \{j : j \equiv 0 \bmod 2 \text{ and } j \in \square_u^*\}, \\
\mathcal{O}_{(1,s)} &= \{j : j \equiv 1 \bmod 2 \text{ and } j \in \square_u^*\}, \\
\mathcal{O}_{(0,n)} &= \{j : j \equiv 0 \bmod 2 \text{ and } j \in \boxslash_u\}, \\
\mathcal{O}_{(1,n)} &= \{j : j \equiv 1 \bmod 2 \text{ and } j \in \boxslash_u\}.
\end{aligned}$$

We now apply our relations between different character sums to these orbits to obtain some rather unexpected results.

Corollary 70. *If $i, j \in \mathbb{Z}_a$ are in the same orbit of the action of $\mathcal{H}$ on $\mathbb{Z}_a$, then $\chi_1\left(\mathfrak{g}^i C\right) = \chi_1\left(\mathfrak{g}^j C\right)$*

Proof. If i and j are in the same orbit, then $j = \psi(i)$ for some $\psi \in \mathcal{H}$. We have already shown that in this case, we have $\chi_1\left(\mathfrak{g}^i C\right) = \chi_1\left(\mathfrak{g}^j C\right)$, so the proof is complete. □

This result allows us to refer to the character sum of an orbit rather than the character sum of a particular coset. This greatly reduces the number of character sums that need to be computed in order to test if a given set is a GDS. Namely, since there are six orbits in this

action, there are six different character sums that need to be computed. Let these character sums be $\mathbb{X}_0$, $\mathbb{X}_u$, $\mathbb{X}_{(0,s)}$, $\mathbb{X}_{(1,s)}$, $\mathbb{X}_{(0,n)}$, and $\mathbb{X}_{(1,n)}$, respectively. As it turns out, however, this number can essentially be reduced to three as the next theorem will show.

Theorem 71. *With the notation established above, we have that* $\mathbb{X}_u = \overline{\mathbb{X}_0}$, $\mathbb{X}_{(1,s)} = \overline{\mathbb{X}_{(0,s)}}$, *and* $\mathbb{X}_{(1,n)} = \overline{\mathbb{X}_{0,n)}}$.

Proof. Note that if $i \in \mathcal{O}_{(0,s)}$, then $i+u \in \mathcal{O}_{(1,s)}$. Similarly, if $i \in \mathcal{O}_{(0,n)}$, then $i+u \in \mathcal{O}_{(1,n)}$. This follows from the Chinese Remainder Theorem, since if $\Phi(l) = (i, j)$, then $\Phi(l+u) = (i+1, j)$. The result follows. □

With this result established, we conclude that we need only compute three character sums in order to test if a set is a GDS. Let $\mathbb{X}_s = \mathbb{X}_{(0,s)}$, and $\mathbb{X}_n = \mathbb{X}_{(0,n)}$. Thus, our goal is now to compute $\mathbb{X}_0$, $\mathbb{X}_s$, and $\mathbb{X}_n$. Using identities derived from orthogonality relations as well as Gauss sums, we can derive several equations that these character sums must satisfy. For ease of notation, let $\mathbb{X}_0 = R_0 + I_0 i$, $\mathbb{X}_s = R_s + I_s i$, and $\mathbb{X}_0 = R_n + I_n i$ with $R_0, R_s, R_n, I_0, I_s, I_n \in \mathbb{R}$. The first equation is a consequence of orthogonality of characters.

Theorem 72. *With the established notation, we have* $-1 = 2R_0 + (u-1)(R_s + R_n)$.

Proof. As χ_1 is a non-principal character, we immediately have

$$0 = \frac{1}{q} \sum_{a \in \mathbb{L}} \chi_1(a).$$

Since the cosets of C partition $\mathbb{L}^\star$, we may rewrite the sum as

$$0 = \frac{1}{q} \left(\chi_1(0) + \sum_{j=0}^{a-1} \chi_1(\mathfrak{g}^j C) \right),$$

From which we have

$$-1 = \sum_{j=0}^{a-1} \chi_1(\mathfrak{g}^j C).$$

We may now make use of the orbit structure of the action of $\mathcal{H}$ on $\mathbb{L}^\star/C$ to rewrite this sum as the following:

$$-1 = \mathbb{X}_0 + \overline{\mathbb{X}_0} + e(\mathbb{X}_s + \overline{\mathbb{X}_s}) + e(\mathbb{X}_n + \overline{\mathbb{X}_n}).$$

Using simple properties of complex numbers, this sum becomes

$$-1 = 2R_0 + 2e(R_s + R_n).$$

Since $e = \frac{u-1}{2}$, we finally arrive at

$$-1 = 2R_0 + (u-1)(R_s + R_n).$$

which was what we wished to show. □

We now apply Theorem 12 to derive two quadratic equations.

Theorem 73. *With the established notation, we have the identity*

$$q - b = 2\left|\mathbb{X}_0\right|^2 + (u-1)\left(\left|\mathbb{X}_s\right|^2 + \left|\mathbb{X}_n\right|^2\right).$$

Proof. Since $|C| = b$, we have

$$b = \frac{1}{q}\sum_{x\in\mathbb{L}} \left|\chi_x(C)\right|^2.$$

By rearranging terms and separating the $a = 0$ term from the summation, we obtain

$$qb = \left|\chi_0(C)\right|^2 + \sum_{x\in\mathbb{L}^\star} \left|\chi_1(xC)\right|^2$$

$$qb - b^2 = \sum_{x\in\mathbb{L}^\star} \left|\chi_1(xC)\right|^2.$$

Since $\left|\mathbb{L}^\star : C\right| = a$, we have that in the above summation, all a cosets of C are added b times. We thus have

$$q - b = \sum_{j=0}^{a-1} \left|\chi_1\left(\mathfrak{g}^j C\right)\right|^2.$$

We may now once again make use of the orbit structure of the action of $\mathcal{H}$ on $\mathbb{L}^\star/C$ to rewrite this sum as

$$\begin{aligned} q - b &= \left|\mathbb{X}_0\right|^2 + \left|\overline{\mathbb{X}_0}\right|^2 + e\left|\mathbb{X}_s\right|^2 + e\left|\overline{\mathbb{X}_s}\right|^2 + e\left|\mathbb{X}_n\right|^2 + e\left|\overline{\mathbb{X}_n}\right|^2 \\ &= 2\left|\mathbb{X}_0\right|^2 + 2e\left(\left|\mathbb{X}_s\right|^2 + \left|\mathbb{X}_n\right|^2\right). \end{aligned}$$

Noting that $e = \frac{u-1}{2}$, we finally arrive at

$$q - b = 2\left|\mathbb{X}_0\right|^2 + (u-1)\left(\left|\mathbb{X}_s\right|^2 + \left|\mathbb{X}_n\right|^2\right),$$

which was what we wished to show. □

We may also prove a similar identity by using a different subgroup of $\mathbb{L}^\star$. Let $\mathcal{E} = \langle C, -1\rangle$. Since $-1 \notin C$, we have that $\mathcal{E} = C \cup -1C$, and so $|\mathcal{E}| = 2b$.

Theorem 74. *With the established notation, we have the identity*

$$\frac{q-2b}{2} = 2R_0^2 + (u-1)\left(R_s^2 + R_n^2\right).$$

Proof. We immediately have

$$2b = \frac{1}{q}\sum_{x\in\mathbb{L}} |\chi_x(\mathcal{E})|^2 .$$

As before, we can rearrange terms and separate the $x = 0$ term from the summation to obtain

$$2qb = (2b)^2 + \sum_{x\in\mathbb{L}} |\chi_x(\mathcal{E})|^2$$

Since $\left|\mathbb{L}^\star : \mathcal{E}\right| = u$, we may rewrite the above sum as

$$2qb = (2b)^2 + 2b\sum_{j=0}^{u-1} \left|\chi_1\left(\mathfrak{g}^j\mathcal{E}\right)\right|^2 .$$

By canceling and rearranging terms, we obtain

$$q - 2b = \sum_{j=0}^{u-1} \left|\chi_1\left(\mathfrak{g}^j\mathcal{E}\right)\right|^2 .$$

Note that for all $0 \le j \le u-1$, we can conclude

$$\begin{aligned}\mathfrak{g}^j\mathcal{E} &= \mathfrak{g}^j C \cup \mathfrak{g}^{-j}C \\ &= \mathfrak{g}^j C \cup \mathfrak{g}^{j+u}C.\end{aligned}$$

Because of this, we have the following equality concerning character sums:

$$\begin{aligned}\chi_1(\mathfrak{g}^j\mathcal{E}) &= \chi_1(\mathfrak{g}^j C) + \chi_1(\mathfrak{g}^{j+u}C) \\ &= \chi_1(\mathfrak{g}^j C) + \overline{\chi_1(\mathfrak{g}^j C)}.\end{aligned}$$

The two terms in the last equality are one of $\mathbb{X}_0$ and $\overline{\mathbb{X}_0}$, $\mathbb{X}_s$ and $\overline{\mathbb{X}_s}$, or $\mathbb{X}_n$ and $\overline{\mathbb{X}_n}$, not necessarily in that order. Since $\mathbb{Z}_u$ contains e nonzero squares and e nonsquares, we may rewrite the original character sum as

$$\begin{aligned} q - 2b &= \left|\mathbb{X}_0 + \overline{\mathbb{X}_0}\right|^2 + e\left|\mathbb{X}_s + \overline{\mathbb{X}_s}\right|^2 + e\left|\mathbb{X}_n + \overline{\mathbb{X}_n}\right|^2 \\ q - 2b &= |2R_0|^2 + e\,|2R_s|^2 + e\,|2R_n|^2 \\ \frac{q-2b}{2} &= 2R_0^2 + (u-1)\left(R_s^2 + R_n^2\right). \end{aligned}$$

This completes the proof. □

By using the last two equalities, the following is a direct consequence.

Corollary 75. *With the established notation, we have*

$$\frac{q}{2} = 2I_0^2 + (u-1)\left(I_s^2 + I_n^2\right).$$

Proof. Recall that for any $z \in \mathbb{C}$, we have that $|z|^2 = \Re(z)^2 + \Im(z)^2$. In our case, this would mean that $|\mathbb{X}_0|^2 = R_0^2 + I_0^2$, $|\mathbb{X}_s|^2 = R_s^2 + I_s^2$, and $|\mathbb{X}_n|^2 = R_n^2 + I_n^2$. By subtracting the equation in Theorem 74 from the equation in Theorem 73, we obtain the desired equation. □

We have derived a linear equation in R_0, R_s, R_n (Theorem 72), a quadratic equation in R_0, R_s, R_n (Theorem 74), and a quadratic equation in I_0, I_s, I_n (Corollary 75). We now wish to derive a linear equation in I_0, I_s, I_n. In order to do this, we use the following result concerning quadratic Gauss sums.

Theorem 76. *Let p be an odd prime, $s \in \mathbb{N}$, and $q = p^s$. Let η be the quadratic character of $\mathbb{F}_q$. We then have*

$$G(\chi_1, \eta) = \begin{cases} (-1)^{s-1}\sqrt{q} & \text{if } p \equiv 1 \bmod 4. \\ (-1)^{s-1} i^s \sqrt{q} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

This was first established for the case $s = 1$ by Gauss. For a proof of the general statement, see [17], theorem 5.15. With this stated, we may now prove the following result.

Theorem 77. *With the established notation, we have* $(-1)^{(e-1)/2}\sqrt{q} = 2I_0 + (u-1)(I_s + I_n)$.

Proof. We compute the Gauss sum $G(\chi_1, \eta)$ in $\mathbb{L}$. By definition, we have

$$G(\chi_1, \eta) = \sum_{x \in \mathbb{L}^\star} \eta(x)\chi_1(x).$$

Since $C = \langle \mathfrak{g}^a \rangle$ and a is even, we have that C must be a subgroup of the group of squares of $\mathbb{L}^\star$. Because of this, we can write $\langle \mathfrak{g}^2 \rangle$, the set of nonzero squares, as a union of cosets of C.

$$\langle \mathfrak{g}^2 \rangle = \bigcup_{j=0}^{u} \mathfrak{g}^{2j} C.$$

We can use this to rewrite $\mathbb{L}^\star$ as well:

$$\mathbb{L}^\star = \left(\bigcup_{j=0}^{u-1} \mathfrak{g}^{2j} C \right) \bigcup \left(\bigcup_{j=0}^{u-1} \mathfrak{g}^{2j+1} C \right).$$

With this partition of $\mathbb{L}^\star$, we can rewrite the quadratic Gauss sum:

$$\begin{aligned} G(\chi_1, \eta) &= \sum_{x \in \langle \mathfrak{g}^2 \rangle} \eta(x)\chi_1(x) + \sum_{x \in \mathbb{L}^\star \setminus \langle \mathfrak{g}^2 \rangle} \eta(x)\chi_1(x) \\ &= \sum_{x \in \langle \mathfrak{g}^2 \rangle} \chi_1(x) - \sum_{x \in \mathbb{L}^\star \setminus \langle \mathfrak{g}^2 \rangle} \chi_1(x). \end{aligned}$$

The last step above was obtained by evaluating the character η on all elements of $\mathbb{L}^\star$. We now use the cosets of C to partition this sum in the following way:

$$G(\chi_1, \eta) = \sum_{j=0}^{u-1} \chi_1\left(\mathfrak{g}^{2j} C\right) - \sum_{j=0}^{u-1} \chi_1\left(\mathfrak{g}^{2j+1} C\right).$$

In the first sum, as j ranges from 0 to $u-1$, we have that $2j$ ranges over the even squares modulo a, the even nonsquares mod a, and 0. Similarly in the second sum, as j ranges from 0 to $u-1$, we have that $2j+1$ ranges over the odd squares mod a, the odd nonsquares mod a, and u. Using this fact, we now have

$$G(\chi_1, \eta) = (\mathbb{X}_0 + e(\mathbb{X}_s + \mathbb{X}_n)) - \left(\overline{\mathbb{X}_0} + e\left(\overline{\mathbb{X}_s} + \overline{\mathbb{X}_n}\right)\right).$$

Using basic properties of complex numbers, this becomes

$$\begin{aligned} G(\chi_1, \eta) &= 2iI_0 + e(2iI_s + 2iI_n) \\ &= i(2I_0 + e(2I_s + 2I_n)) \\ &= i(2I_0 + (u-1)(I_s + I_n)). \end{aligned}$$

We also know, however, that

$$G(\chi_1, \eta) = (-1)^{e-1} i^e \sqrt{q}.$$

Since e is an odd prime, we simplify to obtain $G(\chi_1, \eta) = i^e \sqrt{q}$. We now equate the two expressions for the values of $G(\chi_1, \eta)$ and rearrange terms:

$$i^{e-1} \sqrt{q} = 2I_0 + (u-1)(I_s + I_n)$$

We may rewrite i^{e-1} as $(-1)^{(e-1)/2}$ to obtain

$$(-1)^{(e-1)/2} \sqrt{q} = 2I_0 + (u-1)(I_s + I_n).$$

This completes the proof. □

In summary, we will use the following four identities:

$$\begin{aligned}
-1 &= 2R_0 + (u-1)(R_s + R_n), \\
(-1)^{(e-1)/2} \sqrt{q} &= 2I_0 + (u-1)(I_s + I_n), \\
\frac{q-2b}{2} &= 2R_0^2 + (u-1)\left(R_s^2 + R_n^2\right), \\
\frac{q}{2} &= 2I_0^2 + (u-1)\left(I_s^2 + I_n^2\right).
\end{aligned}$$

We finally have one more equation relating the trace of elements in cosets of C in $\mathbb{L}$.

Theorem 78. *For all j, we have*

$$\sum_{c \in C} \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\mathfrak{g}^j c) = 0.$$

Proof. Since $C = \langle \mathfrak{h} \rangle$, we have

$$\sum_{c \in C} \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{g}^j c\right) = \sum_{l=0}^{b-1} \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{g}^j \mathfrak{h}^l\right).$$

By $\mathbb{F}$-linearity of trace, this becomes

$$\sum_{l=0}^{b-1} \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{g}^j \mathfrak{h}^l\right) = \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\sum_{l=0}^{b-1} \mathfrak{g}^j \mathfrak{h}^l\right).$$

The sum on the right-hand side is one of a geometric sequence.

$$\begin{aligned}\sum_{l=0}^{b-1} \mathfrak{g}^j \mathfrak{h}^l &= \mathfrak{g}^j \frac{1-\mathfrak{h}^b}{1-\mathfrak{h}} \\ &= \mathfrak{g}^j \frac{1-1}{1-\mathfrak{h}} \\ &= 0.\end{aligned}$$

Taking traces of both sides completes the proof. □

9.2 The $q = 3^5$ Case

Throughout this section, let $e = 5$. This means that $q = 243$, $u = 11$, $a = 22$, and $b = 11$. We also have that $C = \langle \mathfrak{g}^{22} \rangle$. For convenience, let $\mathfrak{h} = \mathfrak{g}^{22}$ so that $C = \langle \mathfrak{h} \rangle$. From the previous section, we immediately have the following equations:

$$-1 = 2R_0 + 10(R_s + R_n), \tag{9.1}$$

$$\sqrt{243} = 2I_0 + 10\left(I_s + I_n\right), \tag{9.2}$$

$$\frac{221}{2} = 2R_0^2 + 10\left(R_s^2 + R_n^2\right), \tag{9.3}$$

$$\frac{243}{2} = 2I_0^2 + 10\left(I_s^2 + I_n^2\right). \tag{9.4}$$

We first compute the possible values of $\mathbb{X}_0$. In what follows, put $\mathfrak{w} = \exp(2\pi i/3) = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$.

Theorem 79. *With the above notation,* $\mathbb{X}_0 = 2 - 3\sqrt{3}i$ *or* $\frac{-11+9\sqrt{3}i}{2}$.

Proof. By definition, we have

$$\mathbb{X}_0 = \sum_{j=0}^{10} \chi_1\left(\mathfrak{h}^j\right).$$

Note that $\mathcal{H}$ acts on C, and this action has three orbits: $\{1\}$, $\{\mathfrak{h}^1, \mathfrak{h}^3, \mathfrak{h}^4, \mathfrak{h}^5, \mathfrak{h}^9\}$, and $\{\mathfrak{h}^2, \mathfrak{h}^6, \mathfrak{h}^7, \mathfrak{h}^8, \mathfrak{h}^{10}\}$. Since $\chi_1(x) = \chi_1(\psi(x))$ for all $\psi \in \mathcal{H}$, we may rewrite $\mathbb{X}_0$ as follows:

$$\mathbb{X}_0 = \chi_1(1) + 5\chi_1\left(\mathfrak{h}^1\right) + 5\chi_1\left(\mathfrak{h}^2\right).$$

By the definition of χ_1, this becomes

$$\mathbb{X}_0 = \mathfrak{w}\exp(1) + 5\,\mathfrak{w}\exp\left(\mathfrak{h}^1\right) + 5\,\mathfrak{w}\exp\left(\mathfrak{h}^5\right).$$

Since $e \equiv 2 \bmod 3$, we have that $\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(1) = 2$, and so $\chi_1(1) = \mathfrak{w}^2$. By (78), we have

$$\begin{aligned} 0 &= \sum_{c \in C} \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(c) \\ &= \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(1) + 5 \cdot \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{h}^1\right) + 5 \cdot \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{h}^2\right) \\ &= 2 + 2\,\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{h}^1\right) + 2\,\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{h}^2\right). \end{aligned}$$

By rearranging terms we obtain the equation

$$2 = \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{h}^1\right) + \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{h}^2\right).$$

From this, we conclude that either $\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{h}^1\right) = \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{h}^2\right) = 1$, or $\left\{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{h}^1\right), \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}\left(\mathfrak{h}^2\right)\right\} = \{0, 2\}$. The former implies

$$\begin{aligned} \mathbb{X}_0 &= \mathfrak{w}\exp(1) + 5\,\mathfrak{w}\exp\left(\mathfrak{h}^1\right) + 5\,\mathfrak{w}\exp\left(\mathfrak{h}^5\right) \\ &= \mathfrak{w}^2 + 5\mathfrak{w} + 5\mathfrak{w} \\ &= \frac{-1 - \sqrt{3}i}{2} + 10\left(\frac{-1 + \sqrt{3}i}{2}\right) \\ &= \frac{-11 + 9\sqrt{3}i}{2}. \end{aligned}$$

The latter implies

$$\begin{aligned} \mathbb{X}_0 &= \mathfrak{w}\exp(1) + 5\,\mathfrak{w}\exp\left(\mathfrak{h}^1\right) + 5\,\mathfrak{w}\exp\left(\mathfrak{h}^5\right) \\ &= \mathfrak{w}^2 + 5(1) + 5\mathfrak{w}^2 \\ &= 5 + 6\left(\frac{-1 - \sqrt{3}i}{2}\right) \\ &= 2 - 3\sqrt{3}i. \end{aligned}$$

This completes the proof. □

Theorem 80. *With the above notation,* $\mathbb{X}_0 = 2 - 3\sqrt{3}i$.

Proof. Note that C is the set of roots of $X^{11} - 1 = \Phi_1(X)\Phi_{11}(X) \in \mathbb{L}[X]$. Since $|\mathbb{L} : \mathbb{F}| = 5$, we conclude that the irreducible factors of $\Phi_{11}(X)$ are of degree 5, and therefore $\Phi_{11}(X) =$

$f(X)g(X)$ where $f(X)$ and $g(x)$ are irreducible quintic polynomials over $\mathbb{F}[X]$. Let $\mathfrak{h}$ be a root of $f(X)$, which means that all the conjugates of $\mathfrak{h}$ are roots of $f(X)$, and let $\mathfrak{h}^2$ and its conjugates be the roots of $g(X)$. Note that the reciprocals of the roots of $f(X)$ are precisely the roots of $g(X)$. This means that $g(X)$ is a constant multiple of the reciprocal polynomial of $f(X)$. The constant multiple ensures that $g(X)$ is monic.

Let

$$f(X) = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0.$$

This means that

$$\begin{aligned} g(X) &= a_0^{-1}X^5 f(X^{-1}) \\ &= a_0^{-1}X^5\left(X^{-5} + a_4X^{-4} + a_3X^{-3} + a_2X^{-2} + a_1X + a_0\right) \\ &= X^5 + a_1a_0^{-1}X^4 + a_2a_0^{-1}X^3 + a_3a_0^{-1}X^2 + a_4a_0^{-1}X + a_0^{-1}. \end{aligned}$$

We now compute a_0. Recall that the coefficient of the X^i term of a monic, degree-n polynomial is $(-1)^{n-i}$ times the $(n-i)$-th elementary symmetric polynomial of its roots. For $f(X)$, this means that $a_0 = -\operatorname{N}_{\mathbb{L}/\mathbb{F}}(\mathfrak{h}) = \mathfrak{h}^{(243-1)/(3-1)} = -\mathfrak{h}^{121} = -1$. This means that

$$g(X) = X^5 - a_1X^4 - a_2X^3 - a_3X^2 - a_4X - 1,$$

and therefore,

$$\Phi_{11}(X) = \left(X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X - 1\right)\left(X^5 - a_1X^4 - a_2X^3 - a_3X^2 - a_4X - 1\right)$$

We also have that $\Phi_{11}(X) = \sum_{i=0}^{10} X^i$. By equating the coefficients of X^9, X^8, and X^5 in these equations for $\Phi_{11}(X)$, we obtain the following three equations:

$$1 = a_4 - a_1 \tag{9.5}$$

$$1 = a_3 - a_1a_4 - a_2 \tag{9.6}$$

$$1 = -2 - a_1^2 - a_2^2 - a_3^2 - a_4^2 \tag{9.7}$$

In order to prove the theorem, it suffices to show that $\operatorname{Tr}_{\mathbb{L}/\mathbb{F}}(\mathfrak{h}) \neq 1$, for otherwise we would have $\mathbb{X}_0 = \frac{-11+9\sqrt{3}i}{2}$. To this end, we assume by way of contradiction that $\operatorname{Tr}_{\mathbb{L}/\mathbb{F}}(\mathfrak{h}) = 1$. Since

$f(X) = m_{\mathfrak{h}}(X)$, we have that $-a_4 = \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\mathfrak{h})$. This together with (9.5) implies $a_1 = 1$ and $a_4 = 2$. Substituting these values into (9.6) implies $a_2 = a_3$. By substituting these values into (9.7), we deduce

$$1 = -2 - 1^2 - a_2^2 - a_2^2 - 2^2,$$

which simplifies to

$$2 = a_2^2$$

This is a contradiction since 2 is not a square in $\mathbb{F}$. The result follows. □

With this theorem proven, we have established that $R_0 = 2$ and $I_0 = -3\sqrt{3}$. By substituting these values into (9.1), (9.2), (9.3), and (9.4), and rearranging terms, we obtain

$$-\frac{1}{2} = R_s + R_n, \tag{9.8}$$

$$\frac{3\sqrt{3}}{2} = I_s + I_n, \tag{9.9}$$

$$\frac{41}{4} = R_s^2 + R_n^2 \tag{9.10}$$

$$\frac{27}{4} = I_s^2 + I_n^2. \tag{9.11}$$

With these new equations, we can deduce the following:

Theorem 81. *With the notation above, we have*

$$\{\mathbb{X}_s, \mathbb{X}_n\} = \left\{2, \frac{-5 + 3\sqrt{3}i}{2}\right\}.$$

Proof. Recall that $\mathbb{X}_s$ and $\mathbb{X}_n$ are both sums of eleven cube roots of unity. This imposes severe limitations on the possible values of R_s, R_n, I_s, and I_n. In general, let

$$\mathbb{X} = a + b\mathfrak{w} + c\mathfrak{w}^2$$

be a sum of eleven cube roots of unity, where $a, b, c \in \mathbb{Z}$ with $a, b, c \geq 0$ and $a + b + c = 11$. By substituting the value of $\mathfrak{w}$ and simplifying, we obtain

$$\begin{aligned}\mathbb{X} &= a + b\frac{-1 + \sqrt{3}i}{2} + c\frac{-1 - \sqrt{3}i}{2} \\ &= a - \frac{1}{2}(b + c) + \frac{\sqrt{3}}{2}(b - c)\, i.\end{aligned}$$

Using the fact that $a + b + c = 11$, we have

$$\begin{aligned}\mathbb{X} &= a - \frac{1}{2}(11 - a) + \frac{\sqrt{3}}{2}(b - c)\, i \\ &= \frac{1}{2}(3a - 11) + \frac{\sqrt{3}}{2}(b - c)\, i.\end{aligned}$$

This means that

$$\begin{aligned}R_s, R_n &\in \left\{\frac{1}{2}(3a - 11) : a = 0, 1, \ldots 11\right\}, \\ I_s, I_n &\in \left\{\frac{\sqrt{3}}{2} b : b = -11, -10, \ldots 11\right\}.\end{aligned}$$

We may now use (9.11) and (9.9) to solve for I_s and I_n. Let $I_s = \frac{\sqrt{3}}{2} b_s$, and $I_n = \frac{\sqrt{3}}{2} b_n$ with $b_s, b_n = -11, -10, \ldots, 11$. From (9.11) we have

$$\frac{27}{4} = \frac{3}{4} b_s^2 + \frac{3}{4} b_n^2,$$

that is,

$$9 = b_s^2 + b_n^2$$

This implies $\left\{b_s^2, b_n^2\right\} = \{0, 9\}$. From (9.9), we can conclude that $\{b_s, b_n\} = \{0, 3\}$, and so

$$\{I_s, I_n\} = \left\{0, \frac{3\sqrt{3}}{2}\right\}.$$

.

Next, let $R_s = \frac{1}{2}(3a_s - 11)$ and $R_n = \frac{1}{2}(3a_n - 11)$ with $a_s, a_n = 0, 1, \ldots, 11$. Then from (9.10) we have

$$\frac{41}{4} = \frac{1}{4}(3a_s - 11)^2 + \frac{1}{4}(3a_n - 11)^2,$$

which simplifies to

$$41 = (3a_s - 11)^2 + (3a_n - 11)^2.$$

Note that 41 can be written as the sum of two integer squares in a unique way: $41 = 16 + 25$. We therefore have

$$\left\{(3a_s - 11)^2, (3a_n - 11)^2\right\} = \{16, 25\}.$$

Also note that $3a_s - 11, 3a_n - 11 \equiv 1 \bmod 3$, and so we can conclude

$$\{3a_s - 11, 3a_n - 11\} = \{4, -5\}.$$

From here it is clear that

$$\{a_s, a_n\} = \{5, 2\},$$
$$\{R_s, R_n\} = \left\{2, -\frac{5}{2}\right\}.$$

Since $\mathbb{X}_s$ and $\mathbb{X}_n$ are algebraic integers, the result follows. □

We were able to determine by computer that $\mathbb{X}_s = 2$ and $\mathbb{X}_n = \frac{-5+3\sqrt{3}i}{2}$, however at the present time, a computer-free proof of this eludes us.

We now let $\mathcal{I} = \{0, 7, 13, 17, 19, 21\}$ and $\mathcal{D} = \cup_{j\in\mathcal{I}} \mathfrak{g}^j C$. Note that the nonzero elements of $\mathcal{J}$ are the odd nonsquares of $\mathbb{Z}_{22}$ and that $|\mathcal{D}| = 6 \cdot 11 = 66$. We now compute the values of $\mathbb{Y}_i$.

Theorem 82. *With the above notation, we have*

$$\mathbb{Y}_r = \begin{cases} -\frac{21}{2} - \frac{21\sqrt{3}}{2}i & \text{if } r = 0 \\ -\frac{21}{2} + \frac{21\sqrt{3}}{2}i & \text{if } r = 11 \\ 3 & \text{if } \left(\frac{r}{11}\right) = 1 \\ -\frac{3}{2} + \frac{3\sqrt{3}}{2}i & \text{if } \left(\frac{r}{11}\right) = -1 \text{ and } r \text{ is odd} \\ -\frac{3}{2} - \frac{3\sqrt{3}}{2}i & \text{if } \left(\frac{r}{11}\right) = -1 \text{ and } r \text{ is even.} \end{cases}$$

Proof. Recall that $\mathcal{D} = \bigcup_{j\in\mathcal{I}} \mathfrak{g}^i C$, where $\mathcal{I}$ contains 0 and the odd nonsquares of $\mathbb{Z}_{22}$. This means that

$$\begin{aligned} \mathbb{Y}_0 &= \mathbb{X}_0 + 5\overline{\mathbb{X}_n} \\ &= \left(2 - 3\sqrt{3}i\right) + 5\left(\frac{-5 - 3\sqrt{3}i}{2}\right) \\ &= -\frac{21}{2} - \frac{21\sqrt{3}}{2}i. \end{aligned}$$

By (67), we can also deduce $\mathbb{Y}_{11} = -\frac{21}{2} + \frac{21\sqrt{3}}{2}i$.

Next, we compute $\mathbb{Y}_r$ when $r \in \mathbb{Z}_{22}$ is an odd square. By definition, we have

$$\mathbb{Y}_r = \sum_{j \in \mathcal{J}+r} \mathbb{X}_j.$$

We must, therefore, determine what elements are in $\mathcal{J} + r = \mathcal{J} - (-r)$. Note that since r is an odd square, we have that $-r$ is an odd nonsquare. Using (3), we can conclude that $\mathcal{J} + r$ contains one odd square, the element 0, two even nonzero squares and two even nonsquares. We thus have

$$\begin{aligned}
\mathbb{Y}_r &= \mathbb{X}_0 + 2\mathbb{X}_s + 2\mathbb{X}_n + \overline{\mathbb{X}_s} \\
&= \left(2 - 3\sqrt{3}i\right) + 2\,(2) + 2\left(\frac{-5 + 3\sqrt{3}i}{2}\right) + 2 \\
&= 3
\end{aligned}$$

By (67), we also have $\mathbb{Y}_r = 3$ for r an even nonzero square as well.

We now apply the same argument to the case in which r is an odd nonsquare. By using (3) again, we can conclude that $\mathcal{I} + r$ contains one odd nonsquare, three even nonzero squares, and two even nonsquares. We thus have

$$\begin{aligned}
\mathbb{Y}_r &= \overline{\mathbb{X}_n} + 3\mathbb{X}_s + 2\mathbb{X}_n \\
&= \left(\frac{-5 - 3\sqrt{3}i}{2}\right) + 3\,(2) + 2\left(\frac{-5 + 3\sqrt{3}i}{2}\right) \\
&= -\frac{3}{2} + \frac{3\sqrt{3}}{2}i.
\end{aligned}$$

Finally, by (67), we also have $\mathbb{X}_r = -\frac{3}{2} - \frac{3\sqrt{3}}{2}i$ if r is an even nonsquare. □

By taking moduli, we immediately have

Corollary 83. *With the above notation, we have*

$$|\mathbb{Y}_r|^2 = \begin{cases} 441 & \text{if } \left(\frac{r}{11}\right) = 0, \\ 9 & \text{otherwise.} \end{cases}$$

With these character sums computed, we may now prove the following:

Theorem 84. *With the above notation, $\mathcal{D}$ is a GDS.*

Proof. We use (4.2) to obtain

$$243\lambda_w - 66^2 = \sum_{j=0}^{21} \left|\mathbb{Y}_j\right|^2 \mathbb{X}_{m+j} = \sum_{j=0}^{21} \left|\mathbb{Y}_{-j}\right|^2 \mathbb{X}_{m-j}.$$

By applying (83) to this equation, we obtain

$$243\lambda_w - 66^2 = 441\mathbb{X}_m + 441\mathbb{X}_{m-11} + 9\sum_{r\neq 0,11} \mathbb{X}_{m-j}.$$

By combining terms and using orthogonality, we deduce

$$\begin{aligned} 243\lambda_w - 66^2 &= 432\left(\mathbb{X}_m + \mathbb{X}_{m-11}\right) + 9\sum_{j=0}^{21} \mathbb{X}_{m-j} \\ &= 432\left(\mathbb{X}_m + \mathbb{X}_{m-11}\right) + 9\left(-1\right). \end{aligned}$$

By using (67) and rearranging terms, we obtain

$$\begin{aligned} 243\lambda_w - 66^2 + 9 &= 432\left(2\Re\left(\mathbb{X}_m\right)\right) \\ \lambda_w &= \frac{864\Re\left(\mathbb{X}_m\right) - 9 + 66^2}{243} \\ \lambda_w &= \frac{32\Re\left(\mathbb{X}_m\right) + 161}{9}. \end{aligned}$$

From the values of $\mathbb{X}_0$, $\mathbb{X}_s$, and $\mathbb{X}_n$, we have that

$$\Re\left(\mathbb{X}_m\right) = \begin{cases} 2 & \text{if } \left(\frac{m}{11}\right) \neq -1, \\ -\frac{5}{2} & \text{otherwise.} \end{cases}$$

By substituting these values, we finally conclude that λ_w can attain exactly two different values for nonzero $w \in \mathbb{F}_q$:

$$\lambda_w = \begin{cases} 25 & \text{if } \left(\frac{m}{11}\right) \neq -1, \\ 9 & \text{otherwise.} \end{cases}$$

What remains is to distinguish between when these cases occur. The first case occurs when m is a square in $\mathbb{Z}_{11}$, i.e. when m is one of the 12 squares $\mathbb{Z}_{22}$. □

9.3 The $q = 3^{11}$ Case

For this case, let $e = 11$. This implies that $q = 3^{11} = 177147$, $u = 23$, $a = 46$, and $b = 3851$. From the previous section, we immediately have the following equations:

$$-1 = 2R_0 + 22(R_s + R_n) \tag{9.12}$$

$$-243\sqrt{3} = 2I_0 + 22\,(I_s + I_n) \tag{9.13}$$

$$\frac{3^{11} - 46}{2} = 2R_0^2 + 22\left(R_s^2 + R_n^2\right) \tag{9.14}$$

$$\frac{3^{11}}{2} = 2I_0^2 + 22\left(I_s^2 + I_n^2\right). \tag{9.15}$$

As these numbers are relatively small, we may still readily determine possible values for the variables above through elementary, number-theoretic means.

Theorem 85. *With the notation above, $I_s = I_n = 0$, and $I_0 = \frac{-243\sqrt{3}}{2}$.*

Proof. Recall that $\mathbb{X}_0$, $\mathbb{X}_s$, and $\mathbb{X}_n$ are all sums of 3851 cube roots of unity. This means that each of these sums is of the form $\mathbb{X} = \frac{1}{2}(3a - 11) + \frac{\sqrt{3}}{2}(b - c)\,i$, where, $a, b, c \in \mathbb{Z} \cup \{0\}$, and $a + b + c = 3851$. By letting $I_0 = \frac{\sqrt{3}}{2}r$, $I_s = \frac{\sqrt{3}}{2}s$, and $I_n = \frac{\sqrt{3}}{2}t$ and substituting into (9.13) and (9.15), we obtain

$$-243 = r + 11\,(s + t) \tag{9.16}$$

$$3^{10} = r^2 + 11\left(s^2 + t^2\right) \tag{9.17}$$

As a result of (78), we have that $3 \mid r, s, t$, so let $r = 3x$, $s = 3y$, and $t = 3z$, where $x, y, z \in \mathbb{N} \cup \{0\}$. Substitution into (9.16) and (9.17) and simplification yields the following:

$$-81 = x + 11\,(y + z) \tag{9.18}$$

$$3^8 = x^2 + 11\left(y^2 + z^2\right) \tag{9.19}$$

By isolating x in (9.18) and squaring, we obtain

$$x^2 = 3^8 + 11^2\,(y + z)^2 + 2 \cdot 11 \cdot 81\,(y + z) \tag{9.20}$$

By substituting this into (9.19) and simplifying, we get

$$3^8 = 3^8 + 11^2 (y+z)^2 + 2 \cdot 11 \cdot 81 (y+z) + 11 \left(y^2 + z^2\right)$$
$$-162 (y+z) = 11 (y+z)^2 + \left(y^2 + z^2\right).$$

By noting that all terms on the right-hand side are non-negative, we can conclude that $-3 \leq x + y \leq 0$. By reducing this equation modulo 4, we obtain

$$2 (y+z) \equiv y^2 + z^2 - (y+z)^2 \mod 4. \tag{9.21}$$

From this congruence, we immediately see that $x + y$ is even. If $x + y = -2$, then we would have

$$-162 (-2) = 11 (4) + x^2 + y^2$$
$$280 = x^2 + y^2.$$

This equation has no integer solutions since $280 = 2^3 \cdot 5 \cdot 7$, $7 \equiv 3 \bmod 4$, and the power of 7 in the factorization of 280 is odd. Therefore, we conclude that $x + y = 0$. This forces $x = y = 0$, and therefore, $I_s = I_n = 0$. The result follows. □

We thus have that $\mathbb{X}_s, \mathbb{X}_n \in \mathbb{Q}(\mathfrak{w}) \cap \mathbb{R} = \mathbb{Q}$. Since $\mathbb{X}_s$ and $\mathbb{X}_n$ are algebraic integers, we also have that $\mathbb{X}_s, \mathbb{X}_n \in \mathbb{Z}$. By direct computation, we have the following:

Theorem 86. *With the above notation, we have $R_s = 44$, $R_n = -37$, and $R_0 = -\frac{155}{2}$. Thus, $\mathbb{X}_0 = \frac{-155-243i\sqrt{3}}{2}$, $\mathbb{X}_s = 44$, and $\mathbb{X}_n = -37$.*

With these character sums computed, we may directly compute which subsets $\mathcal{D}$ form GDS's of $\mathbb{L}$.

Theorem 87. *For each $\mathcal{J} \subseteq \mathbb{Z}_a$, let $\mathcal{D}_{\mathcal{J}} = \cup_{j \in \mathcal{J}} \mathfrak{g}^j C$. Then $\mathcal{D}_{\mathcal{J}}$ is a GDS for the following subsets $\mathcal{J}$:*

- $\mathcal{O}_{(0,n)}$
- $\mathcal{O}_{(1,n)}$

- $\mathcal{O}_{(0,0)} \cup \mathcal{O}_{(0,s)} \cup \mathcal{O}_{(0,n)}$
- $\mathcal{O}_{(0,0)} \cup \mathcal{O}_{(0,s)} \cup \mathcal{O}_{(1,n)}$
- $\mathcal{O}_{(0,0)} \cup \mathcal{O}_{(1,s)} \cup \mathcal{O}_{(0,n)}$
- $\mathcal{O}_{(1,0)} \cup \mathcal{O}_{(1,s)} \cup \mathcal{O}_{(1,n)}$
- $\mathcal{O}_{(1,0)} \cup \mathcal{O}_{(0,s)} \cup \mathcal{O}_{(0,n)}$
- $\mathcal{O}_{(1,0)} \cup \mathcal{O}_{(0,s)} \cup \mathcal{O}_{(1,n)}$
- $\mathcal{O}_{(1,0)} \cup \mathcal{O}_{(1,s)} \cup \mathcal{O}_{(0,n)}$
- $\mathcal{O}_{(1,0)} \cup \mathcal{O}_{(1,s)} \cup \mathcal{O}_{(1,n)}$
- $\mathcal{O}_{(0,0)} \cup \mathcal{O}_{(1,0)} \cup \mathcal{O}_{(0,s)} \cup \mathcal{O}_{(1,s)} \cup \mathcal{O}_{(0,n)}$
- $\mathcal{O}_{(0,0)} \cup \mathcal{O}_{(1,0)} \cup \mathcal{O}_{(0,s)} \cup \mathcal{O}_{(1,s)} \cup \mathcal{O}_{(1,n)}$.

Moreover, for those values of $\mathcal{J}$ in the above list that are the union of three orbits, the corresponding GDS is actually a SHDS.

It is unknown if these GDS's are part of an infinite class found over larger finite fields. It is also unclear which orbits are to be taken in order to obtain potential infinite classes.

Chapter 10

SUMMARY AND FUTURE WORK

In Chapter 2, we proved an integrality condition concerning the parameters of a PDS. In Chapter 3, we proved a group-ring equation that holds over any prime characteristic as opposed to just characteristic 3. As previously stated, it was proven in [11] that if a finite projective plane of Lenz-Barlotti type I.4 has order n with $3 \mid n$, then $9 \mid n$ or $n = 3$. The major step in the proof of this result is derivation of the equation found in (16) in the case in which $p = 3$. Unfortunately, the techniques used in finishing the proof do not generalize very well to other primes. As p increases, the number of group-ring elements to account for become unwieldy very quickly. If an analogous result is to be proven, one suspects different methods would need to be employed. The use of characters might prove useful in this regard.

In Chapters 4-7 we provided a method of constructing infinite classes of PDS's as well as three examples of such classes. In the search for infinite families of GDS's among image sets of polynomials, only binomials were considered in creating classes I-III. This was primarily for ease of computation. Perhaps more complicated families of polynomials can be considered for future investigation. It might also be the case that an infinite family of GDS's can be found through a completely different method, and this family could be reproduced as the image set of a well-known collection of polynomials. The appendix features tables of PDS's and DS's in small fields found by binomials. In Chapter 8 we show that these classes are equivalent to those coming from Maiorana-Mcfarland bent functions and orthogonal arrays.

Finally, in Chapter 9 we attempted to construct a new family of GDS's in fields of characteristic 3. The motivation for finding class III was investigating the image set of the polynomial $X^i(X^d - 1)$, where $rs = q + 1$, $d = r(q - 1)$, $i = rk$, $\gcd(k, q - 1) = 1$ and $k \not\equiv 1 \left(\mathrm{mod}\, \frac{q^2-1}{d}\right)$. In this case $|\mathcal{D}| = (s - 1)(q - 1)$. Empirical data seems to suggest another

infinite family of PDS's achieved through different polynomials. Using the above notation, the parameters are $\Big(q^2, (q-1)(s-1), s(r+1)+(s-1)(s-5), (s-1)(s-2)\Big)$. Whether these are the parameters of an infinite class of PDS's remains to be seen, and whether a binomial generates these PDS's is also unknown.

Although we found some GDS's in $\mathbb{F}_{3^5}$ and $\mathbb{F}_{3^{11}}$, it is still unclear if GDS's always exist in $\mathbb{F}_{3^e}$, where e is a prime. This answer seemingly rests on the solution set of equations (9.1), (9.2), (9.3), and (9.4). If either of I_s and I_n is 0, then the corresponding character sum $\mathbb{X}_s$ or $\mathbb{X}_n$ is real. Because of the nature of (4.3), these character sums being real restricts the number of potential values of λ_w, which may result in the corresponding subset being a GDS. If the character sums in these fields satisfy some pattern, then it should be possible to find infinite families of GDS's. Once these GDS's are found, the next question to address would be which of these GDS's are actually PDS's or DS's. In $\mathbb{F}_{3^{11}}$, for example, there were eight GDS's found out of 10 that were actually SHDS's.

BIBLIOGRAPHY

[1] A. Barlotti, *Le possibili configurazioni del sistema delle coppie punto-retta* (A, a) *per cui un piano grafico risulta* (A, a)*-transitivo*, Boll. Un. Mat. Ital. **12** (1957), 212–226.

[2] L. D. Baumert, W. H. Mills, and Robert L. Ward, *Uniform cyclotomy*, J. Number Theory **14**, no. 1, 67–82.

[3] A. E. Brouwer, R. M. Wilson, and Qing Xiang, *Cyclotomy and strongly regular graphs*, J. Algebraic Combin. **10** (1999), no. 1, 25–28.

[4] R.H. Bruck, *Difference sets in a finite group*, Trans. Amer. Math. Soc. **78** (1955), 464–481.

[5] X. Cao and D. Sun, *Some nonexistence results on generalized difference sets*, Appl. Math. Lett. **21** (2008), 797–802.

[6] S. Chowla, *A property of biquadratic residues*, Proc. Nat. Acad. Sci. India Sect. A. **14** (1944), 45–46.

[7] S. De Winter, E. Kamischke, and Z. Wang, *Automorphisms of strongly regular graphs with applications to partial difference sets*, Des. Codes Cryptogr. **79** (2016), 471–485.

[8] P. Dembowski, *Finite Geometries*, Springer-Verlag, New York, Heidelberg, Berlin, 1968, reprinted 1997.

[9] C. Ding and J. Yuan, *A family of skew Hadamard difference sets*, J. Combin. Theory Ser. A **113** (2006), 1526–1535.

[10] D. Ghinelli and D. Jungnickel, *On finite projective planes in Lenz-Barlotti class at least I.3*, Adv. Geom (2003), suppl., S28–S48.

[11] ———, *A non-existence result for finite projective planes in Lenz-Barlotti class I.4*, Combinatorica **27** (2007), 163–166.

[12] M. Hall, *A survey of difference sets*, Proc. Amer. Math. Soc **7** (1956), 975–986.

[13] D.R. Hughes, *Partial difference sets*, Amer. J. Math. **78** (1956), 650–674.

[14] W.M. Kantor, *Projective planes of type I.4*, Geom. Dedicata **3** (1974), 335–346.

[15] E. Lehmer, *On residue difference sets*, Canad. J. Math. **5** (1953), 425–432.

[16] H. Lenz, *Zur Begründung der analytischen Geometrie*, S.-B. Math.-Nat. Kl. Bayer. Akad. Wiss. (1954), 17–72.

[17] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).

[18] H.B. Mann, *Some theorems on difference sets*, Canad. J. Math. **4** (1952), 222–226.

[19] K. Momihara, Q. Wang, and Q. Xiang, *Cyclotomy, difference sets, sequences with low correlation, strongly regular graphs and related geometric substructures*, RICAM 2018: Proceedings of the Workshop on Pseudo-Randomness and Finite Fields, to appear.

[20] G.L. Mullen and D. Panario, *Handbook of Finite Fields*, Discrete Mathematics and Its Applications, vol. 78, Chapman and Hall, CRC Press, 2013.

[21] R.E.A.C. Paley, *On orthogonal matrices*, J. Math. Phys. MIT **12** (1933), 311–320.

[22] W. Qiu, Z. Wang, G. Weng, and Q. Xiang, *Pseudo-Paley graphs and skew Hadamard difference sets from presemifields*, Des. Codes Cryptogr. **44** (2007), 49–62.

[23] G. Seroussi and A. Lempel, *Factorization of symmetric matrices and trace-orthogonal bases in finite fields*, Siam J. Comp. **9** (1980), 758–767.

Appendix A

TABLES OF PDS'S AND GDS'S

A.1 Computational results

We now wish to detail a small number of computational results for binomials of the form $X^i(X^d - 1)$ with $d|(q-1)$. We have much more data than is presented here, but as seen below, there are many examples of PDS or DS arising even in this simple case, and so we have chosen to simply present tables for various fields to underline that the phenomena is widespread and not characteristic dependent. It should be mentioned that the phenomenon is not due to a small characteristic property (law of small numbers): for example, for $q = 47^2 = 2209$, one obtains 13 distinct parameters (plus their complements) for a PDS. To avoid extending an already long thesis any further, we choose only to give a few select field sizes to emphasize how much there is here to do. Anyone with the inclination could replicate what is presented here and more. In cases where we write, for example $(64,21,8,6)^c$ in the comments for the parameters (64,42,26,30), we mean that the PDS generated with the parameters (64,42,26,30) is the complement in $\mathbb{F}_{64}^\star$ of the PDS generated in the entry (64,21,8,6); of course, the latter will have a similar comment.

A.1.1 Brief comments on the characteristic 2 examples

Computational results for when $X^i(X^d - 1)$ yields an image set in $\mathbb{F}_q$ that exhibits a regularity of differences in characteristic 2 are given for $16 \leq q \leq 256$ in Tables A.1and A.2. In this characteristic, it is known that all DS arising must be connected to bent functions, so we make little further comment on these examples. For $q = 32$, we get two different sets $\mathcal{D}$ from the two lines. Both are divisible difference sets, with exceptional subgroup $\mathcal{N} = \{0, 1\}$ – all of $\mathbb{F}_q \setminus \mathcal{N}$ occurs as a difference in $\mathcal{D}$ 12 times, while $1 \in \mathcal{N}$ occurs 20 times.

Table A.1: $q \in \{16, 32, 64\}$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
(16,10,6)	1	$\{2, 6, 8, 12\}$	DS	$(3, 1)$-biregular
	5	$\{1, 3, 4, 6, 7, 9\}$	DS	
(16,12,8,12)	3	{2,4,5,7,8,10}	PDS	$\mathcal{D} = \mathbb{F}_q \setminus \mathbb{F}_4$
(16,9,4,6)	1	{4,10}	PDS	$(2, 1)$-biregular
(32,20,12,20)	1	$\{2, 14, 16, 28\}$		
	1	$\{4, 8, 22, 26\}$		
(64,36,20)	9	$\pm\{1, 4, 8, 11, 22, 25\}$ mod 54	DS	$(3, 1)$-biregular
(64,56,48,56)	7	32 in range $2 \leq i \leq 54$	PDS	$\mathcal{D} = \mathbb{F}_q \setminus \mathbb{F}_8$
(64,42,26,30)	21	$\gcd(i, 21) = 1$	PDS	$(64,21,8,6)^c$
(64,35,18,20)	1	$\{8, 54\}$	PDS	$(2, 1)$-regular
(64,27,10,12)	9	$\pm\{2, 10, 16, 17, 23\}$ mod 54	PDS	2-regular
(64,21,8,6)	7	$\pm\{4, 13, 16, 22, 25, 31\}$ mod 65	PDS	$(64,42,26,30)^c$
				$(3, 2)$-regular
(64,14,6,2)	21	$3k$ with $k \not\equiv 1$ mod 3	PDS	3-regular

Table A.2: $q = 256$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
(256,240,224,240)	15	many	PDS	$\mathcal{D} = \mathbb{F}_q \setminus \mathbb{F}_{16}$
(256,204,164,156)	51	many	PDS	$(256,51,2,12)^c$
(256,170,114,110)	5	many	PDS	$(2, 1)$-biregular
	85	many	PDS	$(256,85,24,30)^c$
(256,135,70,72)	1	{16,238}	PDS	$(2, 1)$-biregular
(256,119,54,56)	17	30 in range $2 \leq i \leq 236$	PDS	2-regular
(256,85,24,30)	85		PDS	2-regular, $(256,170,114,110)^c$
(256,68,12,20)	51	26, all of form $3k$	PDS	3-regular
(256,51,2,12)	51	many	PDS	4-regular, $(256,204,164,156)^c$

No PDS or DS are generated from binomials for $q = 128$. For $q = 256$, the entries for (256,170,114,110) are the first examples of binomials yielding inequivalent PDS with the same parameters.

Table A.3: $q \in \{81, 243\}$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
(81,64.49,56)	16	$i = 2k + 1 \not\equiv 7 \bmod 10$	PDS	$\mathcal{D} = \mathbb{F}_q^\star \setminus \langle \mathfrak{g}^5 \rangle$, $(81,16,7,2)^c$
(81,60,45,42)	20	$\gcd(i, 10) = 1$	PDS	$\mathcal{D} = \mathbb{F}_q^\star \setminus \langle \mathfrak{g}^4 \rangle$
(81,48,27,30)	4	$i = 10k + 3$, $0 \le k \le 7$	PDS	$(81,32,13,12)^c$
(81,40,19,20)	8	$i = 2k + 1 \not\equiv 1 \bmod 10$	PDS	Paley SHDS
	40	$\gcd(i, 10) = 1$	PDS	Paley SHDS
(81,32,13,12)	16	$\{6, 10, 14, 18\} \bmod 20$	PDS	2-regular
(81,20,1,6)	20	$\{6, 14, 22, 38\} \bmod 40$	PDS	$(4, 2)$-biregular, $(81, 60, 45, 42)^c$
	40	$\{2, 6, 14, 18\} \bmod 20$	PDS	2-regular
(81,16,7,2)	8	{6,26,46,66}	PDS	$(81, 64, 49, 56)^c$
	16	{7,17,27,37,47,57}	PDS	4-regular, $(81, 64, 49, 56)^c$
(243,121,60)	11	$\{12, 21\} \bmod 22$	DS	$(2, 1)$-biregular
	121	$\gcd(i, 11) = 1$	DS	
(243,220,199,220)	22	$\pm\{7, 9\} \bmod 22$	PDS	
(243,110,37,60)	22	$\pm\{5, 6\} \bmod 22$	PDS	2-regular

A.1.2 Brief comments on the odd characteristic examples

All DS and SHDS found in odd characteristics can be explained by Theorem 50.

The $q = 243$ case requires several comments.

- The DS generated for $d = 11$: Set $\mathcal{D}_{12}$ and $\mathcal{D}_{21}$ to be the DS generated for $i \equiv 12$ or 21 mod 22, respectively. Then $\mathcal{D}_{12} = -\mathcal{D}_{21}$.

- The DS generated for $d = 121$: Set $\mathcal{D}_{odd}$ and $\mathcal{D}_{even}$ to be the DS generated from i being odd or even, respectively. Then $\mathcal{D}_{even} = -\mathcal{D}_{odd}$, and $\mathcal{D}_{even}$ is the Paley DS.

Table A.4: $q = 729$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
(729,676,625,650)	52	many	PDS	$\mathcal{D} = \mathbb{F}_q^\star \setminus \langle \mathfrak{g}^{14} \rangle$, (729,52,25,2)^c
(729,624,531,552)	104	many	PDS	$\mathcal{D} = \mathbb{F}_q^\star \setminus \langle \mathfrak{g}^{7} \rangle$, (729,104,31,12)^c
(729,364,181,182)	26	3 mod 4 & more	PDS	$(2,1)$-biregular, Paley SHDS
	182	1 mod 4 & more	PDS	$(2,1)$-biregular, Paley SHDS
	364	as for $d = 26$	PDS	Paley SHDS
(729,312,135,132)	104	2 mod 4 & more	PDS	2-regular
(729,182,55,42)	26	1 mod 4 & more	PDS	$(4,3)$-biregular
	52	2 mod 4 & more	PDS	$(4,2)$-biregular
	182	3 mod 4 & more	PDS	3-regular
	364	2 mod 4 & more	PDS	2-regular
(729,156,45,30)	104	4 mod 8 & more	PDS	4-regular
(729,104,31,12)	26	8 mod 14 & more	PDS	(729,624,531,552)^c
	52	9 mod 14 & more	PDS	$(7,6)$-biregular, (729,624,531,552)^c
	104	11 mod 14 & more	PDS	6-regular, (729,624,531,552)^c
(729,52,25,2)	26	15 mod 28 & more	PDS	$(14,13)$-biregular, (729,676,625,650)^c
	52	16 mod 28 & more	PDS	(729,676,625,650)^c
	104	18 mod 28 & more	PDS	12-regular, (729,676,625,650)^c
	182	21 mod 28 & more	PDS	$(14,7)$-biregular, (729,676,625,650)^c
	364	7 mod 14 & more	PDS	7-regular, (729,676,625,650)^c

Table A.5: $q = 625$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
(625,576,529,552)	48	$2k+1, k \not\equiv 1 \bmod 3$		$\mathcal{D} = \mathbb{F}_q^\star \setminus \langle \mathfrak{g}^{13} \rangle$
		& $i \neq 26t+15, t \equiv 1,2 \bmod 3$	PDS	$(625, 48, 23, 2)^c$
(625,520,435,420)	104	$2k+1, k \not\equiv 2 \bmod 3$		$\mathcal{D} = \mathbb{F}_q^\star \setminus \langle \mathfrak{g}^{6} \rangle$
		& $i \neq 26t+13, t \equiv 0,1 \bmod 3$	PDS	$(625, 104, 3, 20)^c$
(625,416,279,272)	208	$2k+1, k \not\equiv 0 \bmod 3$		$\mathcal{D} = \mathbb{F}_q^\star \setminus \langle \mathfrak{g}^{3} \rangle$
		& $i \neq 26t+13, t \equiv 1,2 \bmod 3$	PDS	$(625, 208, 63, 72)_1^c$
(625,336,179,182)	12	$26k+7, k \not\equiv 1 \bmod 3$	PDS	
(625,312,155,156)	24	$\gcd(i,6) = 1, i \not\equiv 1 \bmod 26$	PDS	$(2,1)$-biregular, (Paley SHDS)^c
	312	$\gcd(i,78) = 1$	PDS	(Paley SHDS)^c
(625,288,133,132)	48	$4k+2, k \not\equiv 1 \bmod 3$		2-regular
		& $i \neq 52t+2, t \equiv 0,2 \bmod 3$	PDS	this is not $(625, 336, 179, 182)^c$
(625,208,63,72)	104	$\gcd(6k+5,13) = 1$	PDS	$(3,2)$-biregular, (625,416,279,272)^c
	208	$\gcd(6k+1,13) = 1$	PDS	2-regular, (625,416,279,272)^c
	208	$\gcd(4k+2,13) = 1, k \not\equiv 2 \bmod 3$	PDS	2-regular
(625,192,65,56)	48	$\{3, 27\} \bmod 78$	PDS	3-regular
(625,104,3,20)	208	$12k+10, k \not\equiv 10 \bmod 13$	PDS	4-regular, $(625, 520, 435, 520)^c$
	312	$\gcd(6k+3,13) = 1$	PDS	3-regular, equivalent to above
(625,48,23,2)	24	$52k+14, k \not\equiv 1 \bmod 3$	PDS	
	48	$26k+15$	PDS	12-regular

- ⊡ The (243,110,37,60)-PDS is a known example which, despite much effort, remains not part of a known infinite family, see the discussion between Theorems 4.10 and 4.11 of [19].

For $q = 625$, we note that there are two inequivalent (625,208,63,72)-PDS, the third row being inequivalent to the first two rows (which generate the same $\mathcal{D}$).

Appendix B

COPYRIGHT INFORMATION

B.1 Copyright Information for *Image sets with regularity of differences*

1. Publication

The copyright to this article, (including any supplementary information and graphic elements therein (e.g. illustrations, charts, moving images) (the 'Article'), is hereby assigned for good and valuable consideration to Springer Science+Business Media, LLC, part of Springer Nature (the 'Assignee'). Headings are for convenience only.

2. Grant of Rights

In consideration of the Assignee evaluating the Article for publication, the Author(s) grant the Assignee without limitation the exclusive (except as set out in clauses 3, 4 and 5 a) iv), assignable and sub-licensable right, unlimited in time and territory, to copy-edit, reproduce, publish, distribute, transmit, make available and store the Article, including abstracts thereof, in all forms of media of expression now known or developed in the future, including pre- and reprints, translations, photographic reproductions and extensions. Furthermore, to enable additional publishing services, such as promotion of the Article, the Author(s) grant the Assignee the right to use the Article (including the use of any graphic elements on a stand-alone basis) in whole or in part in electronic form, such as for display in databases or data networks (e.g. the Internet), or for print or download to stationary or portable devices. This includes interactive and multimedia use as well as posting the Article in full or in part or its abstract on social media, and the right to alter the Article to the extent necessary for such use. The Assignee may also let third parties share the Article in full or in part or its abstract on social media and may in this context sub-license the Article and its abstract to

social media users. Author(s) grant to Assignee the right to re-license Article metadata without restriction (including but not limited to author name, title, abstract, citation, references, keywords and any additional information as determined by Assignee).

3. Self-Archiving

Author(s) are permitted to self-archive a pre-print and an author's accepted manuscript version of their Article. A pre-print is the author's version of the Article before peer-review has taken place ("Pre-Print"). Prior to acceptance for publication, Author(s) retain the right to make a Pre-Print of their Article available on any of the following: their own personal, self-maintained website; a legally compliant, non-commercial pre-print server such as but not limited to arXiv and bioRxiv. Once the Article has been published, the Author(s) should update the acknowledgement and provide a link to the definitive version on the publisher's website: "This is a pre-print of an article published in [insert journal title]. The final authenticated version is available online at: https://doi.org/[insert DOI]". An Author's Accepted Manuscript (AAM) is the version accepted for publication in a journal following peer review but prior to copyediting and typesetting that can be made available under the following conditions: Author(s) retain the right to make an AAM of their Article available on their own personal, self-maintained website immediately on acceptance, Author(s) retain the right to make an AAM of their Article available for public release on any of the following 12 months after first publication ("Embargo Period"): their employer's internal website; their institutional and/or funder repositories. AAMs may also be deposited in such repositories immediately on acceptance, provided that they are not made publicly available until after the Embargo Period. An acknowledgement in the following form should be included, together with a link to the published version on the publisher's website: "This is a post-peer-review, pre-copyedit version of an article published in [insert journal title]. The final authenticated version is available online at: http://dx.doi.org/[insert DOI]".

4. Authors' Retained Rights

Author(s) retain the following non-exclusive rights for the published version provided that, when reproducing the Article or extracts from it, the Author(s) acknowledge and reference first publication in the Journal: to reuse graphic elements created by the Author(s)

and contained in the Article, in presentations and other works created by them; they and any academic institution where they work at the time may reproduce the Article for the purpose of course teaching (but not for inclusion in course pack material for onward sale by libraries and institutions); and to reproduce, or to allow a third party Assignee to reproduce the Article in whole or in part in any printed volume (book or thesis) written by the Author(s).

5. Warranties

The Author(s) warrant and represent that: (i) the Author(s) are the sole copyright owners or have been authorised by any additional copyright owner(s) to assign the rights defined in clause 2, (ii) the Article does not infringe any intellectual property rights (including without limitation copyright, database rights or trade mark rights) or other third party rights and no licence from or payments to a third party are required to publish the Article, (iii) the Article has not been previously published or licensed, (iv) if the Article contains material from other sources (e.g. illustrations, tables, text quotations), Author(s) have obtained written permissions to the extent necessary from the copyright holder(s), to license to the Assignee the same rights as set out in Clause 2 but on a non-exclusive basis and without the right to use any graphic elements on a stand-alone basis and have cited any such material correctly; all of the facts contained in the Article are according to the current body of science true and accurate; nothing in the Article is obscene, defamatory, violates any right of privacy or publicity, infringes any other human, personal or other rights of any person or entity or is otherwise unlawful and that informed consent to publish has been obtained for all research participants; nothing in the Article infringes any duty of confidentiality which any of the Author(s) might owe to anyone else or violates any contract, express or implied, of any of the Author(s). All of the institutions in which work recorded in the Article was created or carried out have authorised and approved such research and publication; and the signatory (the Author or the employer) who has signed this agreement has full right, power and authority to enter into this agreement on behalf of all of the Author(s).

6. Cooperation

The Author(s) shall cooperate fully with the Assignee in relation to any legal action that might arise from the publication of the Article, and the Author(s) shall give the Assignee

access at reasonable times to any relevant accounts, documents and records within the power or control of the Author(s). The Author(s) agree that the distributing entity is intended to have the benefit of and shall have the right to enforce the terms of this agreement.

7. Author List

After signing, changes of authorship or the order of the authors listed will not be accepted unless formally approved in writing by the Assignee.

8. Edits and Corrections

The Author(s) agree(s) that the Assignee may retract the Article or publish a correction or other notice in relation to the Article if the Assignee considers in its reasonable opinion that such actions are appropriate from a legal, editorial or research integrity perspective.

B.2 Copyright Information for *A Wilbrink-Like Equation for Neo-Difference Sets*

1. Publication

The copyright to this article, (including any supplementary information and graphic elements therein (e.g. illustrations, charts, moving images) (the 'Article'), is hereby assigned for good and valuable consideration to Springer International Publishing AG, part of Springer Nature (the 'Assignee'), effective with the conclusion of this agreement or the acceptance of the Article for publication, whichever is later. Headings are for convenience only.

2. Grant of Rights

In consideration of the Assignee evaluating the Article for publication, the Author(s) grant the Assignee without limitation the exclusive (except as set out in clauses 3, 4 and 5 a) iv), assignable and sub-licensable right, unlimited in time and territory, to copy-edit, reproduce, publish, distribute, transmit, make available and store the Article, including abstracts thereof, in all forms of media of expression now known or developed in the future, including pre- and reprints, translations, photographic reproductions and extensions. The Assignee may use the Article (including the use of any graphic elements on a stand-alone basis) in

whole or in part in electronic form, such as use in databases or data networks (e.g. the Internet) for display, print or download to stationary or portable devices. This includes interactive and multimedia use as well as posting the Article in full or in part or its abstract on social media, and the right to alter the Article to the extent necessary for such use. The Assignee may also let third parties share the Article in full or in part or its abstract on social media and may in this context sub-license the Article and its abstract to social media users. Author(s) grant to Assignee the right to re-license Article metadata without restriction (including but not limited to author, name title, abstract, citation, references, keywords and any additional information as determined by Assignee).

3. Self-Archiving

Author(s) are permitted to self-archive a pre-print and an author's accepted manuscript version of their Article. a pre-print is the author's version of the Article before peer-review has taken place ("Pre-Print"). Prior to acceptance for publication, Author(s) retain the right to make a Pre-Print of their Article available on any of the following: their own personal, self- maintained website; a legally compliant, non-commercial pre-print server such as but not limited to arXiv and bioRxiv. Once the Article has been published, the Author(s) should update the acknowledgement and provide a link to the definitive version on the publisher's website: "This is a pre-print of an article published in [insert journal title]. The final authenticated version is available online at: https://doi.org/[insert DOI]". An Author's Accepted Manuscript (AAM) is the version accepted for publication in a journal following peer review but prior to copyediting and typesetting that can be made available under the following conditions: Author(s) retain the right to make an AAM of their Article available on their own personal, self- maintained website immediately on acceptance, Author(s) retain the right to make an AAM of their Article available for public release on any of the following 12 months after first publication ("Embargo Period"): their employer's internal website; their institutional and/or funder repositories. AAMs may also be deposited in such repositories immediately on acceptance, provided that they are not made publicly available until after the Embargo Period. An acknowledgement in the following form should be included, together with a link to the published version on the publisher's website: "This is a post-peer-review,

pre-copyedit version of an article published in [insert journal title]. The final authenticated version is available online at: http://dx.doi.org/[insert DOI]".

4. Author's Retained Rights

Author(s) retain the following non-exclusive rights for the published version provided that, when reproducing the Article or extracts from it, the Author(s) acknowledge and reference first publication in the Journal: to reuse graphic elements created by the Author(s) and contained in the Article, in presentations and other works created by them; they and any academic institution where they work at the time may reproduce the Article for the purpose of course teaching (but not for inclusion in course pack material for onward sale by libraries and institutions); to reproduce, or to allow a third party Assignee to reproduce the Article in whole or in part in any printed volume (book or thesis) written by the Author(s).

5. Warranties

The Author(s) warrant and represent that: (i) the Author(s) are the sole owners or have been authorised by any additional copyright owner(s) to assign the rights defined in clause 2, (ii) the Article does not infringe any intellectual property rights (including without limitation copyright, database rights or trade mark rights) or other third party rights and no licence from or payments to a third party are required to publish the Article, (iii) the Article has not been previously published or licensed, (iv) if the Article contains material from other sources (e.g. illustrations, tables, text quotations), Author(s) have obtained written permissions to the extent necessary from the copyright holder(s), to license to the Assignee the same rights as set out in Clause 2 but on a non-exclusive basis and without the right to use any graphic elements on a stand-alone basis and have cited any such material correctly; all of the facts contained in the Article are according to the current body of science true and accurate; nothing in the Article is obscene, defamatory, violates any right of privacy or publicity, infringes any other human, personal or other rights of any person or entity or is otherwise unlawful and that informed consent to publish has been obtained for all research participants; nothing in the Article infringes any duty of confidentiality which any of the Author(s) might owe to anyone else or violates any contract, express or implied, of any of the Author(s), and all of the institutions in which work recorded in the Article was

created or carried out have authorised and approved such research and publication; and the signatory (the Author or the employer) who has signed this agreement has full right, power and authority to enter into this agreement on behalf of all of the Author(s) including where applicable any government entity or the Crown.

6. Cooperation

The Author(s) shall cooperate fully with the Assignee in relation to any legal action that might arise from the publication of the Article, and the Author(s) shall give the Assignee access at reasonable times to any relevant accounts, documents and records within the power or control of the Author(s). The Author(s) agree that the distributing entity is intended to have the benefit of and shall have the right to enforce the terms of this agreement.

7. Author List

After signing changes of authorship or in the order of the authors listed will not be accepted unless formally approved by the Assignee.

8. Edits and Corrections

The Author(s) agree(s) that the Assignee may retract the Article or publish a correction or other notice in relation to the Article if the Assignee considers in its reasonable opinion that such actions are appropriate from a legal, editorial or research integrity perspective.