5-2023

Exploring the Structure of Partial Difference Sets With Denniston Parameters

Nicolas Ferree

Exploring the Structure of Partial Difference Sets With Denniston Parameters

Nicolas Ferree

Honors Thesis

Submitted to:

Department of Mathematics and Statistics
University of Richmond
Richmond, VA

April 28, 2023

Advisor: Dr. Jim Davis

1 Introduction

Partial difference sets are algebraic objects that lie at the intersection of algebra, combinatorics, geometry, graph theory, and coding theory. In addition to being a natural way to explore the connections between these fundamental areas of discrete mathematics, partial difference sets have many useful applications. The properties of difference sets are useful in constructing and understanding error correcting codes, which are of fundamental importance to any kind of reliable, long range digital communication as well as to the storage of such data. (For example, error correcting codes are used in satellite communications, video streaming, and encoding data onto CDs). Other uses include precise alignment of physical objects and providing a way to measure radar distances with high levels of precision [1, 5].

Furthermore, each partial difference set immediately provides a construction of a strongly regular graph. Since strongly regular graphs are some of the most symmetric graphs that can be constructed, they have very simple adjacency matrices. For this reason, they are of great interest in the widely studied field of graph theory [9]. Furthermore, strongly regular graphs are useful objects for constructing and understanding association schemes, which are a generalization of error correcting codes [6].

Despite their importance, many questions remain about partial difference sets. While some constructions are known, many partial difference sets (particularly those in non-abelian groups) have been found only through computer search. A deeper understanding of the nature of these objects is a rich problem with application to several branches of mathematics.

In this work, we investigate the structure of particular partial difference sets (PDS) of size 70 with Denniston parameters in an elementary abelian group and in a non-elementary abelian group. We will make extensive use of character theory in our investigation and ultimately seek to understand the nature of difference sets with these parameters. To begin, we will cover some basic definitions and examples of difference sets and partial difference sets. We will then move on to some basic theorems about partial difference sets before introducing a group ring formalism and using it to explore several important constructions of partial difference sets. Finally, we will conclude our introduction by developing the character theory that we will exploit to understand our partial difference sets.

1.1 Basic Definitions

We begin our discussion by defining a difference set. These objects are closely related to partial difference sets, but are somewhat simpler to understand.

Definition 1.1 (Difference Set)**.** A (v, k, λ) difference set D is a subset of a group G of order such that $|G| = v, |D| = k$, and the multiset of pairwise differences $\Delta = \{d_1 - d_2 \,|\, d_1, d_2 \in D, d_1 \neq d_2\}$ contains every nonidentity element of G exactly λ times.

Example 1.1. Consider the group $G = \mathbb{Z}_7$ and the subset $D = \{1, 2, 4\}$. Notice that $1-2 = 6, 1-4 = 4, 2-1 = 1, 2-4 = 5, 4-1 = 3, 4-2 = 2$. Therefore $\Delta = \{1, 2, 3, 4, 5, 6\}$, so D is a $(7, 3, 1)$ difference set in $\mathbb{Z}_7$.

Example 1.2. Consider the group $G = \mathbb{Z}_2^4$ and the subset

$$D = \{(0,0,1,1),(1,0,1,1),(0,1,1,1),(0,0,0,1),(0,0,1,0),(1,1,0,0)\}.$$

Computing all of the pairwise differences shows us that Δ contains two copies of each nonidentity element of $\mathbb{Z}_2^4$, so D is a $(16,6,2)$ difference set in $\mathbb{Z}_2^4$.

The $(16,6,2)$ difference set in the example above is a difference set from a family called the Hadamard difference sets. A Hadamard difference set is a (v,k,λ) difference set with the property that $v = 4(k-\lambda)$. It can be shown that for any Hadamard difference set, there exists a positive integer m such that the set is a $(4m^2, 2m^2-m, m^2-m)$ difference set. We note that the converse is an open question: given some integer m, is there a$(4m^2, 2m^2-m, m^2-m)$ difference set? It is known that such a difference set exists if m is a power of two, but the general existence has not been proven [2, 8, 12].

The Hadamard difference sets are a very well studied example of an infinite family of difference sets. For a more thorough treatment, see [2, 12].

As we can see, difference sets are highly regular objects and therefore have greatly restricted structures. To loosen these restrictions while preserving interesting structural properties (particularly those related to combinatorial objects), we define a related but somewhat less restrictive object: a partial difference set.

Definition 1.2 (Partial Difference Set)**.** A (v,k,λ,μ) partial difference set D is a subset of a group G such that $|G| = v, |D| = k$, and the multiset of pairwise differences $\Delta = \{d_1 - d_2 \,|\, d_1, d_2 \in D, d_1 \neq d_2\}$ contains every nonidentity element of D exactly λ times and every nonidentity element of $G \setminus D$ exactly μ times.

Example 1.3. Consider the group $\mathbb{Z}_5$ and the set $D = \{1,4\}$. Notice that $4-1=3$ and $1-4=2$, so $\Delta = \{2,3\}$. This contains each nonzero element of $G \setminus D$ exactly once and each nonzero element of D exactly zero times, so D is a $(5,2,0,1)$ PDS in $\mathbb{Z}_5$.

Example 1.4. Consider the group $\mathbb{Z}_{13}$ and the subset $D = \{1,4,9,3,12,10\}$. Straightforward computation will show that the multiset of pairwise differences $\Delta = \{d_1 - d_2 | d_1, d_2 \in D, d_1 \neq d_2\}$ contains every nonidentity element of $G \setminus D$ exactly 3 times and every nonidentity element of D exactly 2 times. Therefore D is a $(13,6,2,3)$ PDS in $\mathbb{Z}_{13}$.

In fact, both of the partial difference sets presented above are members of an infinite family of partial difference sets called the Paley squares [11]. It may be shown that in any group $\mathbb{Z}_p$ where p is a prime that is 1 mod 4, the set of elements $\{a^2 | a \neq 0, a \in G\}$ is a partial difference set with parameters $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$ [6]. For a proof that this is a partial difference set, see theorem 6.2 in the appendix.

Example 1.5. Consider the group $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ and the set $D = \{(1,0),(2,0),(0,1),(0,2)\}$. Computing the pairwise differences shows us that Δ contains every nonzero element of $G \setminus D$ exactly twice and every element of D exactly once. Therefore D is a $(9,4,1,2)$ PDS in $\mathbb{Z}_3 \times \mathbb{Z}_3$. Not only is this a Paley partial difference set (it is the set of squares in G), it is also the union of two subgroups (each missing the identity). This is a type of PDS called a partial congruence partition; we will return to this construction later.

1.2 Basic Theorems

Now that we have defined partial difference sets and seen some typical examples of these structures, we will develop some basic theorems that require no formalism beyond these definitions. We conclude this subsection by presenting a method that allows for construction of a strongly regular graph from a given PDS; this one motivation to discover and characterize more partial difference sets.

We begin by discussing trivial partial difference sets in order to become more familiar with the definition of a PDS and as an exercise in the basic style of manipulations that will be used throughout this work.

Theorem 1.1. If G is a finite group of order v, then G is a $(v, v, v, 0)$ partial difference set [6].

Proof: By hypothesis, G has v elements. Thus v and k must be equal to v. The group is closed under its binary operation, so no binary operation $d_1d_2^{-1}$, where $d_1, d_2 \in G$, can produce an element outside of G. Thus μ must be zero.

Let $a \in G$. Then $g = (ga)(a)^{-1}$, so $d_1 = ga$, $g_2 = a$ is a solution pair of $d_1d_2^{-1} = g$ for each $a \in G$. Since each $a \in G$ is distinct, we can find v distinct solutions of this form. Therefore there are at least v distinct solutions to this equation.

Suppose that there exists a $(v{+}1)^{\text{th}}$ distinct solution to this equation, $d_1d_2^{-1} = g$, where $d_1, d_2 \in G$. But since $d_2 \in G$, we also have a solution of the form above corresponding to d_2: we have shown that $d_1' = (gd_2)$ gives a solution pair (d_1', d_2). Then it follows that $g = d_1'd_2^{-1} = d_1d_2^{-1}$. Right multiplying by d_2, we find that $d_1' = d_1$. Then d_1, d_2 is the same as the solution above corresponding to d_2, so it is not distinct. This is a contradiction, so there are at most v distinct solutions.

Therefore there are exactly v distinct solutions to the equation $d_1d_2^{-1}$. This is true for any element of G, so $\lambda = v$. □

Note that this result implies that G is also a trivial example of a difference set. We now discuss another example of a trivial PDS (that is also a trivial difference set).

Theorem 1.2. If G is a finite group of order v, then $D = G \setminus \{e\}$ is a $(v, v-1, v-2, 0)$ partial difference set [6].

Proof: By hypothesis, G has v elements. Thus the first parameter must be equal to v. Since only one element of G is not in D, there are $v - 1$ elements of D. Therefore $k = v - 1$. The group is closed under its binary operation, so no binary operation $d_1d_2^{-1}$, where $d_1, d_2 \in G$, can produce an element outside of G. Thus $d_1d_2^{-1}$ is either an element of D or it is the identity element, so every non-identity element is in D. Therefore μ must be zero.

Let $g \in G, g \neq e$ and let $a \in G, a \neq e, a \neq g^{-1}$. Then $g = (ga)(a)^{-1}$. Let $d_1 = ga$ and $d_2 = a$. Thus (d_1, d_2) is a solution pair of $d_1d_2^{-1} = g$ for all $a \in G, a \neq e, a \neq g^{-1}$. Furthermore, we know that $d_1, d_2 \in D$. Since $g \neq e$, we know that $g^{-1} \neq e$ and therefore $g^{-1} \in D$. Thus the restriction $a \neq e, a \neq g^{-1}$ excludes one element of D. But there are $v - 2$ other distinct elements of D, so there are at least $v - 2$ distinct choices for d_2 and therefore $v - 2$ distinct solutions to the equation $d_1d_2^{-1} = g$.

Suppose that there exists a $(v{-}1)^{\text{th}}$ distinct solution to this equation, $d_1d_2^{-1} = g$, where $d_1, d_2 \in D$. But since $d_2 \in D$, we also have a solution of the form above corresponding to d_2: we have shown that $d_1' = (gd_2)$ gives a solution pair (d_1', d_2). Then it follows that $g = d_1'd_2^{-1} = d_1d_2^{-1}$. Right multiplying by d_2, we find that $d_1' = d_1$. Then d_1, d_2 is the same as the solution above corresponding to d_2, so it is not distinct. This is a contradiction, so there are at most $v - 2$ distinct solutions.

Therefore there are exactly $v - 2$ distinct solutions to the equation $d_1d_2^{-1}$, where $d_1, d_2 \in D$. This is true for any element of D, so $\lambda = v - 2$. □

Next, we will prove a theorem of great computational and theoretical importance.

Theorem 1.3. Let D be a (v, k, λ, μ) be a partial difference set in a group G where $\lambda \neq \mu$. Define $D^{(-1)} = \{d^{-1} | d \in D\}$. Then $D = D^{(-1)}$ [6].

Proof: Let $g \in G$ and note that $d_1 d_2^{-1} = g$ if and only if $d_2 d_1^{-1} = g^{-1}$. Then the number of solution pairs (d_1, d_2) to the equation $d_1 d_2^{-1} = g$ is equal to the number of solution pairs (d_1', d_2') to the equation $d_1'(d_2')^{-1} = g^{-1}$. Then the number of differences of elements of D that yield g (call this number n) is equal to the number of differences of elements of D that yield g^{-1} (call this number n'). That is, $n = n'$. Since $n, n' \in \{\mu, \lambda\}$ by definition of a PDS and $n = n'$, it follows that either $n = n' = \mu$ and thus $g, g^{-1} \in D$ or $n = n' = \lambda$ and $g, g^{-1} \in G \backslash D$. Therefore $g \in D$ if and only if $g^{-1} \in D$, so $D = D^{(-1)}$. □

Note the computational value of this theorem: the fact that D is closed under inversion means that the set $\{d_1 d_2^{-1} | d_1, d_2 \in D\}$ is equal to the set $\{d_1 d_2 | d_1, d_2 \in D\}$. This is an easier condition to check, and its extreme usefulness will become immediately apparent when we introduce a group ring formalism.

This theorem is also of great theoretical use when attempting to construct a new PDS by taking the union of various subsets D_i. We know that the entire PDS must be closed under inversion, so we may guarantee this property if we choose the D_i such that they themselves are each closed under inversion. If a set D_i is closed under inversion, we call it reversible.

Definition 1.3 (Reversible)**.** A subset S of a group G is called reversible if it satisfies the property that $S = S^{(-1)}$, where we define $S^{(-1)} = \{s^{-1} | s \in S\}$.

Finally, we connect the existence of partial difference sets to the existence of strongly regular graphs.

Theorem 1.4. Let G be a group and let $D \subseteq G$ be a (v, k, λ, μ) partial difference set where $\lambda \neq \mu$. Then there is a strongly regular graph corresponding to D.

Proof: We will construct a graph from D as follows. For each $g \in G$, create a vertex on the graph and label it g. For two vertices x and y, connect x to y if and only if $xy^{-1} \in D$.

We have proven that $\lambda \neq \mu$ implies that $D = D^{-1}$. Thus if $xy^{-1} \in D$, we have that $(xy)^{-1} = yx^{-1} \in D$. Likewise, $yx^{-1} \in D$ implies that $xy^{-1} \in D$. Therefore x is connected to y if and only if y is connected to x. Thus our construction must generate a graph, not a digraph, and we can simplify our connected criterion to say that x is connected to y if and only if $xy^{-1} \in D$.

Now suppose that x, y, z are vertices in our graph. Then z is a common neighbor of x, y if and only if $xz^{-1} \in D$ and $yz^{-1} \in D$.

Let $(d_1, d_2) \in D \times D$ be a solution pair of the equation $d_1 d_2^{-1} = xy^{-1}$. Define $z_1 = d_1^{-1} x$ and $z_2 = d_2^{-1} y$, so $d_1 = x_1^{-1}$ and $d_2 = yz_2^{-1}$.

It therefore follows that

$$\begin{aligned} xy^{-1} &= d_1 d_2^{-1} \\ xy^{-1} &= (xz_1^{-1})(yz_2)^{-1} \\ xy^{-1} &= xz_1^{-1} z_2 y^{-1}. \end{aligned}$$

By left and right cancellation, we have that $z_1^{-1} z_2 = 1$. Since inverses are unique, it follows that $z_1 = z_2$.

Then we may say $z = z_1 = z_2$. Define a function f that maps the set of solution pairs $(d_1, d_2) \in D \times D$ of $d_1 d_2^{-1} = xy^{-1}$ to the set of vertices of the graph by $f(d_1, d_2) = d_1^{-1}x = d_2^{-1}y$. Thus for any solution pair (d_1, d_2), we have that $z = f(d_1, d_2) = d_1^{-1}x = d_2^{-1}y$ simultaneously satisfies $xz^{-1} \in D, yz^{-1} \in D$. Thus z is a common neighbor of x and y.

Conversely, suppose that z is a common neighbor of x and y. Then define $d_1 = xz^{-1} \in D$, $d_2 = yz^{-1} \in D$ (they must both be in D by definition of z being a common neighbor of x and y). Then $d_1 d_2^{-1} = xy^{-1}$, so every common neighbor z can be generated by a solution pair (d_1, d_2). That is, for every common neighbor z of x and y, there is a $(d_1 = xz^{-1}, d_2 = yz^{-1})$ such that $f(d_1, d_2) = z$.

We have therefore found that $z = f(d_1, d_2) = d_1^{-1}x$ is a mapping from the set of solutions $(d_1, d_2) \in D \times D$ of the equation $d_1 d_2^{-1} = xy^{-1}$ onto the set of vertices z that are common neighbors of x and y.

Suppose that there exist $z \in G$, $(d_1, d_2), (d_1', d_2') \in D \times D$ such that $z = f(d_1, d_2) = f(d_1', d_2') = d_1^{-1}x = d_1'^{-1}x$. Then right multiplication by x^{-1} shows that $d_1^{-1} = d_1'^{-1}$. Since the inverse is unique, it follows that $d_1 = d_1'$. Thus f is one to one.

We have therefore produced a bijection from the set of solutions $(d_1, d_2) \in D \times D$ of $d_1 d_2^{-1} = xy^{-1}$ onto the set of vertices z that are common neighbors of x and y. Thus the number of distinct common neighbors of x and y must be equal to the number of distinct solutions $(d_1, d_2) \in D \times D$ of $d_1 d_2^{-1} = xy^{-1}$.

But we know that $x \neq y$ and that the inverse is unique, so $y^{-1} \neq x^{-1}$. Thus $xy^{-1} \neq e$. Then, by definition of a partial difference set, the number of solutions $(d_1, d_2) \in D \times D$ of $d_1 d_2^{-1} = xy^{-1}$ depends only upon whether $xy^{-1} \in D$. Furthermore, $xy^{-1} \in D$ if and only if x and y are connected. Thus the number of solutions (d_1, d_2) depends only whether or not x and y are connected. We therefore conclude that the number of distinct common neighbors of x and y is dependent only on whether or not x and y are connected, which is the definition of our graph being strongly regular. □

1.3 Group Rings

We will now introduce the notion of a group ring and then use it to prove several important theorems.

Definition 1.4 (Group Ring)**.** Let G be a group (under multiplication) and let R be a ring. The group ring of G over R (denoted $R[G]$) is the set of mappings $f(g) : G \to R$ of finite support, where we define scalar multiplication by $\alpha \in R, f \in R[G]$ by $x \to \alpha f(x)$, the addition operation of the ring by $f + g$ by $(f + g)(x) = f(x) + g(x)$, and $(fg)(x) = \sum_{ab=x} f(a)g(b)$.

Said less formally: let G be a group and R be a ring. Then the group ring $R[G]$ is the ring of finite polynomials whose scalar coefficients come from the ring R and whose variables come from the group G. The addition and multiplication operations of $R[G]$ are defined as usual for a polynomial ring: addition is defined by adding the scalar coefficients using the addition of R for each element of G and multiplication is defined by a distributive law where scalar multiplication uses the multiplication of R and variable multiplication uses the group operation of G. (To see how this is equivalent to the above definition, we need only note that the mapping from G to R simply defines a list of coefficients. A polynomial may also be thought of as a list of coefficients, so we may switch between these two ways of thinking about a group ring).

To write this out explicitly, we note that any element two elements $x, y \in R[G]$ may be written $x = \sum_{g_1 \in G} a_{g_1} g_1, y = \sum_{g_2 \in G} b_{g_2} g_2$, where $a_{g_1}, b_{g_1} \in R$. Then we may define $x + y = \sum_{g_1 = g_2 = g \in G} (a_g + b_g) g$ and $xy = \sum_{g_1 g_2 = g} (a_{g_1} b_{g_2}) g$, where the group operation of G is denoted multiplicatively. The structure of R and G make it a relatively simple exercise to show that $R[G]$ is in fact a ring.

We should note that although the elements of $R[G]$ are finite polynomials, G need not be a finite group. So long as $x, y \in R[G]$ have finitely many nonzero coefficients, $x + y$ and xy also have finitely many nonzero coefficients.

We also note that no part of our definition requires G to be an abelian group; this construction is completely general.

Example 1.6. Consider the group $G = \{x^n | n \in \mathbb{Z}\}$, where $x^a x^b = x^{a+b}$ and the ring $R = \mathbb{Z}$. Then $R[G]$ is the ring of all finite polynomials with integer coefficients and integer powers with the familiar addition and multiplication operations of ordinary real polynomials. Note that in this example, both our group G and ring R are infinite.

Example 1.7. Consider the group $G = \langle x | x^5 = 1 \rangle$ where the ring $R = \mathbb{Z}_3$. As an example, consider the elements $a = x + 2x^2 + x^3, b = x + x^2$. Then $a + b = (0+0)1 + (1+1)x + (2+1)x^2 + (1+0)x^3 + (0+0)x^4 + (0+0)x^5 = 2x + x^3$ and

$$\begin{aligned} ab &= (x + 2x^2 + x^3)(x + x^2) \\ &= (1 * 1)(x * x) + (1 * 1)(x * x^2) + (2 * 1)(x^2 * x) + (2 * 1)(x^2 * x^3) \\ &+ (1 * 1)(x^3 * x) + (1 * 1)(x^3 * x^5) \\ &= x^2 + x^3 + 2x^3 + 2x^5 + 1x^4 + 1x^8 \\ &= x^4 + x^3 + x^2 + 2. \end{aligned}$$

Note that in this example, both R and G are finite.

Example 1.8. Consider the group $G = D_4$, the dihedral group of order eight. We notate a vertical flip by V, a horizontal flip by H, the diagonal flips by D and D', and a rotation by x degrees by R_x.

Let $R = \mathbb{Z}_2$. Then $a = H + V$, $b = H + R_{90}$ yields $a + b = V + R_{90}$ and $ab = (H + V)(H + R_{90}) = H^2 + HR_{90} + VH + VR_{90} = R_0 + D + R_{180} + D'$. Note that in this example, our group is non-Abelian and the order of the multiplication in our distributive law is therefore important.

Remark. When switching between the language of sets and group rings, we will often abuse notation in order to simplify the presentation of our arguments. In the case where we are considering a group ring $\mathbb{Z}[G]$, it is to be understood from context whether G denotes the set of group elements or their sum in the group ring, $G = \sum_{g \in G} g$. The frequent abuse of this notation in the context of partial difference sets is largely due to the fact that when we analyze a set S, we often wish to take all differences between S and some other set D. By considering S and D as sums in a group ring, the notation $SD^{(-1)}$ allows for a compact way to count the number of times that group elements appear when we take all possible differences: the group ring element $SD^{(-1)}$ has coefficients that correspond to counts of each group element in the multiset $\{sd^{-1} | s \in S, d \in D\}$.

With this understanding, let us now use group rings to explore partial difference sets.

First, we will discuss how group rings provide a natural language to formulate the definitions of difference sets and partial difference sets. A difference set D in a group G is a set such that all pairwise differences of elements of D yield all non-identity elements of G exactly λ times. We note that the identity will occur exactly k times, where $|D| = k$ (it appears once for each element of D, since $dd^{-1} = 1_G$). In the language of group rings, this condition is succinctly written

$$DD^{(-1)} = \lambda(G - 1_G) + k1_G. \tag{1}$$

Similarly, a partial difference set D in a group G is a set such that all pairwise differences of elements of D yield the non-identity elements of D exactly λ times and the non-identity elements of $G \setminus D$ exactly μ times. Again, 1_G will appear k times. This condition may be written

$$DD^{(-1)} = \lambda D + \mu(G - D - 1_G) + k1_G. \tag{2}$$

(Here, we have assumed that $1_G \notin D$; we note that we may always assume this because the complement of a PDS is itself a PDS. This fact will be shown shortly. A similar condition may be written down for a PDS containing the identity).

Given this group ring formulation of a PDS, we will now prove several important theorems.

Lemma 1.5. Let G be a finite group of order v and let S be a subset of G with s' elements. Then, switching to group ring notation, we have that $SG = sG$.

Proof: We know that $G = \sum_{g \in G} g$. Let $S = \sum_{s \in S} s$. Then $SG = \sum_{sg = g' \in G} g'$. But for any $s \in S$, we know that $sg \in G$ by closure. Furthermore, uniqueness of inverses means that $sg = g'$ has only one solution for fixed s, g'. Then, in the group ring, we have that $sG = G$ for all $s \in S$. Since $S = \sum_{s \in S} s$, we have that $SG = \sum_{s \in S} sG = \sum_{s \in S} G = |S|G = s'G$. □

Corollary 1.5.1. If G is a finite group of order v and D is a subset of G with k elements, then it follows that $G^2 = vG$ and that $GD = DG = kG$.

We will now prove an important theorem: namely, that the complement of a partial difference set is itself a partial difference set.

Theorem 1.6. If D is a (v, k, λ, μ) partial difference set that is closed under inversion, then $G \setminus D = D'$ is a $(v, v - k, v + \mu - 2k, v + \lambda - 2k)$ partial difference set.

Proof: If D is closed under inversion, then D' is also closed under inversion (since inverses in a group are unique and $D \cap D' = \varnothing$). Therefore $D'D'^{-1} = D'^2$.

Let 1_G be the identity element of G. Suppose that $1_G \notin D$. Then we have that $D^2 = k(1) + \lambda D + \mu(G - D - 1_G)$. Furthermore, we know that $D = G - D'$, so:

$$\begin{aligned}
D'^2 &= (G-D)(G-D) \\
&= G^2 - GD - DG + D^2 \\
&= vG - 2kG + k(1_G) + \lambda D + \mu(G - D - 1_G) \\
&= (v-2k)G + k(1_G) + \lambda D + \mu(G - D - 1_G) \\
&= (v-2k)(G - 1_G + 1_G) + k(1_G) + \lambda D + \mu(G - D - 1_G) \\
&= (v - 2k + k)(1_G) + (v-2k)(G - 1_G) + \lambda D + \mu(G - D - 1_G) \\
&= (v-k)(1_G) + (v-2k)(G-1_G) + \lambda(G - D') + \mu(D' - 1_G) \\
&= (v-k)(1_G) + (v-2k)(G-1_G) + \lambda(G - 1_G + 1_G - D') + \mu(D' - 1_G) \\
&= (v-k)(1_G) + (v+\lambda-2k)(G-1_G) - \lambda(D' - 1_G) + \mu(D' - 1_G) \\
&= (v-k)(1_G) + (v+\lambda-2k)(G-1_G) + (v+\lambda-2k)D' - (v+\lambda-2k)D' \\
&- \lambda(D' - 1_G) + \mu(D' - 1_G) \\
&= (v-k)(1_G) + (v+\lambda-2k)(G - D') + (v+\lambda-2k)(D' - 1) + (\mu-\lambda)(D' - 1_G) \\
&= (v-k)(1_G) + (v+\lambda-2k)(G - D') + (v+\mu-2k)(D' - 1_G)
\end{aligned}$$

Since $1_G \in D'$, this shows that D' is a $(v, v-k, v+\mu-2k, v+\lambda-2k)$ PDS.

Now suppose that $1_G \in D$. Then we have that $D^2 = k(1_G) + \lambda(D - 1_G) + \mu(G - D)$. Thus:

$$\begin{aligned}
D'^2 &= (G-D)(G-D) \\
&= G^2 - GD - DG + D^2 \\
&= vG - 2kG + k(1_G) + \lambda(D - 1_G) + \mu(G - D) \\
&= (v-2k)G + k(1_G) + \lambda(D - 1_G) + \mu(G - D) \\
&= (v-2k)(G - 1_G + 1_G) + k(1_G) + \lambda(D - 1_G) + \mu(G - D) \\
&= (v-2k+k)(1_G) + (v-2k)(G - 1_G) + \lambda(D - 1_G) + \mu(G - D) \\
&= (v-k)(1_G) + (v-2k)(G-1_G) + \lambda(G - D' - 1_G) + \mu D' \\
&= (v-k)(1_G) + (v-2k)(G-1_G) + \lambda(G - 1_G) - \lambda D' + \mu D' \\
&= (v-k)(1_G) + (v+\lambda-2k)(G-1_G) - \lambda D' + \mu D' \\
&= (v-k)(1_G) + (v+\lambda-2k)(G-1_G) + (v+\lambda-2k)D' - (v+\lambda-2k)D' \\
&- \lambda D' + \mu D' \\
&= (v-k)(1_G) + (v+\lambda-2k)(G - D' - 1_G) + (v+\lambda-2k)D' + (\mu-\lambda)D' \\
&= (v-k)(1_G) + (v+\lambda-2k)(G - D' - 1_G) + (v+\mu-2k)D'
\end{aligned}$$

Since $1_G \notin D'$, this shows that D' is a $(v, v-k, v+\mu-2k, v+\lambda-2k)$ PDS. □

In addition to automatically giving us another PDS whenever we construct a new PDS, this theorem has another important application. Whenever we have a (v, k, λ, μ) partial difference set D in a group G, we may assume that the identity element is not contained in D. If it is, we know that the identity is not contained in the complement D', which is a (v', k', λ', μ') PDS. We may then relabel the primes, thereby eliminating the identity element from the partial difference set of interest.

Another use of this theorem is to let us choose to work with a PDS with $k \leq \frac{v}{2}$. Given a PDS with $k > \frac{v}{2}$, we know that its complement is also a PDS and must have $k < \frac{v}{2}$. We may then work with this PDS instead.

Finally, since the language of group rings gives us a natural way to express counts, we may find a useful expression for the parameter k. This will place a useful constraint on possible parameters of partial difference sets.

Theorem 1.7. Suppose that D is a (v, k, λ, μ) PDS in the group G and that D does not contain the identity. Then $k^2 = \lambda k + \mu(v - k - 1) + k$.

Proof: By definition of a partial difference set, we know that $DD^{(-1)} = \lambda D + \mu(G - D - 1_G) + k1_G$. Furthermore, since $D, G \setminus D \setminus \{1_G\}$, and $\{1_G\}$ are disjoint sets, it follows that $|DD^{(-1)}| = \lambda|D| + \mu|G - D - 1_G| + k|1_G|$, so $k^2 = \lambda k + \mu(v - k - 1) + k$. □

Remark. We note that the same reasoning may be applied to show that if $e \in D$, then $k^2 = \lambda(k - 1) + \mu(v - k) + k$. One may check that this is consistent with the above requirements that $k' = v - k, \lambda' = v + \mu - 2k, \mu' = v + \lambda - 2k$ for a (v, k, λ, μ) PDS and its complement, which is a (v, k', λ', μ') PDS.

1.4 Partial Congruence Partitions

We will now introduce our first major method of constructing partial difference sets. This method, called the partial congruence partition, allows us to construct a generalization of the PDS presented in example 1.5. We will begin with another example, followed by two lemmas.

Example 1.9. Consider the group $\mathbb{Z}_4 \times \mathbb{Z}_4$. Define

$$D = \{(1, 0), (2, 0), (3, 0), (0, 1), (0, 2), (0, 3), (1, 1), (2, 2), (3, 3)\}.$$

This is a $(16, 9, 4, 6)$ partial difference set. Note that it is the union of three disjoint subgroups (each missing the identity).

The construction of this PDS from disjoint subgroups may be generalized. To see how, we will begin with two lemmas.

Lemma 1.8. Let H_1, H_2 be subgroups of G, where H_1, H_2 are of order n and G is of order n^2. If $H_1 \cap H_2 = \{e\}$, then $H_1H_2 = G$.

Proof: Denote $H_1 = 1 + x_1 + x_2 + ... + x_{n-1}$ and $H_2 = 1 + y_1 + ... + y_{n-1}$. Then

$$
\begin{aligned}
H_1H_2 = (1+x_1+...+x_{n-1})&(1+y_1+...+y_{n-1}) \\
&= 1(1+y_1+...+y_{n-1}) \\
&+ x(1+y_1+...+y_{n-1}) \\
&+ ... \\
&+ x_{n-1}(1+y_1+...+y_{n-1}) \\
&= (1+y_1+...+y_{n-1}) \\
&+ (x+x_1y_1+...+x_1y_{n-1}) \\
&+ ... \\
&+ (x_{n-1}+x_{n-1}y_1+...+x_{n-1}y_{n-1}).
\end{aligned}
$$

Clearly, we have n^2 elements in this sum. Since H_1, H_2 are subgroups of G, each element in the sum is an element of G. Thus, if the elements are all distinct, the sum must be equal to G.

Observe that each element in the sum can be written x_iy_j, where $0 \leq i, j < n$. Suppose that we have $x_iy_j = x_ky_m$, where $0 \leq i, j, k, m < n$. Then it follows that $x_ix_k^{-1} = y_my_j^{-1}$.

But since each element has an inverse in the group and groups are closed, it must be true that $x_ix_k^{-1} \in H_1$ and $y_my_j^{-1} \in H_2$. Therefore $x_ix_k^{-1} = y_my_j^{-1} \in H_1 \cap H_2 = \{e\}$, so $x_ix_k^{-1} = y_my_j^{-1} = e$. Thus $i = k$ and $m = j$ (since inverses are unique).

Since no two elements x_iy_j and x_ky_m have both $i = k$ and $m = j$, they are all distinct. Then our sum has n^2 distinct elements of the group, so it must be the entire group. Therefore $H_1H_2 = G$. □

Lemma 1.9. *Let H be a subgroup of G. If H is of order n and G is of order n^2, then $H^2 = nH$.*

Proof: We can write H as $H = 1+x_1+...+x_{n-1}$ (where $x_0 = 1$). Then for $0 \leq i < n$, we have that $x_iH = x_i + x_ix + ... + x_ix_{n-1}$. Each element in this sum is in H since the group is closed. Furthermore, each element in the sum is distinct. Suppose not: then there are $0 \leq j, k < n$ where $j \neq k$ but $x_ix_j = x_ix_k$. Then $x_j = x_k$, which is a contradiction. Therefore $x_iH = H$.

Then $H^2 = (1+x+...+x_{n-1})H = H+H+...+H = nH$. □

We are now equipped to prove the existence of the partial congruence partition PDS.

Theorem 1.10. *If G is a group of order n^2 and $H_1, ..., H_m$ are subgroups of G of order n such that $H_i \cap H_j = \{e\}$ for all $1 \leq i, j \leq m$, then $D = (H_1 \cup H_2 \cup ... \cup H_m) \setminus \{e\}$ is an $(n^2, m(n-1), n+m^2-3m, m^2-m)$ PDS.*

Proof: The group has order n^2 by hypothesis. Similarly, there are $n-1$ nonidentity elements in each subgroup H_i for $1 \leq i \leq m$. Since the subgroups intersect only at the identity, no elements are repeated. Therefore each of the m groups contributes precisely $n-1$ elements to D, so D has $m(n-1)$ distinct elements.

We will prove the rest of the parameters using the group ring formalism.

We wish to examine all pairwise differences in D, so we are interested in $DD^{(-1)}$. However, D is a union of subgroups minus the identity. Each element of a subgroup has an inverse in the subgroup; since inverses are unique and the identity is its own inverse, each nonidentity element of the subgroup has inverse that is another nonidentity element of the subgroup. Therefore each element of D must also have an inverse in D, so $D^{(-1)} = D$. Thus $DD^{(-1)} = D^2$.

Then we have that

$$\begin{aligned}
D^2 &= ((H_1 - 1) + (H_2 - 1) + ... + (H_m - 1))^2 \\
&= (H_1 + H_2 + ... + H_m - m)(H_1 + H_2 + ... + H_m - m) \\
&= (H_1 + ... + H_m)(H_1 + ... + H_m - m) - m(H_1 + ... + H_m - m) \\
&= (H_1 + ... + H_m)^2 - m(H_1 + ... + H_m) - m(H_1 + ... + H_m) + m^2 \\
&= (\sum_{1\leq i,j\leq m} H_iH_j) - 2m(H_1 + ... + H_m) + m^2 \\
&= (\sum_{1\leq i\leq m} H_i^2) + (\sum_{i\neq j} H_iH_j) - 2m(H_1 + ... + H_m) + m^2 \\
&= \sum_{1\leq i\leq m} nH_i + \sum_{i\neq j} G - 2m(H_1 + ... + H_m) + m^2 \\
&= n(H_1 + ... + H_m) + m(m-1)G - 2m(H_1 + ... + H_m) + m^2 \\
&= (n - 2m)(H_1 + ... + H_m) + m(m-1)G + m^2.
\end{aligned}$$

Then we may see that each element of the group appears $m^2 - m$ times in the second term. The nonidentity elements that are not in D do not appear in any other terms, so $\mu = m^2 - m$. The elements of G each appears $n - 2m$ times in the first term, so $\lambda = m^2 - m + n - 2m = n + m - 3m^2$.

The identity element appears m times in $H_1 + ... + H_m$, so the first term contains $m(n - 2m)$ copies of the identity. Similarly, the second term contains $m^2 - m$ copies of the identity and the third term contains m^2 copies, so e appears a total of $mn - 2m^2 + m^2 - m + m^2 = m(n - 1)$ times. This is the same as the k parameter, as expected.

Therefore D is an $(n^2, m(n-1), n + m^2 - 3m, m^2 - m)$ PDS. □

1.5 Character Theory

We will now introduce character theory, which is an incredibly powerful tool to understand partial difference sets in finite abelian groups. We begin by defining a character.

Definition 1.5 (Character)**.** For a finite abelian group G, a character χ on G is a group homomorphism that maps G to the complex numbers $\mathbb{C}$ under multiplication.

In any finite group, all elements must have finite order. Then the images under homomorphism must also have finite order. We note that the only complex numbers with finite order under multiplication are the roots of unity. We remind the reader of this definition below.

Definition 1.6 (Roots of Unity)**.** A complex number $x \in \mathbb{C}$ is an nth root of unity if $x^n = 1$.

Writing $x \in \mathbb{C}$ as a complex exponential allows us to see that every nth root of unity can be written as $e^{\frac{2\pi ik}{n}}$, where $k \in \mathbb{Z}_n$.

One example of such a homomorphism is the principal character.

Definition 1.7 (Principal Character)**.** Given a group G, the principal character χ is the homomorphism $\chi : G \to \mathbb{C}$ by $\chi(g) = 1$ for all $g \in G$.

A natural question is: how many distinct characters are there in a given finite abelian group? Fortunately, this is a relatively straightforward question to answer; it follows directly from the fundamental theorem of finite abelian groups and simple homomorphism properties.

Theorem 1.11. Given a finite abelian group with generators $g_1, ..., g_k$ with orders $n_1, ..., n_k$, there are $n_1...n_k$ distinct characters.

Proof: To define a homomorphism $\chi : G \to \mathbb{C}$ on a group G, we need only define how the homomorphism acts on the generators.

Consider the generator g_i. Then, since the order of g_i is n_i, we know that $g_i^{n_i} = e_1$. Thus, by properties of a homomorphism, it follows that $1 = \chi(e_1) = \chi(g_i^{n_i}) = \chi(g_i)^{n_i}$. Then the possible images of the generator are the n_ith roots of unity, of which there are n_i.

Since there are n_i choices for each generator and the choices are independent, the total number of distinct characters is equal to the product $n_1...n_k$. □

Indeed, this analysis motivates a stronger theorem.

Theorem 1.12. Given a finite abelian group G, the set of characters X considered under the operation $\circ$ defined by $(\alpha \circ \beta)(u) = \alpha(u)\beta(u)$ forms a group isomorphic to G.

Proof: A finite Abelian group can be written as a direct product of cyclic groups of prime order. Denote these cyclic groups G_i. Let each generator g_i of group G_i be of order n_i.

Then a homomorphism is determined by the images of the generators under the homomorphism. Denote a homomorphism $\chi_{j_1,j_2,...,j_m}$, where $\chi(g_i)_{j_1,j_2,...,j_m} = \omega_i^{j_i}$ for all $1 \leq i \leq m$ and $\omega_i = e^{\frac{2\pi i}{n_i}}$. Restrict j_i such that $0 \leq j_i \leq n_i$: any higher power of the generator can have a $g_i^{n_i} = 1$ factored out.

Then it follows that for each i, $(\chi_{j_1,j_2,...,j_m} \circ \chi_{k_1,k_2,...,k_m})(g_i) = \omega_i^{j_i}\omega_i^{k_i} = \omega^{j_i+k_i}$. Since this is true for each g_i, we have that $(\chi_{j_1,j_2,...,j_m} \circ \chi_{k_1,k_2,...,k_m}) = \chi_{j_1+k_1,...\,j_m+k_m}$.

Note that the multiplication of homomorphisms is then reduced to addition of subscripts in each components. This will provide us with an isomorphism.

Define the function $\phi : G \to X$ by $\phi(g_1^{k_1}, ..., g_m^{k_m}) = \chi_{k_1,...,k_m}$. Then $\phi((g_1^{k_1}, ..., g_m^{k_m}) \circ (g_1^{j_1}, ..., g_m^{j_m})) = \phi(g_1^{k_1+j_1}, ..., g_m^{k_m+j_m}) = \chi_{k_1+j_1,...,k_m+j_m}$. But we showed above that

$$\chi_{k_1+j_1,...,k_m+j_m} = \chi_{k_1,k_2,...,k_m} \circ \chi_{j_1,j_2,...,j_m}.$$

Thus

$$\phi((g_1^{k_1}, ..., g_m^{k_m}) \circ (g_1^{j_1}, ..., g_m^{j_m})) = \phi(g_1^{k_1}, ..., g_m^{k_m})\phi(g_1^{j_1}, ..., g_m^{j_m}),$$

so ϕ is a homomorphism.

Suppose that $\chi_{j_1,...,j_m} = \chi_{k_1,...,k_m}$. Then for every i, we have that $\chi_{j_1,...,j_m}(g_i) = \chi_{k_1,...,k_m}(g_i)$. Then $\omega_i^{j_i} = \omega_i^{k_i}$. Since $0 \leq j_i, k_i < n_i$, this is possible if and only if $j_i = k_i$. Therefore $(k_1, ..., k_m) = (j_1, ..., j_m)$, so ϕ is one to one.

Finally, for every $\chi_{k_1,\ldots,k_m}$, we have that $g_i^{k_i} \in G_i$. Then $g_1^{k_1}$, ..., $g_m^{k_m} \in G$. Thus ϕ is onto.

Therefore ϕ is an isomorphism. □

In addition to forming a group isomorphic to G, the character group X has desirable orthogonality properties.

Definition 1.8. Let χ, θ be characters on a finite abelian group G. Define the inner product of χ and θ by $\langle \chi, \theta \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\theta^{-1}(g)$.

Theorem 1.13. The characters on a finite abelian group are an orthonormal set.

Proof: Observe that the map $\phi_x : G \to G$ defined by $\phi(g) = xg$ is one to one by uniqueness of inverses. Since G is finite, this means that $\phi_x(G) = G$; that is, $g \mapsto xg$ is simply a permutation of the elements of G for any element $x \in G$.

Using this fact (i.e., that $xg \in G$ is a reindexing of $g \in G$), homomorphism properties, and recalling that $\chi(g)$ is a complex number and therefore character multiplication is commutative, we have:

$$\begin{aligned}
\langle \chi, \theta \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(g)\theta^{-1}(g) \\
&= \frac{1}{|G|} \sum_{xg \in G} \chi(xg)\theta^{-1}(xg) \\
&= \frac{1}{|G|} \sum_{xg \in G} \chi(x)\chi(g)\theta^{-1}(x)\theta^{-1}g \\
&= \frac{1}{|G|} \sum_{g \in G} \chi(x)\chi(g)\theta^{-1}(x)\theta^{-1}(g) \\
&= \chi(x)\theta^{-1}(x)\frac{1}{|G|} \sum_{g \in G} \chi(g)\theta^{-1}(g) \\
&= \chi(x)\theta^{-1}(x)\langle \chi, \theta \rangle.
\end{aligned}$$

Then we have that

$$\langle \chi, \theta \rangle - \chi(x)\theta^{-1}(x)\langle \chi, \theta \rangle = 0,$$

so

$$\langle \chi, \theta \rangle (1 - \chi(x)\theta^{-1}(x)) = 0.$$

This multiplication is in the complex numbers and is true for any $x \in G$, so we conclude that either $1 = \chi(x)\theta^{-1}(x)$ for all x or that $\langle \chi, \theta \rangle = 0$.

If $\chi \neq \theta$, then there exists some x such that $\chi(x) \neq \theta(x)$. By uniqueness of the inverse, we know that $\theta^{-1}(x) \neq \chi^{-1}(x)$. Then it follows that $\chi(x)\theta^{-1}(x) \neq 1$, so it must be that $\langle \chi, \theta \rangle = 0$.

If $\chi = \theta$, then we have by definition that

$$\begin{aligned}\langle \chi, \theta \rangle &= \frac{1}{|G|}\sum_{g\in G}\chi(g)\theta^{-1}(g)\\ &= \frac{1}{|G|}\sum_{g\in G}\chi(g)\chi^{-1}(g)\\ &= \frac{1}{|G|}\sum_{g\in G}1\\ &= \frac{1}{|G|}|G|\\ &= 1.\end{aligned}$$

We have therefore shown that $\langle \chi_i, \theta_j \rangle = \delta_{ij}$; that is, the characters are orthonormal. □

Having established some basic facts about characters, we are prepared to begin working towards a proof of the most important result of character theory in partial difference sets: namely, that character sums (of non-principal characters) over a set D take on exactly two specified values if and only if D is a partial difference set.

This key result will require several lemmas and theorems to prove.

Lemma 1.14. If χ is not the principal character, then $\chi(G) = 0$.

Proof: Suppose that χ is not the principal character. Then there exists a $g \in G$ such that $\chi(g) \neq 1$. Observe that gG is simply a permutation of G (since the group is closed and all groups have the cancellation property, so $gh = gk$ if and only if $h = k$).

Then $\chi(gG) = \sum_{h\in G}\chi(gh) = \sum_{h\in G}\chi(g)\chi(h) = \chi(g)\sum_{h\in G}\chi(h) = \chi(g)\chi(G)$.

That is, $\chi(gG) = \chi(g)\chi(G)$. However, gG is just a permutation of G; it does not matter what order of the elements we use for summing their characters, so $\chi(H) = \chi(G)$ for any permutation H of G. Thus $\chi(gG) = \chi(G)$.

Therefore $\chi(gG) = \chi(G)$ and $\chi(gG) = \chi(g)\chi(G)$. Thus $\chi(G) = \chi(g)\chi(G)$. Thus $\chi(G) - \chi(g)\chi(G) = 0$, so $\chi(G)(1 - \chi(G)) = 0$. Either $\chi(G) = 0$ or $1 - \chi(g) = 0$. However, we chose g such that $\chi(g) \neq 1$, so $1 - \chi(g) \neq 0$. Therefore $\chi(G) = 0$. □

Theorem 1.15. Let D be a subset of a finite Abelian group G. If D is a PDS, $e \in D$, and $\chi : D \to \mathbb{C}$ is a character, then $\chi(D) = \frac{-\mu+\lambda\pm\sqrt{(\mu-\lambda)^2-4(\lambda-k)}}{2}$ or $\chi(D) = |D|$. If $e \notin D$, then $\chi(D) = \frac{-\mu+\lambda\pm\sqrt{(\mu-\lambda)^2-4(\mu-k)}}{2}$ or $\chi(D) = |D|$.

Proof: If χ is the principal character, then $\chi(g) = 1$ for all $g \in G$, so $\chi(D) = |D|$.

Suppose then that χ is not the principal character.

We will prove this by cases. For the first case, suppose that $e = 1 \in D$. Then we know that $D^2 = k(1) + \lambda(D-1) + \mu(G-D) = (k-\lambda)(1) + \mu G + (\lambda-\mu)D$.

Therefore $D^2+(\mu-\lambda)D+(\lambda-k)(1)-\mu G = 0$, so $\chi(D^2+(\mu-\lambda)D+(\lambda-k)(1)-\mu G) = \chi(0(1))$. (For a group ring element $H = \sum_{g_i\in G} a_i g_i$, we define $\chi(H) = \sum_{g_i\in G} a_i\chi(g_i)$; this makes it consistent with our notion of a homomorphism and group rings as representing linear combinations of group elements).

Therefore

$$\begin{aligned}\chi(0(1)) &= \chi(D^2 + (\mu - \lambda)D + (\lambda - k)(1) - \mu G)\\ 0(\chi(1)) &= \chi(D^2) + (\mu - \lambda)\chi(D) + (\lambda - k)\chi(1) - \mu\chi(G).\end{aligned}$$

But we know that $\chi(1) = 1$ for any homomorphism. Furthermore, the previous lemma tells us that $\chi(G) = 0$. Finally, we know that $\chi(D^2) = \chi(D)^2$, since $\chi(D^2) = \sum_{a_i,b_i \in D} \chi(a_i b_i) = \sum_{a_i,b_i \in D} \chi(a_i)\chi(b_i) = \chi(D)^2$. Thus

$$0 = \chi(D^2) + (\mu - \lambda)\chi(D) + (\lambda - k)$$

Notice that the output of χ is a complex number. This is therefore a quadratic in the complex variable $\chi(D)$, so we can apply the quadratic formula. Thus $\chi(D) = \frac{-\mu+\lambda\pm\sqrt{(\mu-\lambda)^2-4(\lambda-k)}}{2}$.

In the second case where $e = 1 \notin D$, we use a similar argument. However, the group ring expression for D^2 becomes $D^2 = k(1) + \lambda(D) + \mu(G - D - 1) = (k - \mu)(1) + \mu G + (\lambda - \mu)D$.

Then $D^2 + (\mu - \lambda)D + (\mu - k)(1) - \mu G = 0$, so $\chi(D^2 + (\mu - \lambda)D + (\mu - k)(1) - \mu G) = \chi(0(1))$.

Using the same arguments as before, this gives us that $0 = \chi(D)^2 + (\mu - \lambda)D + (\mu - k)$, so $\chi(D) = \frac{-\mu+\lambda\pm\sqrt{(\mu-\lambda)^2+4(\mu-k)}}{2}$. □

Lemma 1.16. If G is a finite abelian group and χ is a character, then for all $h \in G$, $\sum_j \chi_j(h) = |G|$ if $h = e$ and $\sum_j \chi_j(h) = 0$ if $h \neq e$.

Proof: Recall that we have shown previously that if a group G is isomorphic to $G_1 \times G_2 \times ... \times G_k$, where $|G_k| = n_k$, then there are $n_1 ... n_k$ distinct characters on the group.

By the Fundamental Theorem of Finite Abelian Groups, we know that $G \approx G_1 \times G_2 \times ... \times G_k$, where G_i is a cyclic group of prime power order n_i. We know also that $n_1 ... n_k = |G|$. Then the theorem mentioned above tells us that there are $n_1 ... n_k = |G|$ distinct characters.

If $h = e$, then $\chi(h) = 1$ for any character χ. Thus $\sum_j \chi_j(h) = \sum_j 1 = |G|$.

Then suppose that $h \neq e$. We know that we can write $h = g_i^m$, where g_i is a generator for one of the cyclic groups and $m \in \mathbb{Z}^+$. Furthermore, since $h \neq e$, it follows that $n_i > 1$. Then $\chi(h) = \chi(g_i^m)$ for all characters χ. Define $\eta(g_i) = e^{\frac{2\pi i}{mn_i}}$ (this is well defined, as $m, n_i > 0$). Then $\eta(g_i^x)\eta(g_i^y) = e^{\frac{2\pi ix}{mn_i}} e^{\frac{2\pi iy}{mn_i}} = e^{\frac{2\pi i}{mn_i}}(x + y) = \eta(g^{x+y}) = \eta(g^x g^y)$, so this function is a homomorphism. Furthermore, this function has the property that $\chi(h) = \chi(g^m) = e^{\frac{2\pi i}{n_i}}$ Since $n_i > 1$, $e^{\frac{2\pi i}{n_i}} \neq 1$. Therefore if $h \neq e$, there exists a homomorphism η such that $\eta(h) \neq 1$.

Furthermore, we know that the characters form a group under multiplication, guaranteeing closure and the cancellation property. Then $\{\eta\chi_j : \chi_j \in \text{the character group}\}$ is just a permutation of the group; the order of the terms does not matter in the sum (since the characters are complex numbers, which commute), so $\sum_j \chi_j(h) = \sum_j \chi_j(h)\eta(h)$.

Therefore $\sum_j \chi_j(h)(\eta(h) - 1) = 0$. Since $\eta(h) - 1$ is independent of j, we have that $(\eta(h) - 1)(\sum_j \chi_j(h)) = 0$, so either $\eta(h) - 1 = 0$ or $\sum_j \chi_j(h) = 0$. But we choose η such that $\eta(h) \neq 1$, so it must be that $\sum_j \chi_j(h) = 0$. □

Lemma 1.17. Let G be a finite abelian group, and let y be an element of the group ring $\mathbb{Z}[G]$. Let $\{\chi_j | j \in \mathbb{Z}_{|G|}\}$ be the set of distinct characters on G. Denote $y = \sum_{g \in G} a_g g$; then $a_h = \frac{1}{|G|} \sum_j \chi_j(h^{-1}y)$.

Proof: By definition, $h^{-1}D = \sum_{g \in G} a_g h^{-1} g$. Therefore for any character χ_j, we have that $\chi_j(h^{-1}D) = \sum_{g \in G} a_g \chi_j(h^{-1}g)$.

Therefore

$$\frac{1}{|G|} \sum_j \chi_j(h^{-1}D) = \frac{1}{|G|} \sum_j \sum_{g \in G} a_g \chi_j(h^{-1}g).$$

Now, in a finite sum of complex numbers, the sum is the same even if the terms are permuted, so

$$\begin{aligned}\frac{1}{|G|} \sum_j \chi_j(h^{-1}D) &= \frac{1}{|G|} \sum_j \sum_{g \in G} a_g \chi_j(h^{-1}g) \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_j a_g \chi_j(h^{-1}g) \\ &= \frac{1}{|G|}(a_h(\sum_j \chi_j(h^{-1}h)) + \sum_{g \in G, g \neq h} \sum_j \chi_j(h^{-1}g).\end{aligned}$$

Since $g \neq h$ in the second sum, the uniqueness of inverses guarantees that $h^{-1}g \neq e$. Applying the previous lemma to both sums, we have that

$$\begin{aligned}\frac{1}{|G|} \sum_j \chi_j(h^{-1}D) &= \frac{1}{|G|}(a_h(\sum_j \chi_j(h^{-1}h)) + \sum_{g \in G, g \neq h} \sum_j \chi_j(h^{-1}g) \\ &= \frac{1}{|G|}(a_h|G| + \sum_{g \in G, g \neq h} 0) \\ &= a_h.\end{aligned}$$

□

Corollary 1.17.1. Let $y, y' \in \mathbb{Z}[G]$, where G is an abelian group. Then $\chi(y) = \chi(y')$ for any character χ implies that $y = y'$.

Proof: Suppose $\chi(y) = \chi(y')$ for any character χ. Since y, y' are in the group ring, we have $y = \sum_{g \in G} a_g g$ and $y' = \sum_{g \in G} a'_g g$. But $a_h = \frac{1}{|G|} \sum_j \chi_j(h^{-1}y')$ and $a'_h = \frac{1}{|G|} \sum_j \chi_j(h^{-1}y)$. Since $\chi_j(y) = \chi_j(y')$, we have that $a_h = a'_h$ and thus $y = y'$. □

That is, the set of character sums on a group element contains all of the information about the element. With this insight, we are finally prepared to prove our main theorem.

Theorem 1.18. Let D be a reversible subset of a finite abelian group G. Then, if $e \notin D$, we have that D is a PDS if and only if and $\chi(D) = \frac{-\mu+\lambda \pm \sqrt{(\mu-\lambda)^2 - 4(\mu-k)}}{2}$ for every non-principal character χ and that $k^2 = \lambda k + \mu(v - k - 1) + k$ [3].

Proof: We have already shown that if D is a PDS, then the character sum $\chi(D)$ is as claimed (see theorem 1.15).

Suppose now that D is a subset of a group G that does not contain the identity. Let $|G| = v$, $|D| = k$, and $\beta = \lambda - \mu$ and $\gamma = \mu - k$. Furthermore, suppose that $\chi(D) = \frac{-\mu+\lambda\pm\sqrt{(\mu-\lambda)^2-4(\mu-k)}}{2}$ for every non-principal character χ. That is, $\chi(D) = \frac{\beta\pm\sqrt{\beta^2-4\gamma}}{2}$ for every non-principal χ. To simplify notation, define $\Delta = \beta^2 - 4\gamma$. Therefore $\chi(D) = \frac{\beta\pm\sqrt{\Delta}}{2}$ for every non-principal character.

Let us consider the group ring $R[G]$ with the group G and the ring $R = \mathbb{Z}$. Let D' denote the group ring element $D' = \sum_{d\in D} d$. Let 1_G denote the group ring element $1e$, where e is the identity element of G.

Consider the group ring element $y = (D' - \frac{\beta+\sqrt{\Delta}}{2}1_G)(D' - \frac{\beta-\sqrt{\Delta}}{2}1_G)$. Carrying out this multiplication, we find that

$$\begin{aligned}
y &= (D' - \frac{\beta+\sqrt{\Delta}}{2}1_G)(D' - \frac{\beta-\sqrt{\Delta}}{2}1_G) \\
&= D'^2 - D'\left(\frac{\beta-\sqrt{\Delta}}{2}\right)1_G - D'\left(\frac{\beta+\sqrt{\Delta}}{2}\right)1_G + \frac{\beta^2-\Delta}{4} \\
&= D'^2 - \beta D' + \frac{\beta^2-\Delta}{4}1_G.
\end{aligned}$$

Suppose that we apply a non-principal character χ to this equation. Then homomorphism properties give us that

$$\begin{aligned}
\chi(y) &= \chi(D'^2) - \chi(\beta D') + \chi\left(\frac{\beta^2-\Delta}{4}1_G\right) \\
&= \chi(D')^2 - \beta\chi(D') + \frac{\beta^2-\Delta}{4}\chi(1_G) \\
&= \chi(D')^2 - \beta\chi(D') + \frac{\beta^2-\Delta}{4}.
\end{aligned}$$

That is,

$$\chi(y) = \chi(D')^2 - \beta\chi(D') + \frac{\beta^2-\Delta}{4}. \tag{3}$$

Consider the equation

$$0 = \chi(D')^2 - \beta\chi(D') + \frac{\beta^2-\Delta}{4}. \tag{4}$$

This equation is a quadratic in the variable $\chi(D')$ in the complex numbers, so we may apply the quadratic formula. This tells us that the solutions of the equation are

$$\begin{aligned}
\chi(D') &= \frac{\beta \pm \sqrt{\beta^2 - 4(\frac{\beta^2-\Delta}{4})}}{2} \\
&= \frac{\beta\pm\sqrt{\Delta}}{2}.
\end{aligned}$$

But this is exactly what we have said that the value of χ is for any non-principal character. That is, for any non-principal character χ, $\chi(D')$ satisfies equation 4. But the right side of equation 4 is the same of the right side of equation 3. We know that equation 3 is always true, and we have just argued that equation 4 is true for any non-principal χ. We therefore conclude that for any non-principal χ, the left hand sides of equations 3 and 4 are equal. That is, $\chi(y) = 0$.

For a principal character χ_1, equation 3 tells us that $\chi_1(y) = |D|^2 - \beta|D| + \frac{\beta^2-\Delta}{4}$. That is, $\chi_1(y) = k^2 - \beta k + \frac{\beta^2-\Delta}{4}$; define this constant to be $\chi_1(y) = C$.

Consider now the group ring element $y' = (\frac{C}{v})G'$, where $G' = \sum_{g\in G} 1g$. It is clear that for the principal character, $\chi_1((\frac{C}{v})G = \frac{C}{v}\chi_1(G) = \frac{C}{v}|G| = \frac{C}{v}v = C$.

Furthermore, we know that for a non-principal character χ, we have that $\chi(G) = 0$. Then $\chi(y') = \frac{C}{v}\chi(G) = 0$.

We therefore know that $\chi(y) = \chi(y')$ for every character χ. By the previous corollary, it follows that $y = y'$. Therefore

$$\begin{aligned}\frac{C}{v}G' &= D'^2 - \beta D' + \frac{\beta^2-\Delta}{4}1'_G\\ D'^2 &= \beta D' - \frac{\beta^2-\Delta}{4}1_G + \frac{C}{v}(G'-D'-1_G) + \frac{C}{v}D' + \frac{C}{v}1_G\\ D'^2 &= (\beta + \frac{C}{v})D' + \frac{C}{v}(G'-D'-1_G) + (\frac{C}{v} - \frac{\beta^2-\Delta}{4})1_G.\end{aligned}$$

That is,

$$D'^2 = (\beta + \frac{C}{v})D' + \frac{C}{v}(G'-D'-1_G) + (\frac{C}{v} - \frac{\beta^2-\Delta}{4})1_G, \tag{5}$$

the general form of the group ring equation we are looking for.

Now,

$$\begin{aligned}C &= k^2 - \beta k + \frac{\beta^2-\Delta}{4}\\ &= k^2 - \beta k + \frac{\beta^2 - (\beta^2 - 4(\mu-k))}{4}\\ &= k^2 - k(\lambda-\mu) + \mu - k.\end{aligned}$$

By theorem 1.7, it follows that

$$\begin{aligned}C &= k^2 - k(\lambda-\mu) + \mu - k\\ &= [\lambda k + \mu(v-k-1) + k] - k(\lambda-\mu) + \mu - k\\ &= k\lambda + v\mu - k\mu - \mu + k - k\lambda + k\mu + \mu - k\\ &= v\mu.\end{aligned}$$

Therefore $\frac{C}{v} = \frac{v\mu}{v} = \mu$.

Finally, we have that

$$\begin{aligned}\frac{C}{v} - \frac{\beta^2 - \Delta}{4} &= \mu - \frac{\beta^2 - (\beta^2 - 4(\mu - k)}{4} \\ &= \mu - (\mu - k) \\ &= k.\end{aligned}$$

Using $\frac{C}{v} = \mu$, $\frac{C}{v} - \frac{\beta^2 - \Delta}{4} = k$, and $\beta = \lambda - \mu$ in equation 5,

$$D'^2 = (\lambda - \mu + \mu)D' + \mu(G' - D' - 1_G) + k1_G.$$

That is,

$$D'^2 = \lambda D' + \mu(G' - D' - 1_G) + k1_G. \tag{6}$$

Since D is reversible, this means that $D'^2 = D'(D')^{(-1)}$ and thus equation 6 implies that D is a (v, k, λ, μ) partial difference set.

Corollary 1.18.1. Let D' be a subset of a finite abelian group G with $e \in D$. Then D is a (v, k', λ, μ') PDS if and only if $\chi(D') = \frac{\lambda' - \mu' \pm \sqrt{(\lambda' - \mu')^2 - 4(\lambda' - k')}}{2}$, where $k'^2 = \lambda'(k' - 1) + \mu'(v - k') + k'$, for every character χ.

Proof: We know that D' is a (v, k', λ', μ') PDS if and only if $G \setminus D'$ is a (v, k, λ, μ) PDS, where $k' = v - k, \lambda' = v + \mu - 2k$, and $\mu' = v + \lambda - 2k$. Furthermore, we note that given these definitions, the condition on k'^2 in the statement of the corollary is equivalent to the condition on k^2 in the statement of the previous theorem.

Define $D = G \setminus D'$. The previous theorem tells us that D is a PDS if and only if $\chi(D) = \frac{\lambda - \mu \pm \sqrt{(\mu - \lambda)^2 - 4(\mu - k)}}{2}$. Now, we know that $\chi(G) = 0$ and that $D \cup D' = G$, so we have that $\chi(D') = -\chi(D)$. Then D is a PDS if and only if $\chi(D') = \frac{\mu - \lambda \pm \sqrt{(\lambda - \mu)^2 - 4(\mu - k)}}{2}$. Now, we note that $\mu - \lambda = \lambda' - \mu'$ and that $\mu - k = \lambda' + k - v = \lambda' - k'$. Substituting these into our character expression, we have that $\chi(D') = \frac{(\lambda' - \mu') \pm \sqrt{(\lambda' - \mu')^2 - 4(\lambda' - k')}}{2}$. That is, we have shown that the $\chi(D')$ condition in the corollary is equivalent to the $\chi(D)$ statement in the previous theorem.

Taking this together with the counting condition, we have that $\chi(D') = \frac{\lambda' - \mu' \pm \sqrt{(\lambda' - \mu')^2 - 4(\lambda' - k')}}{2}$, where $k'^2 = \lambda'(k' - 1) + \mu'(v - k') + k'$, for every character χ, if and only if $D = G \setminus D'$ is a partial difference set. But we know that D is a PDS if and only if its complement D' is a PDS. That is, $\chi(D') = \frac{\lambda' - \mu' \pm \sqrt{(\lambda' - \mu')^2 - 4(\lambda' - k')}}{2}$, where $k'^2 = \lambda'(k' - 1) + \mu'(v - k') + k'$, for every character χ, if and only if D' is a (v, k', λ', μ') PDS. □

An analogous result also exists for difference sets. Not only will this theorem be used in our exploration of partial difference sets, this is one of the earliest foundational character theory results. We will state it below; the proof will be given in the appendix.

Theorem 1.19. Let G be a finite abelian group of order v and let D be a subset of G of order k. Then D is a (v, k, λ) difference set if and only if $|\chi(D)| = \sqrt{k = \lambda}$ for every character χ [10].

Proof: see theorem 6.1 in the appendix.

2 Denniston Partial Difference Sets

We will now explore a family of partial difference sets called the Denniston family. We begin with a construction of a simple example of a Denniston PDS.

First, we remind the reader of the definition of a quadratic form.

Definition 2.1 (Quadratic Form)**.** Let F be a field. A quadratic form is a polynomial $Q : F^2 \to F$ such that $Q(ax, ay) = a^2Q(x, y)$.

We will also define a special type of quadratic form: an irreducible.

Definition 2.2 (Irreducibility)**.** Let F be a field and $Q : F^2 \to F$ be a quadratic form. Then the quadratic form is irreducible over F if $Q(x, y) = 0$ if and only if $(x, y) = 0$.

We will now proceed with a specific example.

Let $F_4 = \{0, 1, \alpha, \alpha + 1\}$ be the field with four elements. We desire $Q : F_4^2 \to F_4$ that is a quadratic form such that $Q(x, y) = 0$ if and only if $(x, y) = (0, 0)$. We will show that $x^2 + xy + \alpha y^2$ is such a quadratic form.

Note that $Q(x, y)$ takes on the following values for the specified inputs:

(x,y)	Q(x,y)
(0,0)	0
(0,1)	α
(0, α)	1
(0, α^2)	α^2
(1,0)	1
(1,1)	α
(1,α)	α
(1, α^2)	1

Table 1: Some outputs of $Q(x, y) = x^2 + xy + \alpha y^2$.

Then we consider $Q(x, y)$ for an (x, y) not in the table. Since (x, y) is not in the table, we know that $x \neq 0$. Therefore if we want to write $y = xy'$, we know that $y' = x^{-1}y$ exists and will satisfy this equation.

We therefore have that $(x, y) = (x(1), x(x^{-1}y'))$. Since Q is a quadratic form, it follows that $Q(x, y) = x^2Q(1, x^{-1}y)$. Since we are working in a field, there are no zero divisors. Since $x \neq 0$, we conclude that $Q(x, y) = 0$ if and only if $Q(1, x^{-1}y) = 0$. But table 1 shows that $Q(1, a) \neq 0$ for any $a \in F$, so we may conclude that $Q(x, y) \neq 0$ if (x, y) is not in the table.

We have thus shown that $Q(x, y) = 0$ if and only if $(x, y) = 0$.

Now define $K = \{0, 1\}$ and $S = \{(1, a, b)|Q(a, b) \in K\}$. Referencing our table (and using the calculation for $Q(x, y)$ above), we may see that

$$S = \{(1, 0, 0), (1, 0, \alpha), (1, 1, 0), (1, 1, \alpha^2), (1, \alpha, \alpha), (1, \alpha, \alpha^2)\}.$$

Then consider the set $D = S \cup \alpha S \cup \alpha^2 S$. It may be shown that each set $S, \alpha S$, and $\alpha^2 S$ are (16,6,2) Hadamard difference sets. Furthermore, one may show that D is a $(64, 18, 2, 6)$ PDS in the additive group of F_4^3, which is isomorphic to $\mathbb{Z}_2^6$.

We can replicate this construction to get a Denniston PDS in a larger group. Suppose that we use the field F_8 instead of F_4. In much the same way as we did in the simpler case, one may verify that $Q(x, y) = x^2 + xy + y^2$ is irreducible over the field. We then define $K = \{0, 1, \alpha, \alpha + 1\}$ and $S = \{(1, a, b)|Q(a, b) \in K\}$. Then, we have that $D = \sum_{x \in F \setminus \{0\}} xS$ is a PDS in $\mathbb{Z}_2^9$ [4]. The parameters of this PDS are $(512, 196, 60, 84)$.

Indeed, we may construct a $(512, 70, 6, 10)$ PDS in $\mathbb{Z}_2^9$ by following the same construction using the field of eight elements but replacing K with $K' = \{0, 1\}$ [3, 4].

Each multiplicative coset of S has 10 elements. Since the first component is just the multiplicative coset representative, it is fruitful to consider S as a subset of $\mathbb{Z}_2^3 \times \mathbb{Z}_2^6$. In this work, we set out to answer the question: what is the structure of the second and third components (a, b) in each coset (viewed as a subset of $\mathbb{Z}_2^6$)?

We observe that each multiplicative coset may be written as a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ taken together with a $(16, 6, 2)$ difference set. See appendix 6.1 for a list of these PDS elements and how they may be partitioned into subgroups and difference sets. This may be considered analogous to the structure of the $(64, 18, 2, 6)$ PDS; instead of three sets of $(16, 6, 2)$ difference sets, we have seven sets of the union of a $\mathbb{Z}_2 \times \mathbb{Z}_2$ subgroup and a $(16, 6, 2)$ difference set.

2.1 McFarland Construction

We claimed that the sets of six elements in our $(64, 18, 2, 6)$ example were $(16, 6, 2)$ difference sets. A useful way to think of these difference sets is via the McFarland construction, which we will develop now.

Suppose that we have groups G and E such that $E = \mathbb{Z}_2^n$ and $|G| = 2^n$.

First, we define a hyperplane.

Definition 2.3 (Hyperplane)**.** Let S be a linear vector space of dimension n. Then any subspace $H \subseteq S$ of dimension $n - 1$ is called a hyperplane.

We will now develop several lemmas concerning hyperplanes.

Lemma 2.1. *The group E has $2^n - 1$ subgroups isomorphic to $\mathbb{Z}_2^{n-1}$ [7].*

Proof: Think of E as an n dimensional linear vector space over $\mathbb{Z}_2$. Each subgroup isomorphic to $\mathbb{Z}_2^{n-1}$ is an $n - 1$ dimensional subspace (or hyperplane), so it is the unique complement of a one dimensional subspace. Therefore the number of $n - 1$ dimensional subspaces is exactly equal to the number of one dimensional subspaces.

Now, any nonzero vector generates a unique subspace (since we are working over $\mathbb{Z}_2$ and there are no scalar multiples of a vector. We have $2^n - 1$ nonzero vectors, so we therefore have $2^n - 1$ one dimensional subspaces and thus $2^n - 1$ hyperplanes. □

Define $D = \cup_{i=1}^{2^n-1}(g_i, H_i) \subseteq G \times E$, where the H_i are the distinct hyperplanes of E. We will notate (g_i, H_i) as $g_i H_i$ for the sake of brevity.

Lemma 2.2. *Using group ring notation, $H_i(H_i^{-1}) = 2^{n-1}H_i$.*

Proof: We know that H_i is a subgroup, so it is closed under addition. Furthermore, given $h_1 \in H_i$, we know that $h_1 + h_2 \neq h_1 + h_3$ for distinct $h_2, h_3 \in H_i$. Thus $h + H_i = H_i$ for any $h \in H$.

Since H_i is closed under inversion, $H_i^{-1} = H_i$. Thus

$$\begin{aligned} H_i(H_i^{-1}) &= H_iH_i \\ &= \sum_{j=1}^{2^{n-1}} h_j + H_i \\ &= \sum_{j=1}^{2^{n-1}} H_i \\ &= 2^{n-1}H_i. \end{aligned}$$

□

Lemma 2.3. In group ring notation, $H_iH_j^{-1} = 2^{n-2}E$ for two distinct hyperplanes $H_i \neq H_j$.

Proof: Let β be a basis for E that is a basis of H_i (which we will call β_i) plus another vector v. For H_j to be a distinct hyperplane, it must contain the vector v. Then we can write a basis of H_j that contains v as a basis vector. Therefore (using the Gram-Schmidt construction) we know that there exists an orthogonal basis β_j of H_j that contains v. Since H_j is $n-1$ dimensional, there are $n-2$ other vectors in H_j, all of which are orthogonal to v.

Now, we know that the $n-2$ vectors in $\beta_j \setminus \{v\}$ are orthogonal to v. Thus span$(\beta_j \setminus \{v\})$ is orthogonal to v. Therefore span$(\beta_j \setminus \{v\})$ is in the complement of span(v). But we know that the complement of span(v) is H_i, so span$(\beta_j \setminus \{v\})$ is contained in H_i.

The intersection of two subspaces is itself a subspace. Furthermore, we know that the intersection of H_i and H_j is at least $n-2$ dimensional, since span$(\beta_j \setminus \{v\}) \subseteq H_i \cap H_j$. However, $v \notin H_i$, so $H_i \cap H_j$ is a proper subspace of H_i. Since H_i is $n-1$ dimensional, it therefore follows that $H_i \cap H_j$ is exactly $n-2$ dimensional.

Furthermore, we know that $H_j^{-1} = H_j$ because H_j is a subgroup. Additionally, for $h_i \in H_i \cap H_j$, we have that $h_i + H_j = H_j$ because H_j is closed under addition. Finally, consider $h_i \in H_j^C$. If $h_i + h_j \in H_j$, where $h_i \in H_i$ and $h_j \in H_j$, then this would imply that $h_i \in H_j$. This can't be, so it must be the case that $h_i + H_j \in H_j^C$. But for fixed i, we know that $h_i + h_j = h_i + h_{j'}$ if and only if $j = j'$. Thus $h_i + H_j$ is a subset of H_j^C with $|H_j| = 2^{n-1}$ elements. But, since H has size 2^{n-1} and E has size 2^n, we know that $|H_j^C| = 2^{n-1}$. It therefore follows that $h_i + H_j = H_j^C$ for $h_i \notin H_j$.

Therefore $H_iH_j^{-1} = \sum_{k=1}^{2^{n-1}} h_k + H_j = \sum_{h_k \in H_j} H_j + \sum_{h_k \notin H_j} H_j^C = |H_i \cap H_j|H_j + |H_i \cap H_j^C|H_j^C$. Now, $H_i \cap H_j$ has dimension $n-2$, so there are 2^{n-2} elements of $H_i \cap H_j$. Furthermore, H_i has 2^{n-1} elements and $\{H_i \cap H_j, H_i \cap H_j^C\}$ is a partition of H_i. Therefore $|H_i \cap H_j^C| = |H_i| - |H_i \cap H_j| = 2^{n-1} - 2^{n-2} = 2^{n-2}$.

We then have that $H_iH_j^{-1} = 2^{n-2}H_j + 2^{n-2}H_j^C = 2^{n-2}(H_j + H_j^C) = 2^{n-2}E$. □

Lemma 2.4. Each nonzero element of E appears in $2^{n-1} - 1$ hyperplanes of E.

Proof: Consider an arbitrary nonzero element $v \in E$. We wish to know how many hyperplanes contain a.

If v is in a hyperplane, we may fix it as a basis element. A given hyperplane is therefore specified by the other $n-2$ basis elements, which we know we may force to be orthogonal to v. Our question then becomes: how many choices of $n-2$ other basis vectors are there that give distinct hyperplanes?

Note that if two hyperplanes have v as a fixed basis element, they are distinct if and only if their $n-2$ dimensional subspaces not containing v are distinct. Furthermore, we are forcing these vectors to be orthogonal to v, so we are choosing these $n-2$ vectors from the $n-1$ dimensional space that is $\text{span}(v)^{\perp}$ (the complement of $\text{span}(v)$). Our question is then to count the number of $n-2$ dimensional subspaces of the $n-1$ dimensional $\text{span}(v)^{\perp}$. This is exactly equivalent to our count of hyperplanes, only with n reduced by 1. We therefore count $2^{n-1}-1$ distinct subspaces of dimension $n-2$, so there are $2^{n-1}-1$ distinct hyperplanes containing v. Since v was an arbitrary nonzero element, it therefore follows that each nonzero v appears in $2^{n-1}-1$ distinct hyperplanes. □

Lemma 2.5. Given H, E as described above, $\sum_{i=1}^{2^n-1} H_i = (2^{n-1}-1)(E-1_E)+(2^n-1)1_E$, where 1_E is the identity element of E.

Proof: The left hand side is a multiset that contains all of the nonzero elements of all of the hyperplanes (counting multiplicity of elements). The above lemma tells us that each nonzero element appears in $2^{n-1}-1$ hyperplanes, so each nonzero element appears $2^{n-1}-1$ times in the left hand sum. Since the left hand sum is some group ring element, it can be written $\sum_{i=0}^{2^n-1} c_i h_i$, where the h_i are the elements of E and c_i is the number of times that h_i appears in the sum.

We just argued that $c_i = 2^{n-1}-1$ for every nonzero element, so the sum is $c_0 1_e + \sum_{i=1}^{2^n-1}(2^{n-1}-1)h_i = (2^{n-1}-1)(E-1_E)+c_0 1_E$. Since 1_E appears exactly once in every hyperplane, we have that $\sum_{i=1}^{2^n-1} H_i = (2^{n-1}-1)(E-1_E)+(2^n-1)1_E$. □

Lemma 2.6. In group ring notation, where $1 \leq i, j \leq 2^n-1$ and $g_0 = 1_G$ is the identity of G, we have that $\sum_{i \neq j} g_i g_j^{-1} = (2^n-2)(G-1_G)$.

Proof: Fix g_j and consider $g_i g_j^{-1}$ where i ranges from 1 to 2^n-1. We know that inverses are unique, so $g_i g_j^{-1} \neq 1_G$. Furthermore, we know that $g_i \neq 1_G$, so $g_i g_j^{-1} \neq g_j^{-1}$. Then $g_i g_j^{-1} = G - 1_G - g_j^{-1}$.

Then, when we let j range over all nonidentity elements of G, we will miss each g_j^{-1} exactly once. That is, each g_j will appear exactly one time fewer than the number of values that g_j takes on. Since g_j takes on 2^n-1 values, each g_j appears $2^n-1-1 = 2^n-2$ times.

But g_j ranges over all values besides 1_G, so the set of all g_j values is $G-1_G$. Each of these appears in the sum 2^n-2 times, so the whole sum must be $(2^n-2)(G-1_G)$.

(In group ring notation: for a fixed g_j, $g_i g_j^{-1} = G - 1_G - g_j^{-1}$. Therefore $\sum_{i \neq j} g_i g_j^{-1} = \sum_{j=1}^{2^n-1} G - 1_G - g_j^{-1} = (2^n-1)G - (2^n-1)1_G - \sum_{j=1}^{2^n-1} g_j^{-1} = (2^n-1)G-(2^n-1)1_G-(G-1) = (2^n-2)(G-1_G)$ by the fact that each element has a unique inverse.) □

We are finally prepared to prove the McFarland construction.

Theorem 2.7. The set D defined above is a $(2^{2n}, 2^{n-1}(2^n-1), 2^{n-1}(2^{n-1}-1))$ difference set [7].

Proof: We will prove this using a group ring computation and our above lemmas. Furthermore, since $g_i H_i$ is a shorthand for the more formal (g_i, H_i), we have that $g_i H_i H_j g_j = (g_i + g + j, H_i + H_j) = (g_i g_j)(H_i H_j)$. Furthermore, note that we are working over rings of characteristic two, so addition and subtraction are the same. Therefore

$$\begin{aligned}
DD^{-1} &= (\sum_{i=1}^{2^n-1} g_iH_i)(\sum_{j=1}^{2^n-1} H_jg_j^{-1}) \\
&= \sum_{i=1}^{2^n-1} g_iH_iH_ig_i^{-1} + \sum_{i\neq j} g_iH_iH_jg_j^{-1} \\
&= \sum_{i=1}^{2^n-1} g_ig_i^{-1}H_iH_i + \sum_{i\neq j} g_ig_j^{-1}H_iH_j \\
&= \sum_{i=1}^{2^n-1} 1_G|H_i|H_i + \sum_{i\neq j} 2^{n-2}Eg_ig_j^{-1} \\
&= 1_G2^{n-1}\sum_{i=1}^{2^n-1} H_i + 2^{n-2}E\sum_{i\neq j} g_ig_j^{-1} \\
&= 1_G2^{n-1}[(2^{n-1}-1)(E-1_E)+(2^n-1)1_E] + 2^{n-2}E(2^n-2)(G-1_G) \\
&= 2^{n-1}(2^{n-1}-1)(1_GE-1_E1_G) + 2^{n-1}(2^n-1)(1_E1_G) + 2^{n-2}(2^n-2)(EG-1_GE) \\
&= 2^{n-1}(2^{n-1}-1)(1_GE-1_E1_G) + 2^{n-1}(2^n-1)(1_E1_G) + 2^{n-1}(2^{n-1}-1)(EG-1_GE) \\
&= 2^{n-1}(2^{n-1}-1)EG + 2^{n-1}(2^n-1)1_G1_E.
\end{aligned}$$

Therefore D is a $(2^{2n}, 2^{n-1}(2^n-1), 2^{n-1}(2^{n-1}-1))$ difference set in $G \times E$. □

We should note that a similar analysis allows for a generalization of the McFarland construction for any group G' where $|G'| = 2^{2n}$ and G' contains a normal subgroup E that is isomorphic to $\mathbb{Z}_2^n$. We may then construct a difference set with McFarland parameters in G'.

We will prove this generalized case using character theory. (Contrasting this with the tedious group ring proof we have just presented is an excellent demonstration of the power of character theory).

Theorem 2.8. Let G be a group with $|G| = 2^{2n}$ that contains a normal subgroup E that is isomorphic to $\mathbb{Z}_2^n$. Then $D = \cup_{i=1}^{2^n-1}(g_i, H_i)$, where the H_i are the distinct hyperplanes of E and the g_i are distinct coset representatives of E in G, is a $(2^{2n}, 2^{n-1}(2^n-1), 2^{n-1}(2^{n-1}-1)$ difference set in G.

Proof: Let p be a prime such that $|E| = p^n$. (We are concerned with the case where $p = 2$, but using this notation allows us to see how this might be generalized).

We know that the cosets of E partition the group G, so we have that for any $x \in G$, there exists a g, e such that $x = g + e$, where $e \in E$.

Either $\chi : E \to \mathbb{C}$ is principal on E or it is not.

Suppose that χ is non-principal on E. Then it maps E onto the pth roots of unity. That is, $|\chi(E)| = p$. The kernel of this homomorphism is a subgroup of E; since the character is non-principal, the kernel is therefore a subgroup of order $\frac{p^n}{p} = p^{n-1}$. However, the hyperplanes H_i are all subgroups of E of order p^{n-1}, so exactly one of the hyperplanes is the kernel of χ.

Call this hyperplane H' and the associated coset representative g'. For any $H_i \neq H'$, we use the fact that $\chi : H_i \to \mathbb{C}$ is a non-principal character on an abelian group, so

$\chi(H_i) = 0$. Therefore the character sum over D is $\chi(D) = \sum_i \chi(g_i)\chi(H_i) = \chi(g')\chi(H') + \sum_{i:H_i \neq H'} \chi(g_i)\chi(H_i) = \chi(g')\chi(H') = 2^{n-1}\chi(g')$ (because $\chi(H_i) = 0$ for every term in the sum where $H_i \neq H'$). Since $\chi(g')$ is a root of unity, we have that $|\chi(D)| = 2^{n-1}$.

Suppose instead that χ is principal on E. Let $a, b \in G$ be two elements in the same coset of E. Then there exists an $e \in E$ such that $a = b + e$. Then $\chi(a) = \chi(b + e) = \chi(b)\chi(e) = \chi(b)$. That is, $\chi(a) = \chi(b)$ for any a, b in the same coset of E. We may therefore define a homomorphism $\theta : G/E \to \mathbb{C}^*$, which we will call the character on G/E induced by χ. Define this mapping by $\theta(a + E) = \chi(a)$. This is well defined, since $\chi(a) = \chi(b)$ for any a, b such that $a + E = b + E$. Furthermore, observe that $\theta((a+E)+(b+E)) = \theta(a+b+E) = \chi(a+b) = \chi(a)\chi(b) = \theta(a+E)\theta(b+E)$, using the fact that χ is a homomorphism. This shows that θ is a homomorphism, as claimed.

Then $\sum_i \chi(g_i H_i) = \sum_i \chi(g_i)(2^{n-1}) = 2^{n-1}\sum_i \chi(g_i)$. We wish to evaluate $\sum_i \chi(g_i)$. Using our induced homomorphism, we observe that $\sum_i \chi(g_i) = \sum_i \theta(g_i + E)$. Now, we know that since G/E is a group, $\sum_{g+E \in G/E} \theta(g + E) = 0$. But the sum $\chi_i \theta(g_i + E)$ ranges from $i = 1$ to $i = 2^n - 1$, which is one less than the size of the factor group G/E. Furthermore, we know by hypothesis that the g_i all correspond to different cosets of E in G. We therefore conclude that $\{g_i + E | 1 \leq i \leq 2^n - 1\}$ is equal to $G/E \setminus A$, where A is one of the distinct cosets. Then $\sum_i \theta(g_i + E) = -\theta(A) + \sum_{g+E \in G/E} \theta(g + E) = -\theta(A) + 0 = -\theta(A)$. But $\theta(A)$ is a root of unity, so we therefore conclude that $\sum_i \chi(g_i)$ is some root of unity ω. Therefore $\sum_i \chi(g_i H_i) = 2^{n-1}\sum_i \chi(g_i) = \omega 2^{n-1}$. Then $|\chi(D)| = |\sum_i \chi(g_i H_i)| = |2^{n-1}\omega| = 2^{n-1}$.

Then we conclude that $|\chi(D)| = 2^{n-1}$ for any character that is not principal on G. Furthermore, we can see that there are $2^{n-1}(2^n - 1)$ elements of D (since there are $2^n - 1$ hyperplanes, each with 2^{n-1} elements). Let $k = 2^{n-1}(2^n - 1)$ and $\lambda = 2^{n-1}(2^{n-1} - 1)$. Then $\sqrt{k - \lambda} = \sqrt{2^{n-1}(2^n - 1) - 2^{n-1}(2^{n-1} - 1)} = \sqrt{2^{n-1}(2^n - 1 - 2^{n-1} + 1}$. Thus $\sqrt{k - \lambda} = \sqrt{2^{n-1}(2^n - 2^{n-1})} = \sqrt{2^{n-1} \cdot 2^{n-1}(2 - 1)} = 2^{n-1}$. By theorem 6.1, it follows that D is a $(2^{2n}, k, \lambda)$ difference set in G. □

2.2 S as a McFarland Difference Set

We have claimed that the S described in this section is a $(16, 6, 2)$ difference set. Using the McFarland construction, we can show that this is the case if we can show that S is the union of three hyperplanes with different coset representatives.

Consider an element $(1, a, b) \in S$. For brevity, we express only the (a, b) part below.

We see that S may be written as the union of the hyperplanes $(0, 0) + \langle(0, \alpha)\rangle$, $(1, 0) + \langle(0, \alpha + 1)\rangle$, and $(\alpha, \alpha) + \langle(0, 1)\rangle$. We can see that the three hyperplanes all have a zero in the first component, and so are the hyperplanes of the subgroup $E = \{(0, a) | a \in \mathbb{F}_4\}$. (We note that the first component does essentially nothing; since the additive group of $\mathbb{F}_4$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, this subgroup E satisfies the criterion in the generalized McFarland construction). Furthermore, the coset representatives are distinct elements of G/E. Thus, by the generalized McFarland construction, the set S is a $(16, 6, 2)$ difference set.

Similar arguments may be applied to αS and $\alpha^2 S$, which are also $(16, 6, 2)$ difference sets.

3 Dual PDS

We will now discuss a construction of another $(512, 70, 6, 10)$ PDS. However, we will seek to construct this PDS in the non-elementary abelian group $\mathbb{Z}_4^3 \times \mathbb{Z}_2^3$. We begin by constructing a $(512, 196, 60, 84)$ PDS in this group.

3.1 A $(512, 196, 60, 84)$ PDS

We will outline a construction presented by Davis and Xiang [3]. Let

$$K_0 = \{(0,0,0), (0,2,0), (2,0,0), (2,2,0)\} \subseteq GR(4,3)$$

and let $h = (0,1,0)$. Define $E_i = \cup_{j=0}^{6} h^i + h^{2i-j} + 2h^j + K_j$. It may be shown that this is a Hadamard difference set in the additive group of $GR(4,3)$.

We now define $D = \sum_{i=0}^{6}(E_i, g^i) \subseteq GR(4,3) \times GR(2,3)$, where g is the multiplicative generator of $GR(2,3)$. It may also be shown that D is a $(512, 196, 60, 84)$ PDS in the additive group of $GR(4,3) \times GR(2,3)$ (which is isomorphic to $\mathbb{Z}_4^3 \times \mathbb{Z}_2^3$).

3.2 Duality Example

Before we proceed with the construction of our $(512, 70, 6, 10)$ PDS, we will describe a construction of a PDS using PDS duality.

Consider the set $\{(0,1), (0,2), (0,3), (1,1), (2,2), (3,3), (1,0), (2,0), (3,0)\} \subset \mathbb{Z}_4 \times \mathbb{Z})_4$. Note that this is a union of three subgroups (with the identity element subtracted from each), so the partial congruence partition construction tells us that this is a $(16, 9, 4, 6)$ PDS in $\mathbb{Z}_4 \times \mathbb{Z}_4$. We may also verify this by straightforward computation of the character sums; we write out the character table below. For compactness of notation, a group element (a, b) is notated by ab. These appear as column labels. Similarly, a character χ with $\chi((1,0)) = \alpha$ and $\chi((0,1)) = \beta$ is denoted by $\alpha\beta$; these appear as row labels on the left. That is, the i, j entry is the character label of row i acting on the group element label of column j. For ease of viewing, the elements in the PDS have been written in red text. The right hand column indicates the character sums over the PDS D; that is, the right hand column entry of row i is the character sum of the character label of row i over the set D. We note that these sums are always $+1$ or -3 for non-principal characters, as expected from our character sum theorem.

$$\left(\begin{array}{c|cccccccccccccccc|c}
 & 00 & 01 & 02 & 03 & 10 & 11 & 12 & 13 & 20 & 21 & 22 & 23 & 30 & 31 & 32 & 33 & \\
\hline
00 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 9 \\
01 & 1 & i & -1 & -i & 1 & i & -1 & -i & 1 & i & -1 & -i & 1 & i & -1 & -i & 1 \\
02 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
03 & 1 & -i & -1 & i & 1 & -i & -1 & i & 1 & -i & -1 & i & 1 & -i & -1 & i & 1 \\
10 & 1 & 1 & 1 & 1 & i & i & i & i & -1 & -1 & -1 & -1 & -i & -i & -i & -i & 1 \\
11 & 1 & i & -1 & -i & i & -1 & -i & 1 & -1 & -i & 1 & i & -i & 1 & i & -1 & -3 \\
12 & 1 & -1 & 1 & -1 & i & -i & i & -i & -1 & 1 & -1 & 1 & -i & i & -i & i & -3 \\
13 & 1 & -i & -1 & i & i & 1 & -i & -1 & -1 & i & 1 & -i & -i & -1 & i & 1 & 1 \\
20 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \\
21 & 1 & i & -1 & -i & -1 & -i & 1 & i & 1 & i & -1 & -i & -1 & -i & 1 & i & -3 \\
22 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\
23 & 1 & -i & -1 & i & -1 & i & 1 & -i & 1 & -i & -1 & i & -1 & i & 1 & -i & -3 \\
30 & 1 & 1 & 1 & 1 & -i & -i & -i & -i & -1 & -1 & -1 & -1 & i & i & i & i & 1 \\
31 & 1 & i & -1 & -i & -i & 1 & i & -1 & -1 & -i & 1 & i & i & -1 & -i & 1 & 1 \\
32 & 1 & -1 & 1 & -1 & -i & i & -i & i & -1 & 1 & -1 & 1 & i & -i & i & -i & -3 \\
33 & 1 & -i & -1 & i & -i & -1 & i & 1 & -1 & i & 1 & -i & i & 1 & -i & -1 & -3
\end{array}\right)$$

Now, we have considered this table as representing the character determining the row acting on the group element determining the column. However, the output of such a calculation is $e^{2\pi i * \sum_j c_j \chi(g_j)}$, where c_j is the coefficient on the generator g_j and $\chi(g_j)$ is the image of the generator under the character. Define $c_j = a$ and $\chi(g_j) = b$. Since multiplication of real numbers is commutative, we may just as well think of ab as ba; that is, we will let c_j be the image of the generator and $\chi(g_j)$ be the coefficient on the generator. Note that this both implies that our table is symmetric and is equivalent to interchanging the role of the group element and the character.

Recall that the character group is isomorphic to the group G. Furthermore, the difference set D is the set of elements whose character sums are one of two values. An analogous structure when we interchange the roles of characters and elements (which we will refer to as the dual of D) is the set of characters whose sum on the set D is some number n. Since the character group is isomorphic to G, we might suspect that the dual of D should itself be a PDS.

In our example, we identify the set of characters whose character sum on D is 1. These are labeled in the left hand column in blue text for ease of viewing. This set is $\{(0,1),(0,2),(0,3),(1,0),(2,0),(3,0),(1,3),(3,1),(2,2)\}$.

One may use character theory, brute computation, or the partial congruence partition theorem to confirm that this is indeed a $(16,9,4,6)$ partial difference set. Indeed, it may be proven that this construction will always work: the isomorphism of the two groups will imply that the dual of a partial difference set is itself a partial difference set [6].

Note, then, that a partial difference set will always come as a family of four: given a PDS $D \subseteq G$, we know that $G \setminus D$, dual(D), and $G\setminus$ dual(D) will also be partial difference sets.

3.3 A $(512, 70, 6, 10)$ PDS

Let G be the group of characters on $\mathbb{Z}_4^3 \times \mathbb{Z}_2^3$ and D be the $(512, 196, 60, 84)$ PDS defined previously in this chapter. Let $D' = \{\chi \in G | \chi(D) = -28\}$. It may be shown that D' is a PDS with 70 elements. In fact, we know that the character group is isomorphic to $\mathbb{Z}_4^3 \times \mathbb{Z}_2^3$, so this isomorphism gives us a $(512, 70, 6, 10)$ PDS in $\mathbb{Z}_4^3 \times \mathbb{Z}_2^3$.

Closer inspection of this PDS in fact reveals a structure similar to that of our $(512, 70, 6, 10)$ PDS in the elementary abelian group. The PDS D' may be written as a union of seven sets of ten elements that all have the same $\mathbb{Z}_2^3$ part. Furthermore, each set of ten elements may be decomposed into a set of four whose $\mathbb{Z}_4^3$ part is isomorphic to $\mathbb{Z}_4$ and a set of six elements that forms an additive coset of a $(16, 6, 2)$ Hadamard difference set in a subgroup of $\mathbb{Z}_4^3$.

Note the similarity to the PDS with the same parameters in the elementary abelian group: that PDS could be written as seven sets of ten elements, with each set of ten being the union of a $\mathbb{Z}_2 \times \mathbb{Z}_2$ subgroup and a $(16, 6, 2)$ Hadamard difference set.

3.4 Computations

Even with the powerful theoretical tools we have developed, the computations required to implement character theory are daunting in a group of 512 characters. (We are generally interested in knowing all characters of all elements of a group G, which is a set of $|G|^2$ numbers. This is prohibitively time consuming to do by hand.)

To perform the analysis in this thesis, we have developed a Python implementation of basic galois ring calculations. We will briefly describe these below; a sample of code may be found in the appendix.

Our implementation relies on the fact that any element of an abelian group may be thought as a list of coefficients of the generators of the group. In our implementation, a group element is an object that stores a list of coefficients and a galois ring object, as well as overloading basic arithmetic operators with the correct calculations using the group ring coefficients. Multiplication is done by using a numpy package to perform polynomial multiplication of coefficients. This process yields temporary coefficients. Coefficients of sufficiently high powers are written as nontrivial linear combinations of lower powers using a "power table" in the galois ring stored by the element, which are then combined with the lower power coefficients to find the coefficients describing the appropriate group element to output. This code is found in "galois-rings.py".

The galois ring object is constructed using given m, n values (such that the additive group is $\mathbb{Z}_m^n$) and an irreducible polynomial. A "power table" is constructed by recursively computing h^n (where h is the multiplicative generator of the ring) for $0 \leq n < 2n - 1$ using the irreducible polynomial. This code is also found in "galois-rings.py".

For example: we are primarily interested in $GR(4, 3)$. This ring is constructed as described above using the polynomial $x^3 + 2x^2 + x + 3$, which is represented as the vector $(1, 2, 1, 3)$ (note that coefficients go in descending order). Suppose we wish to construct the element $x^2 + x$. We would input the vector $(1, 1, 0)$ into the constructor for the Element class. Addition and subtraction are performed using numpy built-in modular vector arithmetic; multiplication (such as squaring the element) is done by numpy built-in polynomial multiplication. The resulting polynomial (which, in the case of squaring our example element, would be $x^4 + 2x^3 + x^2$) is then reduced via the power table (which stores values for any power of x that can be achieved by multiplying two elements in reduced form). In our example, the x^4 and x^3 are converted to reduced polynomials, which are then multiplied by the correct coefficients and summed with x^2 to get the result.

We also implement character evaluation on an arbitrary abelian group $G = \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}$. First, we create a function that generates a list of all elements of the group. This is done by recursively appending all allowed values in $\mathbb{Z}_{m_{k+1}}$ to the current list of vectors, which is $\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_k}$.

Next, we implement evaluation of character sums. Homomorphism properties tell us that a character is uniquely defined by the images of the generators of G. We further know that the generators g_j must be mapped to roots of unity; define θ_j such that $\chi(g_j) = e^{2\pi i\theta_j/m_j}$. Then we have that $\chi(y) = e^{2\pi i \sum_j (c_g\theta_j)/m_j}$, where c_j is the coefficient of g_j in y. Our character evaluation is done by using this formula and numpy's complex arithmetic given a vector of the m_j and a vector of the coefficients c_j (and rounding to eliminate the effects of floating point precision). A version of this is found in the "get-character-sum" function in "PDS-list-generator2.py". To find the character sum, we simply range over all the characters in the group and sum the results.

An example of a character computation is as follows. Suppose we are evaluating characters on $\mathbb{Z}_4^3$. A character is defined by the images of the generators; let us consider the character that sends the first generator to the first of the complex fourth roots of unity, the second generator to the second of the complex roots of unity, and the third generator to the third of the complex roots of unity. We represent this character by $(1, 2, 3)$. Let the element we wish to evaluate the character for be $(1, 1, 1)$; then the character evaluates to $e^{2\pi i(\frac{1*1}{4}+\frac{2*1}{4}+\frac{3*1}{4})}$. This evaluation is done using built-in complex multiplication in the numpy package.

This implementation of characters was used to calculate the 70 element PDS described previously in this chapter. To confirm that these computations were done correctly, we computed the character sums over the proposed PDS.

We also created a function to check if a given set was a difference (which appears in "checking-diff-set.py". This checker works by computing every pairwise difference and storing the difference in a vector along with a counter that was updated for the number of times each difference appeared. This allowed for computational exploration of the properties of the $(16, 6, 2)$ difference sets appearing in the 70 element PDS. These properties are discussed in the following section.

3.5 Linking Systems

We will notate the order four subgroups making up our $(512, 70, 6, 10)$ PDS as H_i and the $(16, 6, 2)$ difference sets as D_i (such that $E_i = H_i \cup D_i$).

We know that our PDS D is, in group ring notation, $D = \sum_{i=0}^{6} H_i + D_i$. Then DD^{-1} will yield some terms of the form $D_i - D_j$. Since D is a PDS, DD^{-1} is highly structured; we may explore this structure by considering the $D_i - D_j$ terms. Indeed, [5] explores various applications of "linking systems" to partial difference sets.

Before we proceed, let us formally define a linking system.

Definition 3.1 (Linking Systems)**.** Let G be a finite group of order v and let $\ell \geq 1$. A collection of $\{D_{ij} | 0 \leq i, j \leq \ell\}$ of (v, k, λ) difference sets in G is a $(v, k\lambda; \ell + 1)$ linking system if there exist $\alpha, \beta \in \mathbb{Z}$ such that $D_{ij} = D_{ji}^{-1}$ for all $i \neq j$ and for all distinct $h, i, j \in \{0, ..., \ell\}$, we have that $D_{hi} + D_{ij} = \alpha D_{hj} + \beta(G - D_{hj})$.

Note that since $D_{ij}^{(-1)} = D_{ji}$, the second condition says that taking the pairwise differences between two of the difference sets always produces a third difference set α times and its complement β times.

To explore the possibility of a linking structure in our D_i, we computed all possible $D_i - D_j$. Note that each of these has 36 total differences.

Each $D_i - D_j$ was found to yield 30 distinct elements, with 24 of them appearing exactly once and 6 of them appearing exactly twice. Furthermore, each set of 6 repeated elements was computationally verified to be an additive coset of a $(16, 6, 2)$ difference set. However, none of them were able to be expressed as an additive coset of one of the D_i. That is, our set of D_i is not a linking system as defined in definition 3.1.

However, the existence of these repeats and the fact that they form a difference set appears to be evidence that the D_i form some generalization of a linking system. To better understand this structure, it is useful to think of the D_i as McFarland difference sets formed from three hyperplanes. In this case, the hyperplanes are additive subgroups generated by order two elements (i.e., subgroups isomorphic to $\mathbb{Z}_2$).

For clarity, we will consider only the $\mathbb{Z}_4^3$ part of each element (since the $GF(8)$ part of all elements in E_i is x^i, where x is the generator of the multiplicative group). For notational convenience, the element $(a, b, c) \in \mathbb{Z}_4$ will be written as abc below.

Viewed in this manner, we may write the D_i as

$$\begin{aligned}
D_0 &= (012 + \langle 020 \rangle) \cup (132 + \langle 220 \rangle) \cup (102 + \langle 200 \rangle) \\
D_1 &= (011 + \langle 022 \rangle) \cup (103 + \langle 202 \rangle) \cup (130 + \langle 220 \rangle) \\
D_2 &= (010 + \langle 020 \rangle) \cup (101 + \langle 202 \rangle) \cup (113 + \langle 222 \rangle) \\
D_3 &= (021 + \langle 002 \rangle) \cup (120 + \langle 200 \rangle) \cup (123 + \langle 202 \rangle) \\
D_4 &= (013 + \langle 022 \rangle) \cup (100 + \langle 200 \rangle) \cup (111 + \langle 222 \rangle) \\
D_5 &= (201 + \langle 002 \rangle) \cup (210 + \langle 020 \rangle) \cup (211 + \langle 022 \rangle) \\
D_6 &= (001 + \langle 002 \rangle) \cup (110 + \langle 220 \rangle) \cup (131 + \langle 222 \rangle).
\end{aligned}$$

Note that all seven non-identity order two elements appear as generators for hyperplanes. Indeed, let us consider these order two elements as points on a graph. We will define lines on this graph as follows: given two points a and b, there exists a line through a, b, and a third point c if and only if the generators of a and b sum to the generator of c. (Note that all generators are order two elements, so addition and subtraction are the same and therefore any two points on the line a, b, c will define the same line through a, b, c).

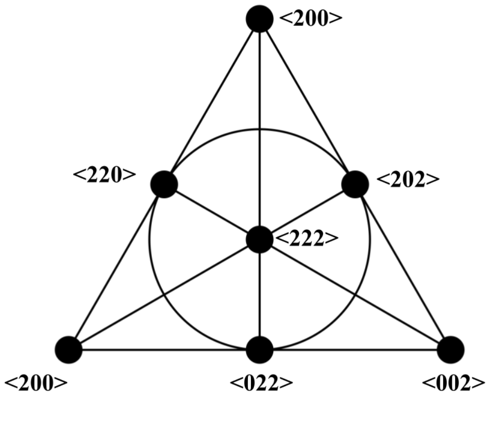


Figure 1: The Fano Plane

The graph shown in figure 1 is an important geometric object known as the Fano plane. The Fano plane is the projective plane of order 7 and has many useful symmetries. In particular, we note that any two points determine a line and any two lines intersect in one point. Likewise, each line has three points, and each point lies on three lines. Indeed, these symmetries allow us to map the points to lines and lines to points in an isomorphic way; for this reason, we say that the Fano plane is "self-dual."

Note that each of these lines corresponds to one of the seven D_i difference sets that make up our PDS (in the sense that each D_i is a union of additive cosets of three hyperplanes that lie on a line in figure 1).

Let us now consider $D_i - D_j$ from this perspective. We know that D_i, D_j correspond to distinct lines on the Fano plane. They therefore have one coset in common; let the generator of this coset be h_1. We may therefore write

$$D_i = (g_1 + \langle h_1\rangle) + (g_2 + \langle h_2\rangle) + (g_3 + \langle h_3\rangle)$$

and

$$D_j = (g_1' + \langle h_1\rangle) + (g_2' + \langle h_2'\rangle) + (g_3' + \langle h_3'\rangle).$$

Furthermore, we know that

$$h_1 = h_2 + h_3 = h_2' + h_3'. \tag{7}$$

Since these are all order two elements, it follows that $h_2 + h_3' = h_2' + h_3$ and that $h_2 + h_2' = h_3 + h_3'$.

We now consider $D_i - D_j$ as a sum of terms of the form $(g_a - g_b) + (\langle h_a\rangle - \langle h_b\rangle)$. Since $\langle h_a\rangle = \{0, h_a\}$ and $\langle h_b\rangle = \{0, h_b\}$, we have that $\langle h_a\rangle - \langle h_b\rangle = \{0, h_b, h_a, h_a - h_b\}$. In particular, when $h_a \neq h_b$, we may view this as $\langle h_a\rangle - \langle h_b\rangle = \{h_a, h_b\} \cup \langle h_a - h_b\rangle$ (because $h_a - h_b$ will always be an order two element).

Recalling $h_2 + h_3' = h_2' + h_3$ and that all h are order two, we have that

$$h_2 - h_3' = h_2 + h_3' = h_2' + h_3 = h_3 - h_2'. \tag{8}$$

Likewise, recalling that $h_2 + h_2' = h_3 + h_3'$, we have that

$$h_2 - h_2' = h_3 - h_3'. \tag{9}$$

Then it follows that $\langle h_2 - h_3'\rangle = \langle h_3 - h_2'\rangle$ is a subset of both $\langle h_2\rangle - \langle h_3'\rangle$ and $\langle h_3\rangle - \langle h_2'\rangle$. Similarly, $\langle h_2 - h_2'\rangle = \langle h_3 - h_3'\rangle$ is a subset of both $\langle h_2\rangle - \langle h_2'\rangle$ and $\langle h_3\rangle - \langle h_3'\rangle$.

Now suppose that the coset representatives on our hyperplanes obey similar subtraction laws: $g_2 - g_3' = g_3 - g_2'$ and $g_2 - g_2' = g_3 - g_3'$. Then we have $(g_2 - g_3') + \langle h_2 - h_3'\rangle$ appearing twice, once in the $\langle h_2\rangle - \langle h_3'\rangle$ term and again in the $\langle h_3\rangle - \langle h_2'\rangle$ term. Similarly, we will have $(g_2 - g_2') + \langle h_2 - h_2'\rangle$ appearing in both $\langle h_2\rangle - \langle h_2'\rangle$ and $\langle h_3\rangle - \langle h_3'\rangle$.

We know of one other hyperplane that will be repeated for a total of two times in the subtraction of $D_i - D_j$: the shared hyperplane $\langle h_1\rangle$. We know that $\langle h_1\rangle - \langle h_1\rangle = \{0, h_1, h_1, 0\} = 2\langle h_1\rangle$. It will appear with the coset representative $g_1 - g_1'$.

Finally, we now observe that the first repeated hyperplanes have generators $h_2 - h_3'$ and $h_2 - h_2'$. The sum of these generators is $h_2 - h_3' + h_2 - h_2'$. But since these are all order two, addition and subtraction are the same. Then the sum must in fact be equal to $h_2' + h_3' = h_1$, so the three repeated hyperplanes form a line in our Fano plane. In fact,we know which line it is. This line must contain $\langle h_1\rangle$; furthermore, the fact that D_i and D_j are distinct means that $\langle h_2 - h_3'\rangle$ and $\langle h_2 - h_2'\rangle$ cannot be points in either D_i or D_j. The only possible line is thus D_k, the third distinct line through the intersection point of D_i and D_k.

We have therefore shown that if the additive cosets obey the stated subtraction laws, then $(g_1 - g_1') + \langle h_1\rangle \cup (g_2 - g_3') + \langle h_2 - h_3'\rangle \cup (g_2 - g_2') + \langle h_2 - h_2'\rangle$ will be repeated for a total of two times. Furthermore, we know that these three hyperplanes form a line in our Fano plane and are therefore distinct. We then have a set of cosets of distinct hyperplanes, so the McFarland construction tells us that this set of six elements is in fact a $(16, 6, 2)$ difference set.

We have therefore shown that if the additive cosets obey the subtraction laws, then there will be six repeated elements that form a $(16, 6, 2)$ difference set.

We note that the coset representatives listed above are not the only possible way to write D. Indeed, given a coset representative g and a hyperplane $\langle 2g \rangle$, we know that $3g$ is also a possible coset representative. The above analysis of the subtraction law begs the question: is there a set of coset representatives that simultaneously obey the stated subtraction laws for all possible combinations?

A spot check of a few $D_i - D_j$ indicate that there seem to be choices of coset representatives that will do this for any particular i, j. Furthermore, the appealing properties of the analysis above (and the natural representation of D_i as lines on the Fano plane) suggest that such a choice likely exists. However, verifying this proposition (and then analyzing the structure of these coset representatives) is an important next step for the project.

We note another interesting observation that suggests the Fano plane is crucial to the structure of this PDS. By writing the hyperplanes as points on a Fano plane, we see that each hyperplane appears in exactly three different D_i. There is a coset rep g_i associated with the hyperplane in each of these. Computation shows that if you take the sum of these three g_i and call it s, the additive subgroup $\langle s \rangle$ is one of the $\mathbb{Z}_4$ subgroups that is contained within an E_i. Furthermore, the order two element of this subgroup is the generator of the hyperplane that we started with. In fact, this condition is sufficient to guarantee reversibility. Suppose that x is a coset representative for a hyperplane H and that $2x \in H$. Suppose the coset rep has at least one odd component. We know that the generators of the hyperplane are order two; the only other element of the hyperplane is the identity, so we may write an arbitrary hyperplane element as $2y$. Let $x + 2y \in x + H$; then $-(x + 2y) = 3x + 2y = x + (2x + 2y)$. But $2y \in H$ and $2x \in H$, so $x + (2x + 2y) \in x + H$. Thus $x + H$ contains $-(x + 2y)$, the additive inverse of our arbitrary element. Therefore $x + H$ is reversible; that is, if x is a coset representative and $2x \in H$, then $x + H$ is reversible. Since we ultimately wish to build a PDS out of such unions of cosets of hyperplanes, and we know that a PDS must be reversible, this is a desirable property.

In summary: empirical observations and initial analysis suggest that the Fano plane is key to the structure of this PDS. If we know which coset representatives to attach to the hyperplanes in the Fano plane, we are able to use the McFarland construction to get the seven $(16, 6, 2)$ difference sets that appear in the PDS, which we have called D_i. Furthermore, the coset representatives for a given hyperplane sum together to generate each of the seven $\mathbb{Z}_4$ subgroups H_j. Taken together, these D_i and H_j (with appropriate $GF(8)$ parts associated) form our 70 element PDS.

4 Conclusion and Future Work

In this thesis, we have explored several useful ways to analyze partial difference sets, including group rings and character theory. With these tools, we have taken two known examples of a partial difference set of size 70 in an abelian group of order 512. We discovered that in each case, the PDS may be thought of as a union of $(16, 6, 2)$ difference sets and order four subgroups.

We further found that the projective plane of order seven (i.e., the Fano plane) is a natural way to describe the PDS in the non-elementary abelian case. We introduced some exploratory theoretical analysis as well as some interesting empirical observations. Together, these motivate further study of how the Fano plane can provide a way to deeply understand this PDS. We made several conjectures and outlined several promising lines of inquiry. We discuss these in more detail below; the desirable combinatorial and geometric properties of the Fano plane give reason to suspect that these questions will help us achieve the project's ultimate goal of understanding the underlying structure of our non-elementary 70 element PDS and generalizing this structure to construct new partial difference sets.

To this end, our work suggests the following questions and conjectures.

A construction of this PDS using the Fano plane does not obviously suggest a relation between the $(16, 6, 2)$ D_i and which H_i it should correspond to. How do we know how to pair the D_i and H_i?

We speculated that there is a representation of D as a set of coset representatives and hyperplanes such that the coset representatives simultaneously satisfy our subtraction laws. Is this true? If so, what are those coset representatives?

We showed that given coset representatives that obey the required subtraction laws, a $(16, 6, 2)$ difference set would be a subset of the repeated elements in $D_i - D_j$. Computationally, we know that these are all such elements. How can we prove this?

The coset representatives obey a subtraction law and interact in such a way that the lines in the Fano plane exhibit a behavior that can be regarded as a generalization of a linking system. What is the best way to define such a generalization of linking? How can we know a priori what the coset representatives should be? Once we have the set of coset representatives, how do we know which ones to associate with which lines? (I.e., given a coset representative, we know which point on the Fano plane corresponds to this element. However, each point has three such representatives associated with it. How do we know which three coset representatives should form a line?)

Once these questions are understood, it seems plausible that a geometric construction of the 70 element non-elementary abelian PDS will become apparent. (This is particularly appealing since our present understanding is that the Fano plane is the fundamental structure behind this PDS. The Fano plane is a projective plane of order 7, and there are several known constructions of finite projective planes).

Finally, we know of a Denniston partial difference set of size 70 in the elementary abelian group of order 512. It has a similar structure to the non-elementary Denniston case in that it is a union of seven sets of ten, each of which are themselves a $(16, 6, 2)$ difference set plus a subgroup of order four. Does the Fano plane appear as a natural way to understand this partial difference set? If so, how does the description of this PDS in terms of projective planes relate to the description of the non-elementary abelian case? Does this relationship suggest anything about a larger family of partial difference sets?

5 Acknowledgements

The author would like to thank Dr. Jim Davis for his mentorship and constant support throughout this project. The author also thanks Dr. Della Dumbaugh for her thoughts and editorial suggestions, as well as Dr. John Polhill and Dr. Ken Smith for insightful

conversations about partial difference sets.

6 Appendix

6.1 Elementary $(512, 70, 6, 10)$ PDS

Here, we list the elements of our Denniston $(512, 70, 6, 10)$ PDS in $\mathbb{Z}_2^9 \cong \mathbb{Z}_2^3 \times \mathbb{Z}_2^6$. These appear in tables that list the $\mathbb{Z}_2^6$ components for each E_i. The $\mathbb{Z}_2^3$ component for each element in E_i is α^i, where α is the generator for the multiplicative group of the field $GF(2^3)$.

H_0	D_0
(0,0,0,0,0,0)	(0,1,0,1,0,0)
(0,0,0,0,0,1)	(0,1,0,1,1,0)
(0,0,1,0,0,0)	(1,1,0,0,1,0)
(0,0,1,0,0,1)	(1,1,0,1,0,0)
	(1,0,0,0,1,0)
	(1,0,0,1,1,0)

Table 2: Elements of E_0.

H_1	D_1
(0,0,0,0,0,0)	(1,0,0,0,1,1)
(0,0,0,0,1,0)	(1,0,0,0,1,1)
(0,1,0,0,0,0)	(0,1,1,1,0,0)
(0,1,0,0,1,0)	(0,1,1,1,1,1)
	(1,1,1,1,0,0)
	(1,1,1,0,1,1)

Table 3: Elements of E_1.

H_2	D_2
(0,0,0,0,0,0)	(0,1,1,1,1,0)
(0,0,0,1,0,0)	(0,1,1,1,0,1)
(1,0,0,0,0,0)	(1,1,0,0,1,1)
(1,0,0,1,0,0)	(1,1,0,1,0,1)
	(1,0,1,0,1,1)
	(1,0,1,1,1,0)

Table 4: Elements of E_2.

H_3	D_3
(0,0,0,0,0,0)	(1,1,0,1,1,1)
(0,0,0,0,1,1)	(1,1,0,0,0,1)
(0,1,1,0,0,0)	(1,1,1,1,1,0)
(0,1,1,0,1,1)	(1,1,1,0,0,1)
	(0,0,1,1,1,0)
	(0,0,1,1,1,1)

Table 5: Elements of E_3.

H_4	D_4
(0,0,0,0,0,0)	(1,1,1,1,0,1)
(0,0,0,1,1,0)	(1,1,1,0,1,0)
(1,1,0,0,0,0)	(1,0,1,1,1,1)
(1,1,0,1,1,0)	(1,0,1,0,1,0)
	(0,1,0,1,1,1)
(0,1,0,1,0,1)	

Table 6: Elements of E_4.

H_5	D_5
(0,0,0,0,0,0)	(1,0,1,0,0,1)
(0,0,0,1,1,1)	(1,0,1,1,0,0)
(1,1,1,0,0,0)	(0,0,1,1,0,1)
(1,1,1,1,1,1)	(0,0,1,1,0,0)
	(1,0,0,1,0,1)
(1,0,0,0,0,1)	

Table 7: Elements of E_5.

H_6	D_6
(0,0,0,0,0,0)	(0,0,1,0,1,0)
(0,0,0,1,0,1)	(0,0,1,0,1,1)
(1,0,1,0,0,0)	(0,1,0,0,0,1)
(1,0,1,1,0,1)	(0,1,0,0,1,1)
	(0,1,1,0,0,1)
	(0,1,1,0,1,0)

Table 8: Elements of E_6.

6.2 Non-Elementary $(512, 70, 6, 10)$ PDS

Here, we list the elements of our $(512, 70, 6, 10)$ PDS in $\mathbb{Z}_2^3 \times \mathbb{Z}_4^3$. These appear in tables that list the $\mathbb{Z}_4^3$ components for each E_i. The $\mathbb{Z}_2^3$ component for each element in E_i is α^i, where α is the generator for the multiplicative group of the field $GF(2^3)$.

H_0	D_0
(0,0,0)	(0,1,2)
(0,0,2)	(0,3,2)
(2,2,1)	(1,0,2)
(2,2,3)	(3,0,2)
	(1,3,2)
	(3,1,2)

Table 9: Elements of E_0.

H_1	D_1
(0,0,0)	(0,1,1)
(2,1,2)	(0,3,3)
(0,2,0)	(1,0,3)
(2,3,2)	(3,0,1)
	(3,1,0)
	(1,3,0)

Table 10: Elements of E_1.

H_2	D_2
(0,0,0)	(0,1,0)
(1,2,2)	(0,3,0)
(2,0,0)	(1,0,1)
(3,2,2)	(3,0,3)
	(1,1,3)
	(3,3,1)

Table 11: Elements of E_2.

H_3	D_3
(0,0,0)	(0,2,1)
(2,1,3)	(0,2,3)
(0,2,2)	(1,2,0)
(2,3,1)	(3,2,0)
	(1,2,3)
	(3,2,1)

Table 12: Elements of E_3.

H_4	D_4
(0,0,0)	(0,1,3)
(1,1,2)	(0,3,1)
(2,2,0)	(1,0,0)
(3,3,2)	(3,0,0)
	(1,1,1)
	(3,3,3)

Table 13: Elements of E_4.

H_5	D_5
(0,0,0)	(2,0,1)
(1,3,3)	(2,0,3)
(2,2,2)	(2,1,0)
(3,1,1)	(2,3,0)
	(2,1,1)
	(2,3,3)

Table 14: Elements of E_5.

H_6	D_6
(0,0,0)	(0,0,1)
(1,2,1)	(0,0,3)
(2,0,2)	(1,1,0)
(3,2,3)	(3,3,0)
	(1,3,1)
	(3,1,3)

Table 15: Elements of E_6.

6.3 Additional Theorems: Difference Sets

Theorem 6.1. Let G be an abelian group of order v and D a subset of G of order k. Then D is a (v, k, λ) difference set in G if and only if $k^2 = \lambda(v-1) + k$ and $|\chi(D)| = \sqrt{k-\lambda}$ for any nonprincipal character $\chi : G \to \mathbb{C}^*$.

We will give a proof that essentially follows the proofs of theorems 1.15 and 1.15. However, the simpler expression for the character sum makes this argument more straightforward.

To begin, we note that we can make a counting argument about difference sets similar to theorem 1.7. All possible differences of elements of a (v, k, λ) difference set D is a set of k^2 possible differences simply by the size of D. However, we know that these differences produce the $v-1$ nonidentity elements λ times and the identity element k times. Thus $k^2 = \lambda(v-1) + k$.

We will now prove the theorem at hand.

Proof: Suppose that D is a (v, k, λ) difference set in G and χ is an arbitrary nonprincipal character. In group ring notation, this means that $DD^{(-1)} = \lambda(G - 1_G) + k1_G = \lambda G + (k-\lambda)1_G$. Then we have that $\chi(DD^{(}-1)) = \lambda\chi(G) + (k-\lambda)\chi(1_G)$. But we know that $\chi(1_G) = 1$ and $\chi(G) = 0$, so $\chi(DD^{(-1)} = k - \lambda$.

Unlike a PDS, a difference set need not be reversible. However, we know that $\chi(g^{-1}) = \overline{\chi(g)}$, so we have that $\chi(D^{(-1)}) = \overline{\chi(D)}$. Then it follows that $\chi(DD^{(-1)}) = \chi(D)\chi(D^{(-1)} = \chi(D)\overline{\chi(D)} = |\chi(D)|^2$. Therefore $|\chi(D)| = \sqrt{k-\lambda}$.

Conversely, suppose that $|\chi(D)| = \sqrt{k-\lambda}$ for any nonprincipal character χ. Then we have that $|\chi(D)|^2 = k - \lambda$. But we have just argued that $\chi(D^{(-1)}) = \overline{\chi(D)}$, so $|\chi(D)|^2 = \chi(D)\overline{\chi(D)} = \chi(D)\chi(D^{(-1)}) = \chi(DD^{(-1)})$.

Therefore $\chi(DD^{(-1)}) = k-\lambda$ for any nonprincipal character χ. Now consider the group ring element $\mathcal{D} = \lambda(G-1_G) + k1_G = \lambda G + (k-\lambda)1_G$. Then $\chi(\mathcal{D}) = \chi(\lambda G + (k-\lambda)1_G) = \lambda\chi(G) + (k-\lambda)\chi(1_G) = k - \lambda$ for any nonprincipal character χ.

Then $\chi(\mathcal{D}) = \chi(DD^{(-1)}$ for any nonprincipal character χ. For the principal character χ_0, we can see that $\chi_0(DD^{-1}) = k^2$ and that $\chi_0(\lambda(G-1_G) + k1_G) = \lambda\chi_0(G-1_G) +$

$k\chi_0(1_G) = \lambda(v-1)+k$. But we know that $k^2 = \lambda(v-1)+k$ by hypothesis, so we have that $\chi(DD^{(-1)}) = \chi(\lambda(G-1_G)+k1_G)$ for any character χ. By corollary 1.17.1, it follows that $DD^{(-1)} = \lambda(G-1_G)+k1_G$. This is the character ring criterion for D to be a (v,k,λ) difference set in G. □

6.4 Additional Theorems: Paley Squares

We examined small cases of the Paley squares as examples of partial difference sets. We will now prove that these objects form an infinite family of partial difference sets.

Theorem 6.2. The set D of nonzero quadratic residues of $\mathbb{Z}_p$ where p is prime is a partial difference set.

Note: If x is a group element, I will use $-x$ to denote the additive inverse and x^{-1} to denote the multiplicative inverse. Since p is prime, we know that every nonzero element has a multiplicative inverse. Every element has an additive inverse by definition of a group.

Lemma 6.3. $0 \notin D$, where D is as described above.

Proof: Suppose that there exists an integer a such that $0 < a < p$ but $a^2 = 0$. Then $p \mid a^2$. By Euclid's Lemma, $p \mid a$. But $a > 0$, so $p \leq a$. This is a contradiction. Thus we conclude that if $0 < a < p$, it must be the case that $a^2 \neq 0$. □

Lemma 6.4. There are $\frac{p-1}{2}$ distinct squares in $\mathbb{Z}_p$.

Proof: Define $S = 1^2, 2^2, ..., (\frac{p-1}{2})^2$. We claim that this is the set of all of the squares.

Let $\frac{p-1}{2} < x < p$. Then $p - x = y$, where $0 < y < \frac{p-1}{2}$. Therefore $x = p - y$. But $p - y = -y$, so $x = -y$. Thus $x^2 = (-y)^2 = y^2$, so $x^2 \in S$. Thus the set of squares is a subset of S.

Now we will show that all of the elements of S are distinct. Suppose that there exist $x, y \in S$ that are not distinct: then there exist $0 < a, b \leq \frac{p-1}{2}$ such that $a > b$ but $a^2 = b^2$. Then $p|a^2 - b^2$, so $p|(a-b)(a+b)$. By Euclid's Lemma, either $p|a-b$ or $p|a+b$.

Suppose that $p|(a-b)$. Then, since $a - b > 0$, it follows that $p \leq a - b \leq \frac{p-1}{2} - 0 < p$. This is a contradiction.

Suppose then that $p|(a+b)$. But $a, b \leq \frac{p-1}{2}$, so $a + b \leq \frac{p-1}{2} + \frac{p-1}{2} = p - 1 < p$. Since $a + b > 0$ and $p|(a+b)$, we know that $p < a + b < p$. This is a contradiction.

Therefore $a^2 \neq b^2$, so all elements of S are distinct and S is therefore the set of all of the quadratic residues. Thus there are $\frac{p-1}{2}$ squares mod p. □

Corollary 6.4.1. There are $\frac{p-1}{2}$ nonzero nonsquares.

Lemma 6.5. If a^2, b^2 are squares, then a^2b^2 is also a square.

Proof: Let $ab = c$. Then $(ab-c)(ab+c) = a^2b^2 - c^2$. Furthermore, since $c = ab$, it must be the case that $p \mid ab - c$. Therefore $p \mid (ab-c)(ab+c) = a^2b^2 - c^2$, so $a^2b^2 = c^2$. That is, D is closed under multiplication. □

Lemma 6.6. The set of squares S and the set of nonzero nonsquares N are both closed under multiplicative inversion.

Proof: Since all of the nonzero elements are relatively prime to p, we know that each nonzero element has a multiplicative inverse.

For any group element, $a^{-2} = (a^{-1})^2$. Since a^{-1} is also a group element, it follows that $a^{-2} = (a^{-1})^2$ is a square. Thus the squares are closed under multiplicative inversion.

Since the squares are closed under multiplicative inversion, none of the multiplicative inverses of the elements of N are in S. Since each multiplicative inverse is nonzero, the inverses not in S must be in N. Thus all of the inverses are in N, so N is closed under multiplicative inversion. □

Lemma 6.7. *If $x \in S$ and $y \in N$, the $xy \in N$. If $g, h \in N$, then $gh \in S$.*

Proof: Let $x \in S$ and $y \in N$. We know that $xy \neq 0$: if it were, Euclid's lemma would imply that one of them is zero. Suppose then that $xy \in S$. Then there exists a $g \in \mathbb{Z}$ such that $xy = g^2$. Therefore $y = x^{-1}g^2$. Since the squares are closed under multiplicative inversion, this is a product of two squares, which must also be square. Thus $y \in S$. This is a contradiction, so $xy \in N$.

Now, for a given square, define the set $F(a^2) = \{a^2g | g \in N\}$. By cancellation, a^2g is distinct for each g. Since we have $\frac{p-1}{2}$ distinct nonsquares, there are $\frac{p-1}{2}$ distinct elements in $F(a^2)$. We know that zero is not in the set, since neither a^2 nor g is zero. Furthermore, we know that a product of a square and a nonsquare is a nonsquare, so each element of $F(a^2)$ is a nonsquare. Then we have $\frac{p-1}{2}$ distinct nonzero nonsquares in $F(a^2)$, so it follows that $F(a^2) = N$.

Then for every square a^2 and nonsquare h, there is exactly one $g \in N$ such that $a^2g = h$. Thus $hg{-}1 = a^2$.

Fix a nonsquare h. For each of the $\frac{p-1}{2}$ squares, the nonsquare g such that $a^2 = hg^{-1}$ is distinct (since inverses are unique and products are well defined). Thus there are $\frac{p-1}{2}$ distinct nonsquares g such that $hg^{-1} \in S$. But there are only $\frac{p-1}{2}$ distinct nonsquares, so for all nonsquares h, g, it follows that $hg^{-1} \in S$. Since N is closed under multiplicative inversion, $g^{-1} \in N$. Thus $h, g^{-1} \in N$, so $h(g^{-1})^{-1} = hg \in S$. Thus the product of two nonsquares is always square. □

With these lemmas, we are now equipped to prove the main theorem.

Proof: Suppose that there exist $a, b \in \mathbb{Z}$ such that $1 = a^2 - b^2$. Then for any square g^2, we have that $g^2 = g^2a^2 - g^2b^2$. But D is closed under multiplication, so $g^2a^2 - g^2b^2$ is a difference of squares. Then each difference of squares solution for one generates a difference of squares solution for each g^2.

Let g^2 be fixed. Then, by the cancellation property, $g^2a^2 = g^2a'^2$ if and only if $a = a'$. Therefore each distinct difference of squares solution for one corresponds to a distinct difference of squares solution for g^2.

Now let g^2 again be an arbitrary nonzero square. Suppose that there exist x, y such that $g^2 = x^2 - y^2$. Then, since D is closed under multiplication, it must be true that $1 = g^2g^{-2} = g^{-2}x^2 - g^{-2}y^{-2}$ is a difference of squares equal to one. Therefore each difference of squares solution for an arbitrary g^2 generates a difference of squares solution for 1.

Let g^2 be fixed. Then, by the cancellation property, $g^{-2}x^2 = g^{-2}x'^2$ if and only if $x = x'$. Therefore each distinct difference of squares solution for g^2 corresponds to a distinct difference of squares solution for g^2.

Thus we have that each element d_0 of D has the same number of solutions $d_0 = d_1d_2^{-1}$, where $d_1, d_2 \in D$. This proves that the parameter λ exists.

Fix an $h \in N$. Suppose that there exist $a, b \in \mathbb{Z}$ such that $h = a^2 - b^2$.

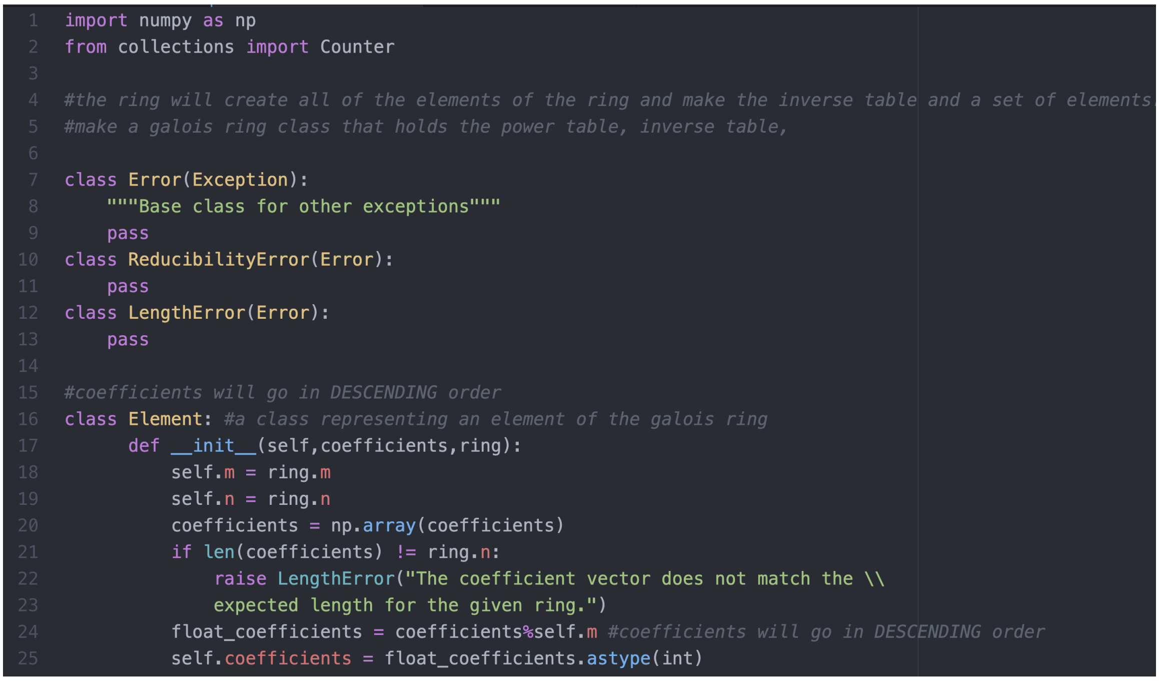
Then for each $g \in N$, we have that $g = gh^{-1}h = (gh^{-1})a^2 - (gh^{-1})b^2$. Since $gh^{-1} \in S$, this is a difference of squares solution for g. By the cancellation property, the solutions for g generated in this way are distinct so long as the solutions for h are distinct. Thus each nonsquare g has at least as many difference of squares solutions as h does.

But h was an arbitrary element of N. Therefore no element h' of N could have more difference of squares than any other element of N; if it did, we could simply let $h = h'$, and this would give us a contradiction.

Thus every element in N has the same number of difference of squares solutions, so the parameter μ exists. Thus D is a PDS. □

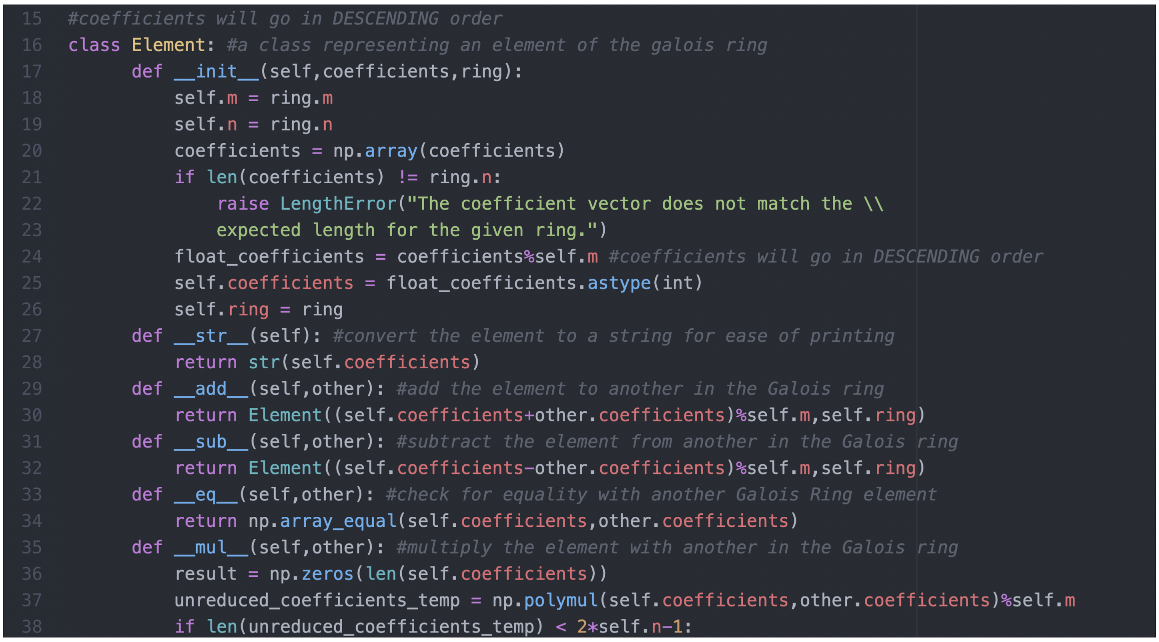
6.5 Sample Code

Here, we include some sample code as described in section 3.4. More complete code is available by request to the author.



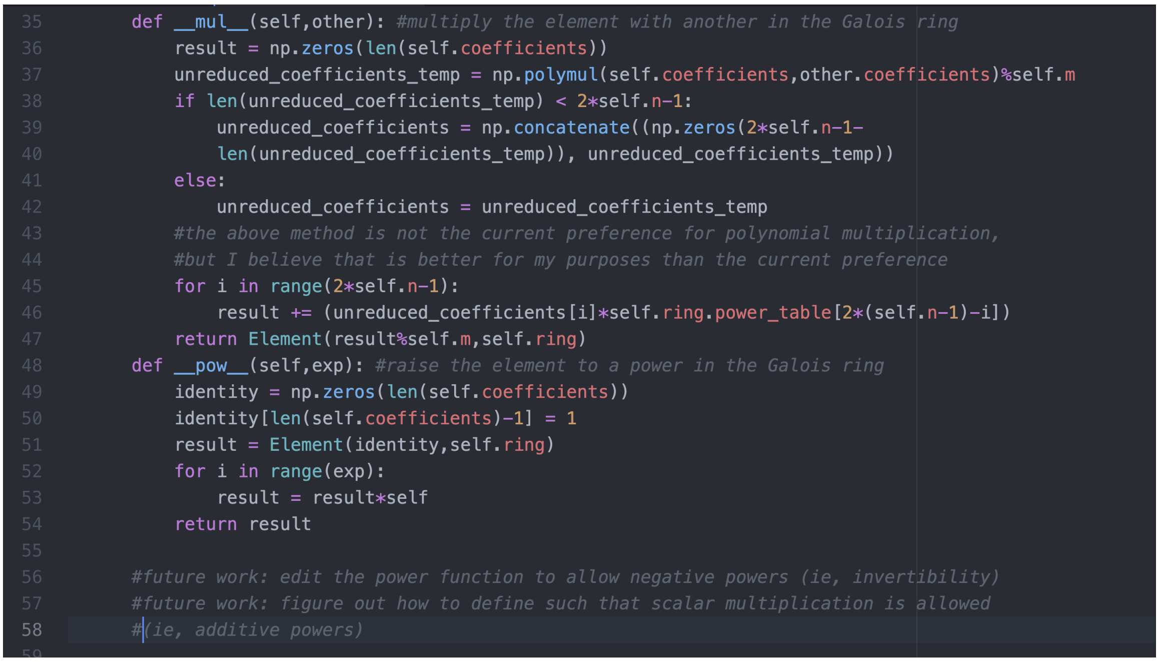
```python
import numpy as np
from collections import Counter

#the ring will create all of the elements of the ring and make the inverse table and a set of elements.
#make a galois ring class that holds the power table, inverse table,

class Error(Exception):
    """Base class for other exceptions"""
    pass
class ReducibilityError(Error):
    pass
class LengthError(Error):
    pass

#coefficients will go in DESCENDING order
class Element: #a class representing an element of the galois ring
      def __init__(self,coefficients,ring):
          self.m = ring.m
          self.n = ring.n
          coefficients = np.array(coefficients)
          if len(coefficients) != ring.n:
              raise LengthError("The coefficient vector does not match the \\
              expected length for the given ring.")
          float_coefficients = coefficients%self.m #coefficients will go in DESCENDING order
          self.coefficients = float_coefficients.astype(int)
```

Figure 2: A code sample from “galois-ring.py”.



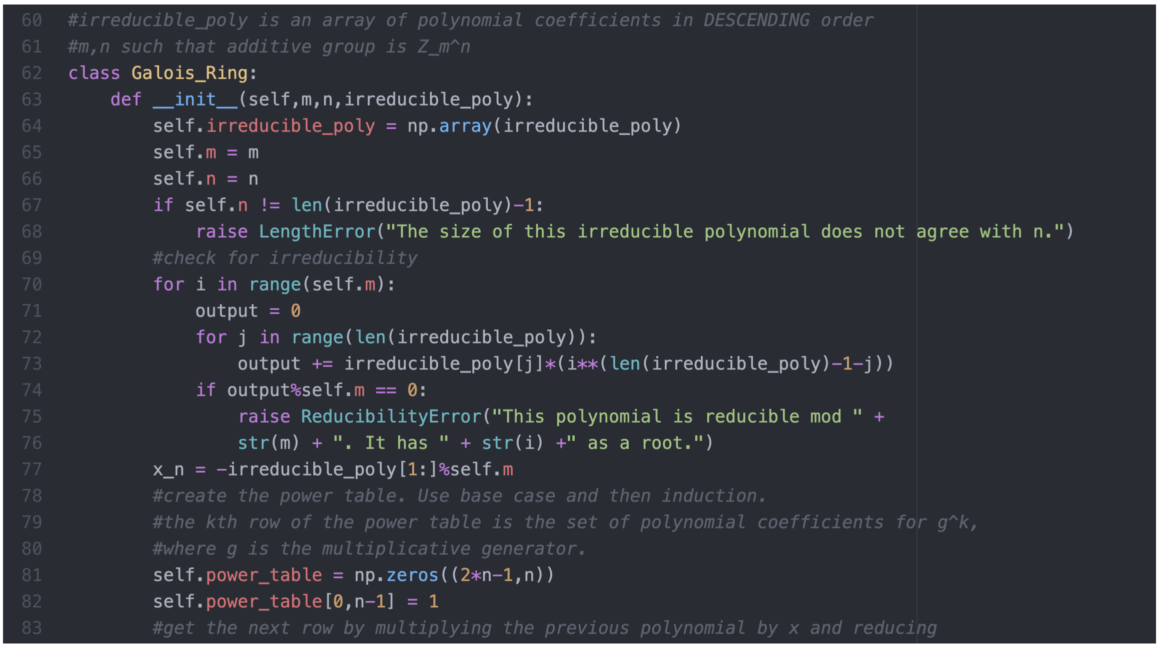
```
#coefficients will go in DESCENDING order
class Element: #a class representing an element of the galois ring
      def __init__(self,coefficients,ring):
          self.m = ring.m
          self.n = ring.n
          coefficients = np.array(coefficients)
          if len(coefficients) != ring.n:
              raise LengthError("The coefficient vector does not match the \\
              expected length for the given ring.")
          float_coefficients = coefficients%self.m #coefficients will go in DESCENDING order
          self.coefficients = float_coefficients.astype(int)
          self.ring = ring
      def __str__(self): #convert the element to a string for ease of printing
          return str(self.coefficients)
      def __add__(self,other): #add the element to another in the Galois ring
          return Element((self.coefficients+other.coefficients)%self.m,self.ring)
      def __sub__(self,other): #subtract the element from another in the Galois ring
          return Element((self.coefficients-other.coefficients)%self.m,self.ring)
      def __eq__(self,other): #check for equality with another Galois Ring element
          return np.array_equal(self.coefficients,other.coefficients)
      def __mul__(self,other): #multiply the element with another in the Galois ring
          result = np.zeros(len(self.coefficients))
          unreduced_coefficients_temp = np.polymul(self.coefficients,other.coefficients)%self.m
          if len(unreduced_coefficients_temp) < 2*self.n-1:
```

Figure 3: A code sample from “galois-ring.py”.



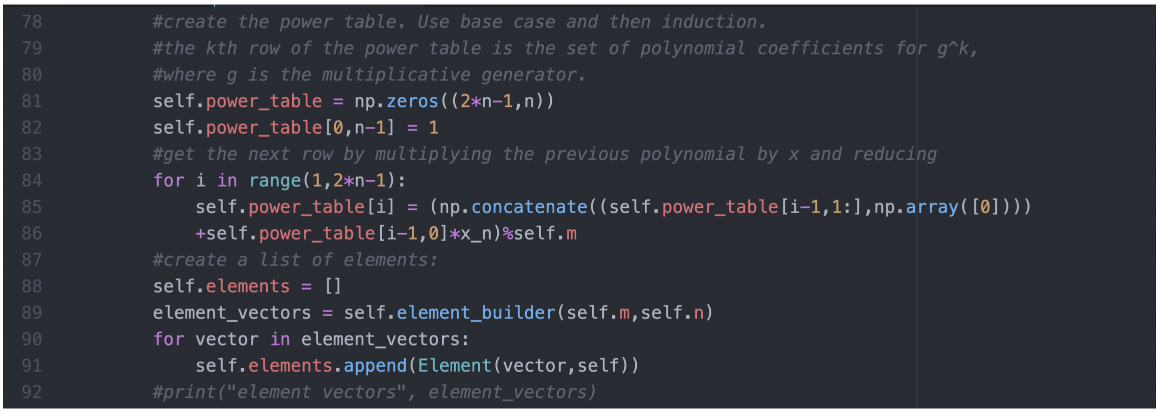
```
      def __mul__(self,other): #multiply the element with another in the Galois ring
          result = np.zeros(len(self.coefficients))
          unreduced_coefficients_temp = np.polymul(self.coefficients,other.coefficients)%self.m
          if len(unreduced_coefficients_temp) < 2*self.n-1:
              unreduced_coefficients = np.concatenate((np.zeros(2*self.n-1-
              len(unreduced_coefficients_temp)), unreduced_coefficients_temp))
          else:
              unreduced_coefficients = unreduced_coefficients_temp
          #the above method is not the current preference for polynomial multiplication,
          #but I believe that is better for my purposes than the current preference
          for i in range(2*self.n-1):
              result += (unreduced_coefficients[i]*self.ring.power_table[2*(self.n-1)-i])
          return Element(result%self.m,self.ring)
      def __pow__(self,exp): #raise the element to a power in the Galois ring
          identity = np.zeros(len(self.coefficients))
          identity[len(self.coefficients)-1] = 1
          result = Element(identity,self.ring)
          for i in range(exp):
              result = result*self
          return result

      #future work: edit the power function to allow negative powers (ie, invertibility)
      #future work: figure out how to define such that scalar multiplication is allowed
      #(ie, additive powers)
```

Figure 4: A code sample from “galois-ring.py”.



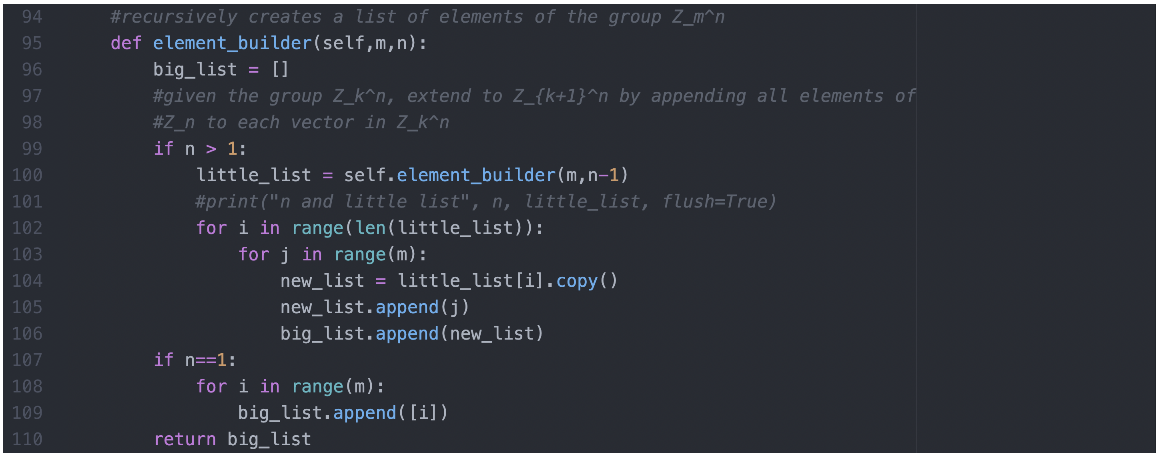
```
#irreducible_poly is an array of polynomial coefficients in DESCENDING order
#m,n such that additive group is Z_m^n
class Galois_Ring:
    def __init__(self,m,n,irreducible_poly):
        self.irreducible_poly = np.array(irreducible_poly)
        self.m = m
        self.n = n
        if self.n != len(irreducible_poly)-1:
            raise LengthError("The size of this irreducible polynomial does not agree with n.")
        #check for irreducibility
        for i in range(self.m):
            output = 0
            for j in range(len(irreducible_poly)):
                output += irreducible_poly[j]*(i**(len(irreducible_poly)-1-j))
            if output%self.m == 0:
                raise ReducibilityError("This polynomial is reducible mod " +
                str(m) + ". It has " + str(i) +" as a root.")
        x_n = -irreducible_poly[1:]%self.m
        #create the power table. Use base case and then induction.
        #the kth row of the power table is the set of polynomial coefficients for g^k,
        #where g is the multiplicative generator.
        self.power_table = np.zeros((2*n-1,n))
        self.power_table[0,n-1] = 1
        #get the next row by multiplying the previous polynomial by x and reducing
```

Figure 5: A code sample from “galois-ring.py”.



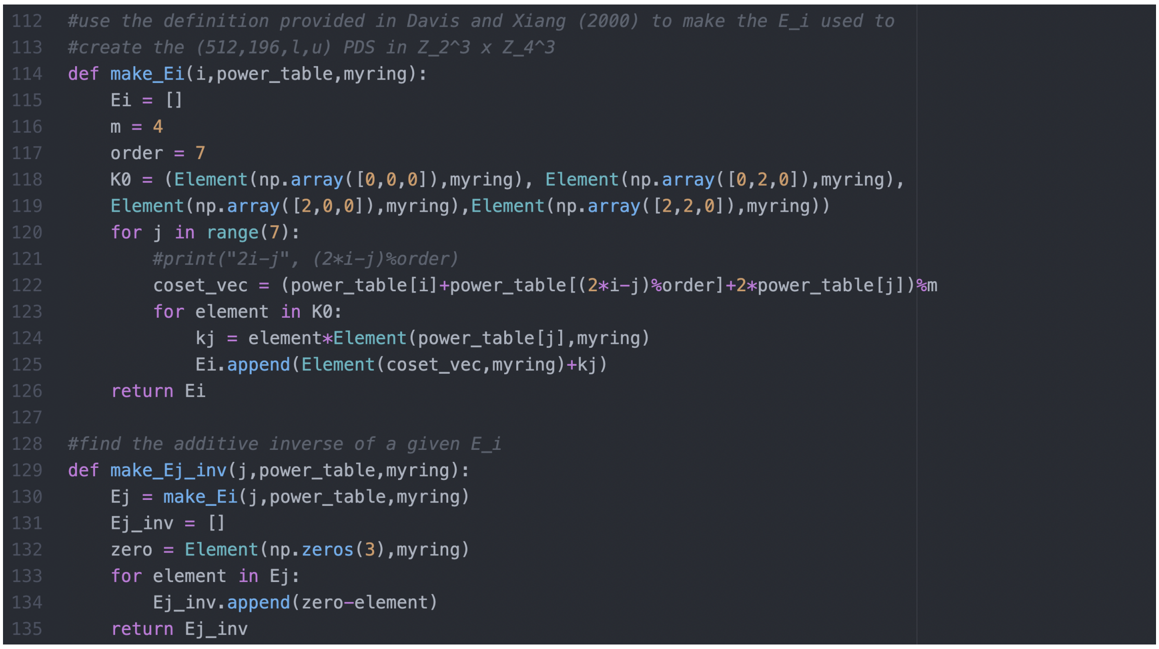
```
        #create the power table. Use base case and then induction.
        #the kth row of the power table is the set of polynomial coefficients for g^k,
        #where g is the multiplicative generator.
        self.power_table = np.zeros((2*n-1,n))
        self.power_table[0,n-1] = 1
        #get the next row by multiplying the previous polynomial by x and reducing
        for i in range(1,2*n-1):
            self.power_table[i] = (np.concatenate((self.power_table[i-1,1:],np.array([0])))
            +self.power_table[i-1,0]*x_n)%self.m
        #create a list of elements:
        self.elements = []
        element_vectors = self.element_builder(self.m,self.n)
        for vector in element_vectors:
            self.elements.append(Element(vector,self))
        #print("element vectors", element_vectors)
```

Figure 6: A code sample from “galois-ring.py”.



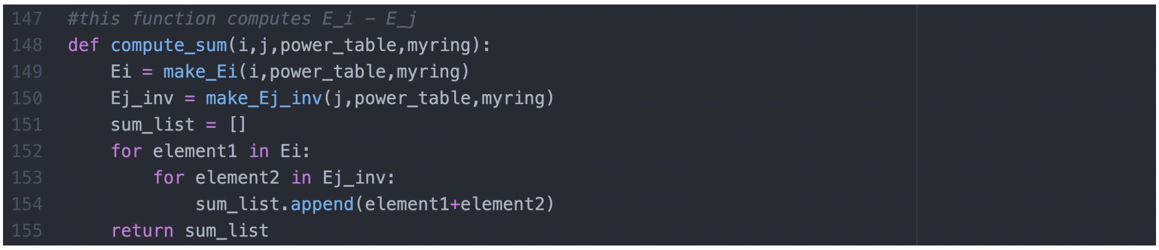
```
    #recursively creates a list of elements of the group Z_m^n
    def element_builder(self,m,n):
        big_list = []
        #given the group Z_k^n, extend to Z_{k+1}^n by appending all elements of
        #Z_n to each vector in Z_k^n
        if n > 1:
            little_list = self.element_builder(m,n-1)
            #print("n and little list", n, little_list, flush=True)
            for i in range(len(little_list)):
                for j in range(m):
                    new_list = little_list[i].copy()
                    new_list.append(j)
                    big_list.append(new_list)
        if n==1:
            for i in range(m):
                big_list.append([i])
        return big_list
```

Figure 7: A code sample from “galois-ring.py”.



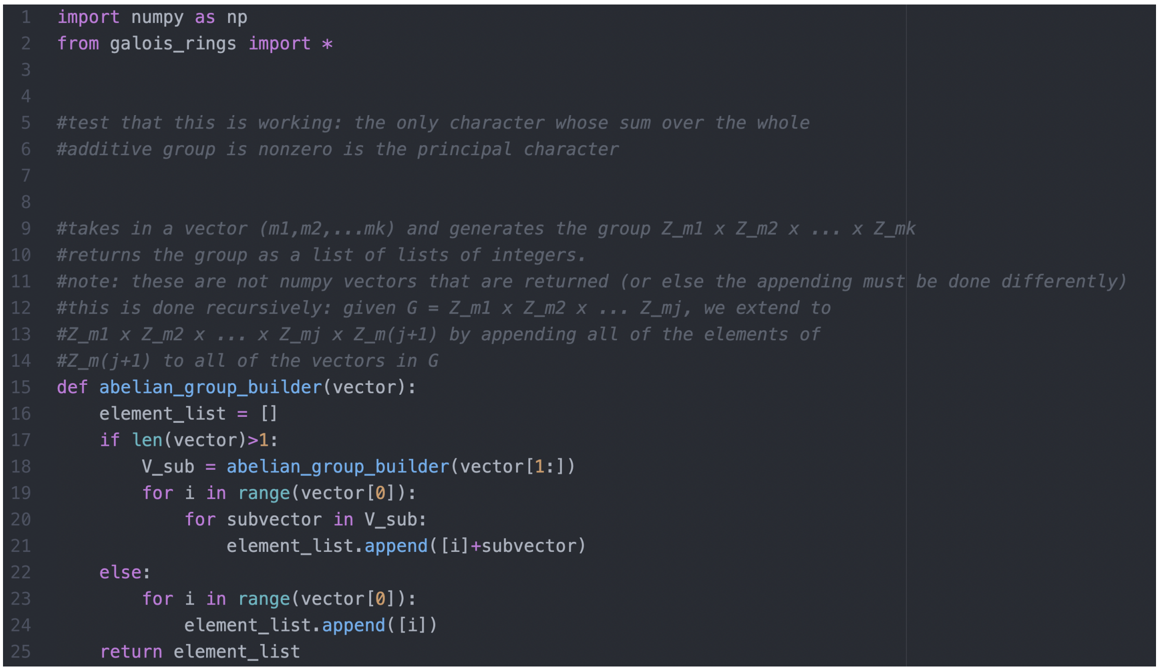
```python
#use the definition provided in Davis and Xiang (2000) to make the E_i used to
#create the (512,196,l,u) PDS in Z_2^3 x Z_4^3
def make_Ei(i,power_table,myring):
    Ei = []
    m = 4
    order = 7
    K0 = (Element(np.array([0,0,0]),myring), Element(np.array([0,2,0]),myring),
    Element(np.array([2,0,0]),myring),Element(np.array([2,2,0]),myring))
    for j in range(7):
        #print("2i-j", (2*i-j)%order)
        coset_vec = (power_table[i]+power_table[(2*i-j)%order]+2*power_table[j])%m
        for element in K0:
            kj = element*Element(power_table[j],myring)
            Ei.append(Element(coset_vec,myring)+kj)
    return Ei

#find the additive inverse of a given E_i
def make_Ej_inv(j,power_table,myring):
    Ej = make_Ei(j,power_table,myring)
    Ej_inv = []
    zero = Element(np.zeros(3),myring)
    for element in Ej:
        Ej_inv.append(zero-element)
    return Ej_inv
```

Figure 8: A code sample from “galois-ring.py”.



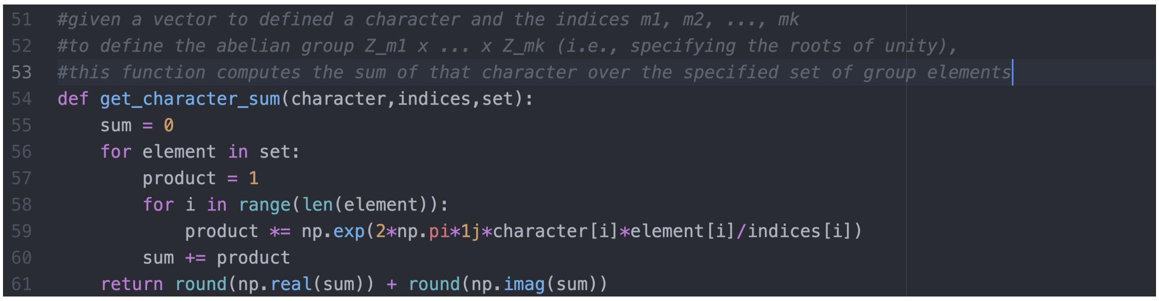
```python
#this function computes E_i - E_j
def compute_sum(i,j,power_table,myring):
    Ei = make_Ei(i,power_table,myring)
    Ej_inv = make_Ej_inv(j,power_table,myring)
    sum_list = []
    for element1 in Ei:
        for element2 in Ej_inv:
            sum_list.append(element1+element2)
    return sum_list
```

Figure 9: A code sample from “galois-ring.py”.



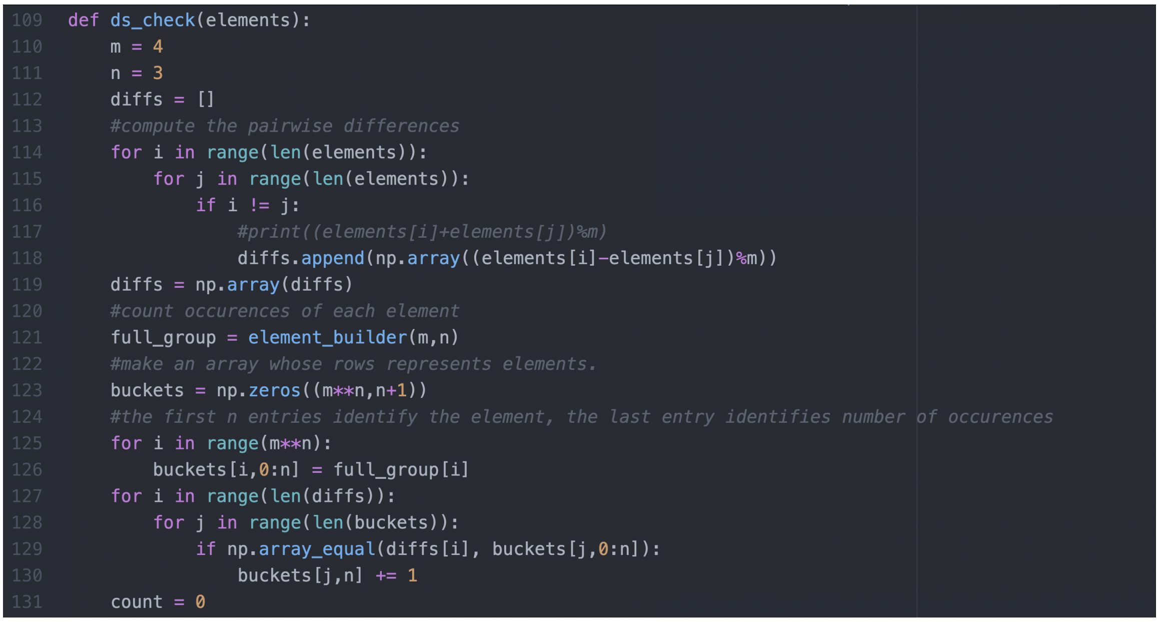
```python
import numpy as np
from galois_rings import *


#test that this is working: the only character whose sum over the whole
#additive group is nonzero is the principal character


#takes in a vector (m1,m2,...mk) and generates the group Z_m1 x Z_m2 x ... x Z_mk
#returns the group as a list of lists of integers.
#note: these are not numpy vectors that are returned (or else the appending must be done differently)
#this is done recursively: given G = Z_m1 x Z_m2 x ... Z_mj, we extend to
#Z_m1 x Z_m2 x ... x Z_mj x Z_m(j+1) by appending all of the elements of
#Z_m(j+1) to all of the vectors in G
def abelian_group_builder(vector):
    element_list = []
    if len(vector)>1:
        V_sub = abelian_group_builder(vector[1:])
        for i in range(vector[0]):
            for subvector in V_sub:
                element_list.append([i]+subvector)
    else:
        for i in range(vector[0]):
            element_list.append([i])
    return element_list
```

Figure 10: A code sample from “PDS-list-generator2.py”.



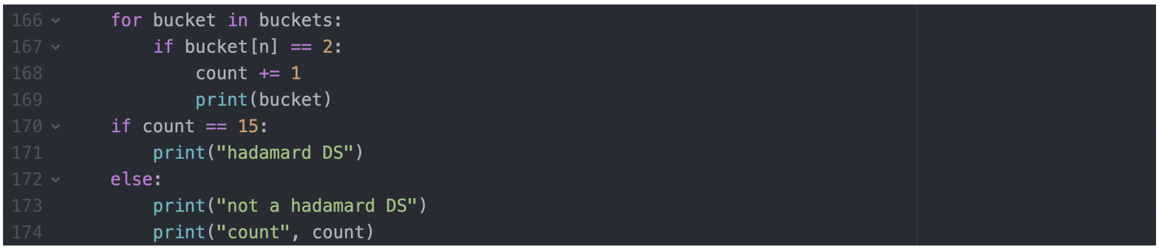
```python
#given a vector to defined a character and the indices m1, m2, ..., mk
#to define the abelian group Z_m1 x ... x Z_mk (i.e., specifying the roots of unity),
#this function computes the sum of that character over the specified set of group elements
def get_character_sum(character,indices,set):
    sum = 0
    for element in set:
        product = 1
        for i in range(len(element)):
            product *= np.exp(2*np.pi*1j*character[i]*element[i]/indices[i])
        sum += product
    return round(np.real(sum)) + round(np.imag(sum))
```

Figure 11: A code sample from “PDS-list-generator2.py”.



```python
def ds_check(elements):
    m = 4
    n = 3
    diffs = []
    #compute the pairwise differences
    for i in range(len(elements)):
        for j in range(len(elements)):
            if i != j:
                #print((elements[i]+elements[j])%m)
                diffs.append(np.array((elements[i]-elements[j])%m))
    diffs = np.array(diffs)
    #count occurences of each element
    full_group = element_builder(m,n)
    #make an array whose rows represents elements.
    buckets = np.zeros((m**n,n+1))
    #the first n entries identify the element, the last entry identifies number of occurences
    for i in range(m**n):
        buckets[i,0:n] = full_group[i]
    for i in range(len(diffs)):
        for j in range(len(buckets)):
            if np.array_equal(diffs[i], buckets[j,0:n]):
                buckets[j,n] += 1
    count = 0
```

Figure 12: A code sample from “PDS-list-generator2.py”.



```python
    for bucket in buckets:
        if bucket[n] == 2:
            count += 1
            print(bucket)
    if count == 15:
        print("hadamard DS")
    else:
        print("not a hadamard DS")
        print("count", count)
```

Figure 13: A code sample from “structure-explorer-v2.py”.

References

[1] James A. Davis and Jonathan Jedwab. A unifying construction for difference sets. *J. Comb. Theory, Ser. A*, 80:13–78, 1997.

[2] James A. Davis and Jonathan Jedwab. A survey of hadamard difference sets. *Groups, Difference Sets, and the Monster: Proceedings of a Special Research Quarter at the Ohio State University, Spring 1993*, pages 145–156, 2000.

[3] James A. Davis and Qing Xiang. A family of partial difference sets with denniston parameters in nonelementary abelian 2-groups. *European Journal of Combinatorics*, 21(8):981–988, 2000.

[4] R. H. F. Denniston. Some maximal arcs in finite projective planes. *Journal of Combinatorial Theory, Series A*, 6:317–319, 1969.

[5] Jonathan Jedwab, Shuxing Li, and Samuel Simon. Linking systems of difference sets, 2018.

[6] S.L. Ma. Partial difference sets. *Discrete Mathematics*, 52(1):75–89, 1984.

[7] Robert L McFarland. A family of difference sets in non-cyclic groups. *Journal of Combinatorial Theory, Series A*, 15(1):1–10, 1973.

[8] Koji Momihara and Qing Xiang. Generalized constructions of menon-hadamard difference sets, 2019.

[9] Eric Swartz and Gabrielle Tauscheck. Restrictions on parameters of partial difference sets in nonabelian groups, 2020.

[10] Richard J. Turyn. Character sums and difference sets. *Pacific Journal of Mathematics*, 15(1):319 – 346, 1965.

[11] Zeying Wang. Paley type partial difference sets in abelian groups. *Journal of Combinatorial Designs*, 28(2):149–152, 2020.

[12] Richard M. Wilson and Qing Xiang. Constructions of hadamard difference sets. *Journal of Combinatorial Theory, Series A*, 77(1):148–160, 1997.