2016

Partitioning groups with difference sets

Rebecca Funke
University of Richmond

Partitioning Groups with Difference sets

Rebecca Funke

Honors Thesis*

Department of Mathematics & Computer Science

University of Richmond

*Under the direction of Dr. James A. Davis

The signatures below, by the thesis advisor, the departmental reader, and the honors coordinator for mathematics, certify that this thesis, prepared by Rebecca Funke, has been approved, as to style and content.

(Dr. James Davis, thesis advisor)

(Dr. Della Dumbaugh, departmental reader)

(Dr. Van Nall, honors coordinator)

Abstract

This thesis explores the use of difference sets to partition algebraic groups. Difference sets are a tool belonging to both group theory and combinatorics that provide symmetric properties that can be map into over mathematical fields such as design theory or coding theory. In my work, I will be taking algebraic groups and partitioning them into a subgroup and multiple McFarland difference sets. This partitioning can then be mapped to an association scheme. This bridge between difference sets and association schemes have important contributions to coding theory.

Contents

0 Preliminaries **1**

1 Introduction **1**

1.1 Applications to design theory 3

1.2 Applications to coding theory 3

1.3 Hyperplane Construction 6

1.4 Character Theory 7

1.5 Group Ring Notation 9

1.6 Contraction Mapping 9

1.7 Proof of Hyperplane Construction 10

1.8 Dealing with Nonabelian Groups 10

2 McFarland Difference Sets **14**

2.1 Order 96 Case 14

2.1.1 Picking the Hyperplanes 15

2.1.2 Picking the Coset Representatives 17

2.1.3 Unique Properties 18

2.2 Groups of order larger than 96 21

3 GAP **22**

4 Appendix **24**

5 Conclusion **29**

0 Preliminaries

Throughout this thesis we will discuss and use an algebraic construction referred to as a *difference set*. As stated by Moore and Pollatsek, "difference sets... belong both to group theory and to combinatorics and... use tools from these areas as well as from geometry, number theory, and representation theory" [1]. In my work, I consider a special family of difference sets known as McFarland difference sets. Specifically, I connect the study of difference sets to the study of association schemes which are used in coding theory. By creating this bridge between difference sets and association schemes, I will provide a method for constructing association schemes.

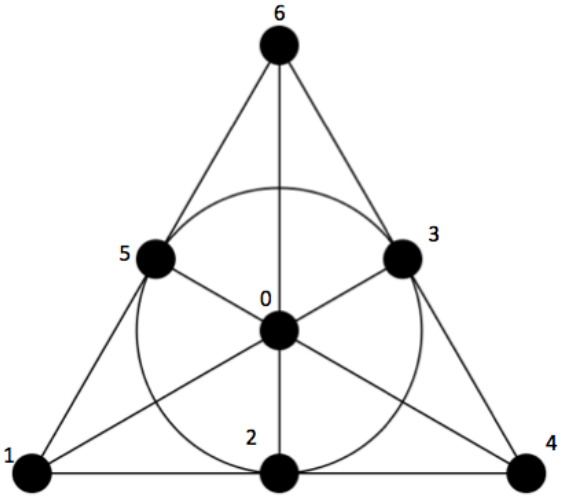
1 Introduction

A (v, k, λ) difference set is a k-element subset of a group G of order v such that the multiset $\{dd^{-1} : d \in D\}$ contains each non-identity element of G, λ times. The following example below has been called the "Design Theorists Coat of Arms".

Example 1. *let* $G = \mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. *Consider the set* $D = \{1, 2, 4\}$. *If you take every difference of the terms in* D *then each nonidentity element of* G *appears exactly once. Specifically,* $1-2 = -1 = 6, 1-4 = -3 = 4, 2-1 = 1, 2-4 = -2 = 5, 4-1 = 3$, *and* $4-2 = 2$. *Thus,* D *is a* $(7, 3, 1)$ *difference set because the group size is 7, the difference set size is 3, and each nonidentity element appears exactly once in the six differences taken.*

The above example is referred to as the "Design Theorists Coat of Arms" because you can use this difference set to create the Fano Plane which is arguably one of the most recognizable images that comes from design theory. Below is the image of the Fano Plane with a description of the image's connection to $(7, 3, 1)$ difference sets.

Figure 1: Fano Plane



Example 2. *Figure 1 is an image of the Fano Plane. Each line in the Fano passes through three different vertices and each vertex has three lines that pass through it. Note that the circle in the middle is considered to be a line. The three vertices on a line form a difference set over* $\mathbb{Z}_7$*. For instance, the bottom line passes through 1, 2, and 4 thus* $\{1, 2, 4\}$ *is a difference set in* $\mathbb{Z}_7$ *which is shown to be true in Example 1. There are seven lines, thus there are at least seven distinct difference sets within the Fano Plane. Note that once you find one difference set, you can find the others by continually adding one to each element in the difference set. Therefore, since* $\{1, 2, 4\}$ *is a difference set, so are* $\{2, 3, 5\}$*,* $\{3, 4, 6\}$*, and so on.*

Let's consider another example of a difference set, specifically a $(16, 6, 2)$ difference set.

Example 3. *Let* $G = \mathbb{Z}_2^4 = \{(0,0,0,0), (0,0,0,1), (0,0,1,0), (0,0,1,1), (0,1,0,0), (0,1,0,1), (0,1,1,0),$
$(0,1,1,1), (1,0,0,0), (1,0,0,1), (1,0,1,0), (1,0,1,1), (1,1,0,0), (1,1,0,1), (1,1,1,0), (1,1,1,1)\}$.

Consider the set $D = \{(0,0,1,1), (0,1,1,1), (1,0,1,1), (1,1,0,0), (1,1,0,1), (1,1,1,0)\}$*. If you take all the differences of the terms in D then each nonidentity element of G appears exactly twice. For instance,* $(0,0,1,1) - (1,1,0,0) = (1,1,1,1)$ *and* $(1,1,0,0) - (0,0,1,1) = (1,1,1,1)$*, but no other difference will result in* $(1,1,1,1)$*. Therefore, D is a* $(16, 6, 2)$ *difference set*

A Boolean function is a function with multiple binary inputs (inputs are 0's or 1's) and one binary output. Consider a Boolean function with four input variables. The elements in G represent the 16 possible inputs for the Boolean function. Suppose that for the input sequences in the set D the Boolean function outputs 1 and for the other input sequences the Boolean function outputs 0. If we passed each input sequence

into the Boolean function starting at (0,0,0,0) and counting up to (1,1,1,1), the output sequence would be 0001000100011110. *This output sequence is famous in coding theory and is referred to as a bent function. They are referred to as "bent" because the output sequences of these functions are as different as possible from all linear and affine functions which are "straight" functions. This makes bent functions hard to approximate, making bent functions an important tool in coding theory. It has been proven that all bent functions can be found using difference sets in a similar approach to the one used above [4].*

1.1 Applications to design theory

As shown in Figure 1, difference sets are used in many branches of mathematics such as design theory. A symmetric (v, k, λ) design is an incidence structure that contains v points and v blocks where each block has size k and any two distinct points appear together in precisely λ common blocks. In design theory, a symmetric (v, k, λ) design with a regular automorphism group G is equivalent to a (v, k, λ) different set in G. Examples of symmetric designs can be found in projective planes.

Definition 1.1. *A projective plane is a nonempty set of points and a nonempty set of lines such that:*

1. *Each pair of points are on a unique line*
2. *Each pair of lines intersects*
3. *Each line contains at least thee points and the plane contains at least two lines*

A projective plane of order n contains $n^2 + n + 1$ points. The smallest example of a projective plane is the projective plane of order 2 also referred to as the Fano plane. As shown in figure one, the Fano plane can be constructed by $(7, 3, 1)$ difference sets.

1.2 Applications to coding theory

Applications of difference sets are also seen in coding theory. The goal of coding theory is to encode a message so that the receiver has a high likelihood of decoding the intended message. This goal can be met by repeating the data in the initial message, but often we look for more sophisticated methods. One good example of a more sophisticated error correcting code is the row span (over $\mathbb{Z}_2$) of the incidence matrix of a symmetric design. An incidence matrix of a symmetric design has a row for each point v in the design and a column for each block e in the design and $(v, e) = 1$ if and only if the v is within the block e, otherwise $(v, e) = 0$. Note that any finite incidence structure corresponds to an incidence matrix.

Moving forward, it will be shown how to use difference sets to construct association schemes which are also used to create error correcting codes in coding theory. Previous research conducted by Davis and Polhill show a connection between Hadamard difference sets and association schemes [2]. A Hadamard difference set is a difference set that has parameters of the form $(v, k, \lambda) = (4n^2, 2n^2, n^2 - n)$ where n is a positive integer. They use an algebraic construction called a Galois ring to partition groups into two disjoint Hadamard difference sets and a subgroup. This partition can then be used to form a three class association scheme which is defined below [2].

Definition 1.2. *An n-class association scheme contains a set X and a partition S of the ordered pairs of X such that:*

1. *there are $n+1$ subsets of $X \times X$ that partition $X \times X$. The subsets are denoted $R_0, .., R_n$.*
2. *$R_0 = \{(x, x) | x \in X\}$.*
3. *$R_i^* = \{(y, x) | (x, y) \in R_i\} = R_j$ for some $1 \leq j \leq n$*
4. *If $(x, y) \in R_k$, then the number of $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ is a constant value p_{ik}^k that is not dependent on a particular choice of x and y but is dependent on i, j, and k.*

The theorem proven by Davis and Polhill connecting Hadamard difference sets and association schemes is listed below.

Theorem 1.3. *Let G be an abelian group containing a $(4N^2, 2N^2 - N, N^2 - N)$-Hadamard difference set D such that $D \cap D^{(-1)} = \emptyset$ and $H = G - D - D^{(-1)}$ is a subgroup of order $2N$. Then the following classes form a nonsymmetric 3-class imprimitive association scheme on G:*

- $R_0 = \{(x, x) | x \in G\}$
- $R_1 = \{(x, y) | x - y \in D\}$
- $R_2 = \{(x, y) | x - y \in D^{(-1)}\}$
- $R_3 = \{(x, y) | x - y \in H^*\}$

Using Theorem 1.3, we construct an association scheme using Hadamard difference sets.

Example 4. *Consider the the set X that contains the elements of $\mathbb{Z}_4 \times \mathbb{Z}_4$. The elements of $\mathbb{Z}_4 \times \mathbb{Z}_4$ can be displayed in a four by four grid as shown below.*

(0,0)	(0,1)	(0,2)	(0,3)
(1,0)	(1,1)	(1,2)	(1,3)
(2,0)	(2,1)	(2,2)	(2,3)
(3,0)	(3,1)	(3,2)	(3,3)

Partition the elements into the table into three sets:

- $D_1 = \{(1,2),(1,3),(2,1),(2,3),(3,1),(3,2)\}$
- $D_2 = \{(0,1),(0,3),(1,0),(1,1),(3,0),(3,3)\}$
- $H = \{(0,0),(0,2),(2,0),(2,2)\}$

I claim that both D_1 and D_2 form a Hadamard difference set. This can be verified by taking the differences of all the elements in each set and showing that each element of the group is created twice. The remaining four elements form the last set H which is isomorphic to $\mathbb{Z}_2^2$. Thus, $\mathbb{Z}_4 \times \mathbb{Z}_4$ is partitioned into two Hadamard difference sets and a subgroup. This partition can be mapped into a three class association scheme. Let

$$R_0 = \{((a,b),(a,b)) | (a,b) \in \mathbb{Z}_4 \times \mathbb{Z}_4\}$$
$$R_1 = \{((a,b),(c,d)) | (c,d) - (a,b) \in D_1\}$$
$$R_2 = \{((a,b),(c,d)) | (c,d) - (a,b) \in D_2\}$$
$$R_3 = \{((a,b),(c,d)) | (c,d) - (a,b) \in H\}.$$

It is evident that the first and second conditions of an association scheme are met. We can also check that D_1, D_2, and H are closed under inversion which implies that the third property of an association scheme holds. The last property, though tedious, can also be checked. Thus, we have formed a three class association scheme.

The last condition of an association scheme is hard to verify thus it is generally harder to identify association schemes than difference sets. The goal of my work is to explore another family of difference sets, McFarland difference sets, in the hopes of proving that groups that contain McFarland difference sets can be partitioned to form an association scheme.

1.3 Hyperplane Construction

When looking at a group it is not always obvious what subset of the elements will form a difference set. Various construction methods are used to find the difference sets within the group. One of the most common construction methods is the hyperplane construction. A hyperplane is a subspace of one dimension less than its surrounding space.

Example 5. *Consider the group* $G = \mathbb{Z}_8 \times \mathbb{Z}_2$ *and the subgroup* $H =< (4,0),(0,1) >= \{(0,0),(4,0),(0,1),(4,1)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. *Because* H *is isomorphic to a 2 dimensional vector space over* $\mathbb{Z}_2$, *the "hyperplanes" of* H *correspond to dimension one subspaces over* $\mathbb{Z}_2$. *Thus, the hyperplanes of* H *are* $< (4,0) >$,$< (0,1) >$, *and* $< (4,1) >$. *The distinct coset representatives of* H *in* G *are* $(0,0),(1,0),(2,0)$, *and* $(3,0)$. *Arbitrarily, three out of the four coset representatives are attached to the hyperplanes, and the resulting set forms a difference set in* G. *By "attaching" the coset representative you are ensuring that we get six distinct elements. For instance, if I attach* $(1,0)$ *to the hyperplane* $< (4,0) >= \{(0,0),(4,0)\}$, *then* $(1,0)+ < (4,0) >= \{(1,0),(5,0)\}$. *I claim that* $D = ((1,0)+ < (4,0) >) \cup ((2,0)+ < (0,1) >) \cup ((3,0)+ < (4,1) >) = \{(1,0),(5,0),(2,0),(2,1),(3,0),(7,1)\}$ *is a difference set of the group* $\mathbb{Z}_8 \times \mathbb{Z}_2$.

Consider a more general case of the above example. Let G be an abelian group of order 2^{2n} and suppose H is an elementary abelian subgroup of order 2^n (note that not all groups G of order 2^{2n} will have such a subgroup). H can be thought of as an n-dimensional subspace over $\mathbb{Z}_2$. Below are the steps to using hyperplanes of H to form a difference set:

1. Find $2^n - 1$ hyperplanes of H. Because H is a n-dimensional subspace over $\mathbb{Z}_2$, each hyperplane is an $(n-1)$-dimensional subspace of H. We know there exist exactly $2^n - 1$ hyperplanes in H because for each one dimensional space $< v >$ where $v \in H$ the perp $< v >^{\perp}$ is an $(n-1)$-dimensional subspace of H. The number of one dimensional spaces is $2^n - 1$ because all 2^n elements can form a one dimensional space besides the identity element. Thus, there are also $2^n - 1$ hyperplanes from H.

2. Choose $g_1, ..., g_{2^n} \in G$ as elements from the distinct cosets of H in G. These are referred to as coset representatives. Note that the number of cosets is equal to $\frac{|G|}{|H|} = \frac{2^{2n}}{2^n} = 2^n$ by Lagrange's Theorem.

3. Using the hyperplanes and coset representatives generate the set D such that $D = \cup_{i=1}^{2^n-1} g_i H_i$. Note that here we are using the multiplicative group operation where as in past examples we have used an additive group operation. Note that you are leaving one of the coset representatives unused.

This hyperplane construction will also work for a vector space over any finite field $GF(q)$.

Example 6. *The subgroup does not always have to be viewed as a vector space over* $\mathbb{Z}_2$. *Consider the group* $G = (GF(4)^+)^2 \times \mathbb{Z}_6$. *Note that GF stands for a Galois field or finite field and* $GF(4) = \{0, 1, \alpha, \alpha + 1\}$ *is the finite field with four elements with* $\alpha^2 = \alpha + 1$. *Thus, the group G has 96 elements. Let* $H \cong (GF(4))^2$ *meaning the subgroup can be viewed as a two dimensional subspace over* $GF(4)$. *The hyperplanes of H have dimension one over* $GF(4)$. *Note that there are 15 nonidentity elements in* $GF(4)^2$ *and each hyperplane will have 3 nonzero elements so there are* $\frac{15}{3} = 5$ *hyperplanes since you can pick any of the three elements of the fifteen to form a hyperplane. The hyperplanes are* $< (0, 1, 0) >, < (1, 0, 0) >, < (1, 1, 0) >$ $, < (1, \alpha, 0) >$, *and* $< (1, \alpha + 1, 0) >$ *where the last generator 0 comes from* $\mathbb{Z}_6$. *Each hyperplane includes four elements (the identity and the generator multiplied by 1,* α, *and* $\alpha + 1$*). For instance,* $< (1, \alpha, 0) >= \{(0, 0, 0), (1, \alpha, 0), (\alpha, \alpha+1, 0), (\alpha+1, 1, 0)\}$. *The unique coset representatives are 0,1,2,3,4, or 5 coming from* $\mathbb{Z}_6$. *Arbitrarily, five out of the six coset representatives will be used to form a difference set. For instance,*
$((0, 0, 0) + < (0, 1, 0) >) \cup ((0, 0, 1) + < (1, 0, 0) >) \cup ((0, 0, 2) + < (1, 1, 0) >) \cup$
$((0, 0, 3) + < (1, \alpha, 0) >) \cup ((0, 0, 4) + < (1, \alpha + 1, 0) >)$ *forms a* $(96, 20, 4)$ *difference set.*

Moving forward, we will show that some groups of order 96 can be partitioned into 4 $(96, 20, 4)$ difference sets and the rest of the elements will form an elementary subgroup. This is always possible for groups that contain difference sets. Not only do we want this partition, we also want the property that $D_1^{(-1)} = D_1, D_2^{(-1)} = D_2, D_3^{(-1)} = D_4$, and $D_4^{(-1)} = D_3$ will allow us to form an association scheme. This second property is harder to find.

1.4 Character Theory

Proving that the hyperplane construction yields a difference set requires some background in character theory. A character χ on the abelian group G is a homomorphism from G to $\mathbb{C}$ under multiplication $\chi : G \rightarrow < e^{\frac{2\pi i}{n}} >$. The principal character χ_0 denotes when each element of G is mapped to 1 in the complex plane. By Euler's Formula we know that $e^{2\pi i} - 1 = 0$, and that the power series of e^x is $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + ...$ Evaluating at $2\pi i$, we get:

$$
\begin{aligned}
e^{2\pi i} &= 1 + 2\pi i + \frac{(2\pi i)^2}{2!} + \frac{(2\pi i)^3}{3!}... \\
e^{2\pi i} &= 1 + 2\pi i - \frac{(2\pi)^2}{2!} - \frac{(2\pi i)^3}{3!}i + \frac{(2\pi)^4}{4!} + ... \\
&= (1 - \frac{(2\pi)^2}{2!} + \frac{(2\pi)^4}{4!} + ...) + i(2\pi - \frac{(2\pi i)^3}{3!} + \frac{(2\pi i)^5}{5!} + ...) \\
&= \cos(2\pi) + i\sin(2\pi) \\
&= 1
\end{aligned}
$$

This result means that you can map the elements of G to complex numbers whose modulus (or length) is one. When finding difference sets, we are interested in calculating the character sum. The character sum of a subset S of a group G for a particular character χ, denoted $\chi(S)$, is the sum of the image of each element in S under χ. More compactly, $\chi(S) = \sum_{s \in S} \chi(s)$. Below is a lemma relating to character sums.

Lemma 1.4. *If χ is a character on an abelian group G then*

$$
\chi(G) = \sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{if } \chi = \chi_0. \\ 0, & \text{otherwise.} \end{cases} \tag{1}
$$

Proof. If $\chi = \chi_0$ then $\chi(G) = |G|$ because you are adding a string of ones.

Suppose $\chi \neq \chi_0$. By definition,there exists g' such that $\chi(g') \neq 1$. This implies that $\chi(g')\chi(G) = \chi(g') \sum_{g \in G} \chi(g) = \sum \chi(g')\chi(g) = \sum \chi(g'g) = \chi(G)$. Note in the last step, multiplying each g by g' is simply reordering the element in G before performing the mapping χ. Because $\chi(g')\chi(G) = \chi(G)$ we know $(\chi(g') - 1)\chi(G) = 0$, so $(\chi(g') - 1) = 0$ or $\chi(G) = 0$. Because $\chi(g') \neq 1$, it is impossible for $(\chi(g') - 1) = 0$, so it must be true that $\chi(G) = 0$. □

Later, when dealing with nonabelian groups we will utilize lemma 1.4 as well as the lemma below.

Lemma 1.5. *Let A be a set of elements from the group G. If the character sum of A is zero then A is some multiple of the group G.*

Moving forward, our goal is to prove that we can use character sums to show that the hyperplane construction will always yield a difference set in an abelian group. Before proving the correctness of the hyperplane construction, we introduce group ring notation and contraction mappings.

1.5 Group Ring Notation

Difference sets are often studied in the context of the group ring which is the set of all formal sums of elements in the group G usually with coefficients from $\mathbb{Z}$. More specifically, the group ring is defined as $\mathbb{Z}[G] = \{\sum_{g\in G} a_g g : a_g \in \mathbb{Z}\}$. If we allow the standard abuse of notation, we have $D = \sum_{d\in D} d$, and we have $D^{(-1)} = \sum_{d\in D} d^{-1}$. D forms a difference set in G if and only if $DD^{(-1)} = n1_G + \lambda G$ where $n = k - \lambda$ and 1_G is the identity of the group.

Consider the group $G = \{x^i : 0 \leq i \leq 6, x^7 = 1\}$. If the difference set includes the elements x,x^2, and x^4 then $D = x + x^2 + x^4$ and $D^{(-1)} = x^6 + x^5 + x^3$ thus $DD^{(-1)} = (x + x^2 + x^4)(x^6 + x^5 + x^3) = 1 + x^6 + x^4 + x + 1 + x^5 + x^3 + x^2 + 1$. Note that each non-identity element of G appears exactly once while the identity appears three times.

Working with the group ring notation allows for a more compact notation that is used for counting. Another tool that assists with these ideas is the contraction mapping.

1.6 Contraction Mapping

Given $K \trianglelefteq G$ define the projection $\phi_K : G \to G/K$ by $\phi(g) = gK$. This endomorphism will extend to an endomorphism from the group ring $\mathbb{Z}[G]$ to $\mathbb{Z}[G/K]$, by defining $\phi_K(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g \phi_K(g)$. Essentially we are contracting each element into the coset it lies in with respect to K and then counting how many elements are in each coset.

Example 7. *Let* $G =< x, y, z, w, u, v | x^2 = y^2 = ... = v^2 = 1,$ *abelian* $>$ *and Let* $K =< x, y, z, w >$. *Let* $A \in \mathbb{Z}[G]$ *such that* $A = 4(1_G) + 13xyuv - 63zuv + 8xu - 4zwu$. *Apply the contraction mapping so that* $\phi_K(A) = 4K + 13uvK - 63uvK + 8uK - 4uK = 4K - 50uvK + 4uK + 0vK$.

When we apply the contraction mapping to a difference set in the group, we get:

$$\begin{aligned}
\phi_K(DD^{(-1)}) &= \phi_K(n(1_G) + \lambda(G)) \\
&= n\phi_K(1_G) + \lambda(\phi_K(G)) \\
&= nK + \lambda(|K|G/K) \\
&= (k - \lambda)K + \lambda|K|G/K
\end{aligned}$$

Thus applying the contraction mapping onto a potential difference set is yet another tool to help verify

that D is in fact a difference set. When applying character theory on G/K, each coset must be mapped to a complex number. Note that because K is the identity coset, $\chi(K) = 1$ because K must map to the identity of the complex plane where χ is a character on the group G/K. Thus $\chi(\phi_K(DD^{(-1)})) = \chi(\phi_K(D))\chi(\phi_K(D^{(-1)})) = k\chi(K) - \lambda\chi(K) = k - \lambda$ as long as χ is a non principal character on G/K.

1.7 Proof of Hyperplane Construction

Using both character theory and the group ring theory, we can now prove a theorem about the validity of the hyperplane construction.

Theorem 1.6. *A subset D of an abelian group G is a (v, k, λ) difference set in G if and only if the character sum over D has modulus $\sqrt{k-\lambda}$ for all non-principal characters χ of G.*

Proof. Suppose that D is a (v, k, λ) difference set in G and let χ be a non-principal character of G. Consider $\chi(DD^{(-1)}) = \chi(D)\chi(D^{(-1)})$. It can be shown that $D^{(-1)} = \overline{\chi(D)}$ where $\overline{\chi(D)} = \{d^{-1}|d \in D\}$ is the complex conjugate of $\chi(D)$. With this, we know that $\chi(DD^{(-1)}) = \chi(D)\overline{\chi(D)} = |\chi(D)|^2$. From the ring notation of a difference set, we know that $DD^{(-1)} = n1_G + \lambda G$. Combining this together we get that $|\chi(D)|^2 = \chi(D)\overline{\chi(D)} = \chi(D)\chi(D)^{(-1)} = \chi(DD^{(-1)}) = \chi((k-\lambda)1_G + \lambda G) = \chi((k-\lambda)1_G) + \chi(\lambda G) = (k-\lambda)\chi(1_G) + 0 = k - \lambda$. Thus $|\chi(D)|^2 = k - \lambda$, therefore $|\chi(D)| = \sqrt{k-\lambda}$.

Suppose that D is a subset of G such that $|\chi(D)| = \sqrt{k-\lambda}$. Through orthogonality relations it can be shown that D will in fact be a (v, k, λ) difference set. □

1.8 Dealing with Nonabelian Groups

So far, all the above examples and proofs have relied on G being abelian. Moving forward, almost all the groups we will work with will be nonabelian. When working with subgroups, we prefer to work only with normal subgroups, so we do not have to worry about left and right cosets. The hyperplane construction still works for nonabelian groups, but you have to be more careful picking coset representives. This is best shown through an example.

Example 8. *Consider the nonabelian group $G = \{< a, b > |a^8 = 1, b^2 = a^2, ba = a^5b\}$. Let $H =< a^4, ab >= \{1, a^4, ab, a^5b\} \cong \mathbb{Z}_2^2$ which is a normal subgroup of G. The hyperplanes of H will be $H_1 =< a^4 >$, $H_2 =< ab >$, and $H_3 =< a^5b >$. The cosets of H in G are $H = \{1, a^4, ab, a^5b\}, aH = \{a, a^5, a^2b, a^6b\}$, $a^2H = \{a^2, a^6, a^3b, a^7b\}$, and $a^3H = \{a^3, a^7, a^4b, b\}$.*

Suppose I choose $1, a, a^2$, *and* a^3 *to be the coset representatives for the four unique cosets of* H *in* G. *According to the hyperplane construction, I attach three out of the four coset representative to the three hyperplanes. Let* $D = aH_1 \cup a^2H_2 \cup a^3H_3$. *I will verify that* D *is a difference set using the group ring notation by showing that* $DD^{(-1)} = n1_G + \lambda G$ *where* $n = k - \lambda$. *We know that* $DD^{(-1)} = (aH_1 + a^2H_2 + a^3H_3)(H_1a^7 + H_2a^6 + H_3a^5) = aH_1H_1a^7 + aH_1H_2a^6 + aH_1H_3a^5 + a^2H_2H_1a^7 + a^2H_2H_2a^6 + a^2H_2H_3a^5 + a^3H_3H_1a^7 + a^3H_3H_2a^6 + a^3H_3H_3a^6 = 6 \times 1_G + 2G$. *Each multiplication needed for the distribution for* $DD^{(-1)}$ *is organized in the table below.*

Table 1: Distribution of terms in $DD^{(-1)}$

term from D	term from $D^{(-1)}$	multiplication of terms	result
aH_1	H_1a^7	$aH_1H_1a^7$	$2(1 + a^4) = 2H_1$
aH_1	H_2a^6	$aH_1H_2a^6$	a^3H
aH_1	H_3a^5	$aH_1H_3a^5$	a^2H
a^2H_2	H_1a^7	$a^2H_2H_1a^7$	aH
a^2H_2	H_2a^6	$a^2H_2H_2a^6$	$2(1 + ab) = 2H_2$
a^2H_2	H_3a^5	$a^2H_2H_3a^5$	a^3H
a^3H_3	H_1a^7	$a^3H_3H_1a^7$	a^2H
a^3H_3	H_2a^6	$a^3H_3H_2a^6$	aH
a^3H_3	H_3a^5	$a^3H_3H_3a^5$	$2(1 + a^5b) = 2H_3$

Table 1 shows that the cosets aH, a^2H *and* a^3H *are all formed exactly twice. The non-identity terms from* H *each appear twice and the the identity appears 6 times. Thus each nonidentity element of* G *appears exactly twice, therefore* D *is a* $(16, 6, 2)$ *difference set.*

However, because G is nonabelian we cannot always arbitrarily choose the coset reps being attached to the hyperplanes. Next is an example where we use the same group but choose coset representatives that do not form a difference set.

Example 9. *Let* $G = \{< a, b > |a^8 = 1, b^2 = a^2, ba = a^5b\}$, *and let* $H =< a^4, ab >= \{1, a^4, ab, a^5b\} \cong \mathbb{Z}_2^2$. *Suppose we arbitrarily decide that instead of using* a, a^2, *and* a^3 *as coset reps, we use* $1, a$, *and* a^2. *Let* $D = 1_GH_1 \cup aH_2 \cup a^2H_3$. *Consider* $DD^{(-1)} = (1_GH_1 + aH_2 + a^2H_3)(H_11_G + H_2a^7 + H_3a^6)$. *Note that* $aH_2H_2a^7 = 2(1+a^5b)$ *and* $a^2H_3H_3a^6 = 2(1+a^5b)$ *meaning the element* a^5b *is produced 4 times. We can also show that there exist no difference of elements in* D *such that the difference is the element* ab. *Therefore,* D

is not a difference set! This example shows that because G is nonabelian, we have to be more careful about our selection of coset reps.

Lets consider why coset reps can be arbitrarily assigned when G is abelian, but cannot be done like this for nonabelian groups. This explanation will rely on the fellowing lemma.

Lemma 1.7. *Let H_i and H_j be distinct hyperplanes of the subgroup $H \cong (GF(q))^n$ in G where q is a prime or a power of a prime. Then:*

$$H_iH_i = q^{n-1}H_i$$
$$H_iH_j = q^{n-2}H$$

Proof. Consider H_iH_i. Let $h \in H_i$. Because H_i is a subspace it is closed under multiplication, so $hH_i = H_i$. There are q^{n-1} elements in the hyperplane, therefore $H_iH_i = q^{n-1}H_i$.

Consider H_iH_j where $i \neq j$. Let χ be non-principal character on H. At most one of the two hyperplanes has the potential of having χ being principal on it. If χ was principal on H_i and H_j then χ would be principal on H because both H_i and H_j are one dimension less than their surrounding space of H, so when the hyperplanes are multiplied it creates H. This would contradict χ being non-principal. Without loss of generality, suppose $\chi(H_j)$ is non-principle. By lemma 1.4, $\chi(H_j) = 0$. Thus $\chi(H_iH_j) = \chi(H_i)\chi(H_j) = \chi(H_i)0 = 0$. By lemma 1.5, because $\chi(H_iH_j) = 0$ H_iH_j is a multiple of H. Specifically, $H_iH_j = q^{n-2}H$. □

This lemma can be used to show why coset reps can be chosen arbitrarily for abelian groups but not for nonabelian groups. If G is abelian then $g_iH_iH_ig_i^{-1} = g_ig_i^{-1}H_iH_i = H_iH_i = q^{n-1}H_i$. So we know that each hyperplane will be generated q^{n-1} times in the product $DD^{(-1)}$, thus we know that each nonidentity element in H is created exactly q^{n-1} times.

But how do we know the rest of the elements of G will be generated exactly q^{n-1} times in $DD^{(-1)}$? Consider G/H which is the quotient group of H in G or simply the group of cosets of H in G. When working with a (v, k, λ) difference set, the group G is partitioned into k cosets which are the elements in G/H. We use coset representatives from $k-1$ of these cosets. It can be shown that the set of coset representatives form a $(k, k-1, k-2)$ difference set. So essentially finding the sum $\sum_{i=1}^{k-1}\sum_{j=1}^{k-1} g_iH_iH_jg_j^{-1}$ when $i \neq j$ in $DD^{(-1)}$ is the same as finding all the differences of the $k-1$ elements in the $(k, k-1, k-2)$ difference set. By lemma 1.7, we know $H_iH_j = H$ so each coset will appear exactly $k-2$ times. This will

hold true for G being abelian or nonabelian.

However, if G is nonabelian then $g_iH_iH_ig_i^{-1}$ does not necessarily generate q^{n-1} copies of the same hyperplane H_i. By lemma 1.7, we know $g_iH_iH_ig_i^{-1}$ will be a copy of some hyperplane but not necessarily the same hyperplane. In Example 8, it so happened that we picked coset reps so that $g_iH_iH_ig_i^{-1} = 2H_i$ for each $i = 1, 2, 3$. This happened because the g_i and g_i^{-1} commuted with the elements in H_i. In the next example we pick some coset representatives that do not commute with the elements of the hyperplane that the coset rep is attached to and show we are still able to construct a difference set.

Example 10. *Let* $G = \{< a, b > |a^8 = 1, b^2 = a^2, ba = a^5b\}$, *and let* $H =< a^4, ab >= \{1, a^4, ab, a^5b\} \cong \mathbb{Z}_2^2$. *The hyperplanes of* H *will be* $H_1 =< a^4 >, H_2 =< ab >$, *and* $H_3 =< a^5b >$. *Let* $D = a^4H_1 \cup a^6bH_2 \cup a^4bH_3$. *Consider* $DD^{(-1)} = (a^4H_1 + a^6bH_2 + a^4bH_3) \times (H_1a^4 + H_2b + H_3a^2b)$. *The distribution table for* $DD^{(-1)}$ *is below.*

Table 2: Distribution of terms in $DD^{(-1)}$

term from D	term from $D^{(-1)}$	multiplication of terms	result
a^4H_1	H_1a^4	$a^4H_1H_1a^4$	$2(1 + a^4) = 2H_1$
a^4H_1	H_2b	$a^4H_1H_2b$	a^3H
a^4H_1	H_3a^2b	$a^4H_1H_3a^2b$	aH
a^6bH_2	H_1a^4	$a^6bH_2H_1a^4$	aH
a^6bH_2	H_2b	$a^6bH_2H_2b$	$2(1 + a^5b) = 2H_3$
a^6bH_2	H_3a^2b	$a^6bH_2H_3a^2b$	a^2H
a^4bH_3	H_1a^4	$a^4bH_3H_1a^4$	a^3H
a^4bH_3	H_2b	$a^4bH_3H_2b$	a^2H
a^4bH_3	H_3a^2b	$a^4bH_3H_3a^2b$	$2(1 + ab) = 2H_2$

In Table 2, we see that H_3 *and* H_2 *are respectively generated twice by* $a^6bH_2H_2b$ *and* $a^4bH_3H_3a^2b$. *Table 2 also shows that* D *creates all the nonidentity elements of* G *exactly twice, therefore* D *is a* $(16, 6, 2)$ *difference set.*

In summary, when working with nonabelian groups, we can still use the hyperplane construction as long as we use care when choosing the coset representatives that are attached to the hyperplanes. Specifically, we must pick coset reps so that each hyperplane H_j is generated exactly once by some $g_iH_iH_ig_i^{-1}$ in the group ring equation $DD^{(-1)}$ where j and i can be the same or different.

2 McFarland Difference Sets

We will now consider McFarland difference sets.

Definition 2.1. *A McFarland difference set is a difference set with the parameters* $(q^{d+1}(\frac{q^{d+1}-1}{q-1}+1), q^d\frac{q^{d+1}-1}{q-1}, q^d\frac{q^d-1}{q-1})$ *where* $q = p^f$ *for* p *a prime and* d *a positive integer.*

We will focus our attention on McFarland difference sets with the parameters $q = 4$ and $d = 1$, thus forming $(96, 20, 4)$ McFarland difference sets. Example 6 provided our first instance of McFarland difference set with these parameters. Another example is given below.

Example 11. *Let* $G =< x, y, z, w, u, v | x^2 = y^2 = z^2 = w^2 = u^2 = v^3 = 1, yx = xyw, zx = xzu, wx = xw, xv = vx, xu = ux, vz = yv, vy = zvz, vu = wv, vw = uvu, zy = yz, yw = wy, uy = yu, zw = wz, zu = uz, wu = uw >$. *More simply,* G *is a semidirect product of* $\mathbb{Z}_6$ *and* $\mathbb{Z}_2^4$. *Let* $H =< y, z, w, u >\cong \mathbb{Z}_2^4$. *Note that* H *is a normal subgroup of* G. *The cosets of* H *in* G *are* H, xv^2H, vH, xH, xvH, *and* v^2H.

We will need five hyperplanes to construct a (96,20,4) difference set. In order to determine the five hyperplanes we should use the mapping θ *from* H *into* $(GF(4))^2$ *where* $\theta(y) = (1, 0), \theta(z) = (\alpha, 0), \theta(u) = (0, 1)$, *and* $\theta(zw) = (0, \alpha)$. *Note that you could have chosen any four generators of* H *at this step not just* $< y, z, u, zw >$. *From this embedding we find that the five hyperplanes of* $(GF(4))^2$, *which are* $< (1, 0) >$, $< (0, 1) >, < (1, 1) >, < (1, \alpha) >$, *and* $< (1, \alpha^2) >$, *are mapped to* $H_1 =< y, z >, H_2 =< u, zw >$, $H_3 =< w, yu >, H_4 =< wu, yzw >$, *and* $H_5 =< yw, zu >$ *respectively. Suppose* $D = xv^2wH_1 \cup vzH_3 \cup xzH_2 \cup xvzH_5 \cup v^2yH_4$. *It can be shown that* $DD^{(-1)} = 161_G + 4G$, *therefore* G *is a (96,20,4) difference set.*

There are 231 groups of order 96. Of these 231 groups, 94 of these groups have a $(96, 20, 4)$ McFarland difference set. AbuGhneim showed that three groups of order 96 could be partitioned into four $(96, 20, 4)$ McFarland difference sets and a subgroup isomorphic to $\mathbb{Z}_2^4$ with the property that $D_1^{(-1)} = D_1, D_2^{(-1)} = D_2, D_3^{(-1)} = D_4$, and $D_4^{(-1)} = D_3$. This last property must hold true in order to fulfill the third property of association schemes [3]. My goal is to show that groups of other orders that fit the McFarland constraints can also be partitioned into association schemes. In order to accomplish this goal, I first must thoroughly study the order 96 case.

2.1 Order 96 Case

There are three groups of order 96 that can be partitioned into four $(96, 20, 4)$ McFarland difference sets and a subgroup isomorphic to $\mathbb{Z}_2^4$ with the property that $D_1^{(-1)} = D_1, D_2^{(-1)} = D_2, D_3^{(-1)} = D_4$, and $D_4^{(-1)} = D_3$.

The three groups will be referred to as groups [96,70], [96,196], and [96,227] because these are the names given to them by a programming language called GAP (more information on GAP can be found in Chapter 4 and in the appendix). For each group we will outline how to partition the group in order to create a structure isomorphic to an association scheme. First, we will start by defining each group and their relations.

Index 70

Group [96,70] was introduced in example 11. It is defined as $G =< x, y, z, w, u, v | x^2 = y^2 = z^2 = w^2 = u^2 = v^3 = 1, yx = xyw, zx = xzu, wx = xw, xv = vx, xu = ux, vz = yv, vy = zvz, vu = wv, vw = uvu, zy = yz, yw = wy, uy = yu, zw = wz, zu = uz, wu = uw >$ or more simply G is a semidirect product of $\mathbb{Z}_6$ and $\mathbb{Z}_2^6$. The center of G is the identity element.

Index 196

Group [96,196] is defined as $< x, y, z, w, u, v | x^2 = y^3 = z^2 = w^2 = u^2 = v^2 = 1, wx = xwz, zx = xz, yx = xy^2, xv = ux, xu = vx, wz = zw, wy = yw, wu = uw, vw = wv, zy = yz, zu = uz, zv = vz, uy = yv, vy = yuv, vu = uv >$ or more simply the group is a semidirect product of D_3 and $\mathbb{Z}_2^4$. The center of G is $< z >$.

Index 227

Group [96,227] is defined as $< x, y, z, w, u, v | x^2 = y^3 = z^2 = w^2 = u^2 = v^2 = 1, yx = xy^2, zx = xw, wx = xz, xv = ux, xu = vx, yw = zy, yzw = wy, yuv = uy, vy = yu, zw = wz, zu = uz, zv = vz, uw = wu, vw = wv, vu = uv >$ or more simply the group is a semidirect product of D_3 and $\mathbb{Z}_2^4$. The center of G is the identity.

2.1.1 Picking the Hyperplanes

The first thing to consider is what hyperplanes we should use to construct a difference set. When working with order 96 groups and a subgroup H isomorphic to $\mathbb{Z}_2^4$ then there will be 35 hyperplanes. We only need five hyperplanes to form a $(96, 20, 4)$ difference set. If we create a mapping from $H \cong \mathbb{Z}_2^4$ to $(GF(4))^2$ then we will have five hyperplanes. For each group there are two sets of hyperplanes that are used to construct difference sets for the partitioning of the groups. Note other hyperplanes can be used to make difference sets for the group, but only these hyperplanes can be used to partition the group into 4 difference sets and a subgroup with the property that $D_1^{(-1)} = D_1, D_2^{(-1)} = D_2, D_3^{(-1)} = D_4$, and $D_4^{(-1)} = D_3$.

Index 70

For group [96,70] there are two sets of hyperplanes we will use to construct difference sets.

1. $< y, z >, < w, yu >, < u, zw >, < yw, zu >$, and $< wu, yzw >$

2. $< y, w >, < z, u >, < yz, wu >, < yu, yzw >$, and $< zw, yzu >$

When looking at a group of four difference sets they always use the same hyperplanes. 192 quadruples use each set of hyperplanes for a total of 384 unique quadruples of difference sets where the above properties hold.

Index 195

In this group there are two different ways of constructing quadruple sets of difference sets. The first case is like above where you use the same hyperplanes for each of the four, and the second uses one set for D_1 and D_2 and a different set for D_3 and D_4. The hyperplanes used are:

1. $< z, w >, < u, v >, < zu, zwv >, < zv, wu >$, and $< wv, zwu >$

2. $< z, w >, < u, v >, < zu, wv >, < zv, zwu >$, and $< wu, zwv >$

3. Use 1. for D_1 and D_2 and then use 2. for D_3 and D_4

4. Use 2. for D_1 and D_2 and then use 1. for D_3 and D_4

Similar to the index 70 case, 192 quadruples use each set of hyperplanes for a total of 768 unique quadruples of difference sets meaning there are 768 ways to partition the group $[96, 195]$ into four difference sets and a subgroup isomorphic to $\mathbb{Z}_2^4$.

Index 227

There are three sets of hyperplanes that can be used.

1. $< z, w >, < u, v >, < zu, wv >, < zv, zwu >$, and $< wu, zwv >$

2. $< z, w >, < u, wv >, < v, zu >, < zv, wu >$, and $< uv, zwu >$

3. $< z, wv >, < w, zu >, < u, v >, < zw, zuv >$, and $< zv, wu >$

Similar to both the index 70 and 195 case, 192 quadruples use each set of hyperplanes for a total of 576 unique quadurples of difference sets meaning there are 576 ways to partition the group $[96, 227]$ into four difference sets and a subgroup isomorphic to $\mathbb{Z}_2^4$.

Now that we know what hyperplanes we can use for the difference sets, we must also consider the coset representatives being used. Because all three of these groups are nonabelian we cannot just randomly attach coset representatives.

2.1.2 Picking the Coset Representatives

Our goal in this section is to find patterns occurring with the coset representatives for the four difference sets in a quadruple. Lets start with an example of four (96,20,4) difference sets from the group [96,70] that partition the group into four difference sets and H.

Example 12. *Let $G = [96, 70]$, and $H =< y, z, w, u >$ where H is isomorphic to $\mathbb{Z}_2^4$. The following D_i are all difference sets, that satisfy $D_1^{(-1)} = D_1, D_2^{(-1)} = D_2, D_3^{(-1)} = D_4$, and $D_4^{(-1)} = D_3$.*

$$D_1 = xv^2w < y, z > +vz < w, yu > +xz < u, zw > +xvz < yw, zu > +v^2y < wu, yzw >$$
$$D_2 = xv^2 < y, z > +v < w, yu > +x < u, zw > +xv < yw, zu > +v^2 < wu, yzw >$$
$$D_3 = xv^2wu < y, z > +vyz < w, yu > +xyz < u, zw > +xvyz < yw, zu > +v^2w < wu, yzw >$$
$$D_4 = xv^2u < y, z > +vy < w, yu > +xy < u, zw > +xvy < yw, zu > +v^2z < wu, yzw >$$
$$H =< y, z, w, u >$$

There are several observations that can be made in this example that remain true for all quadruple sets of difference sets for the three Mcfarland groups of order 96 we are examining:

1. The elements that are not in any of the difference sets will always form H which is isomorphic to $\mathbb{Z}_2^4$. In order for this to be true the coset representative attached to each hyperplane for each difference set cannot be from the coset H because then some elements of H would be present in the difference sets, thus preventing all of the elements of H to be left to form the subgroup. Therefore, the coset representatives must comes from the cosets xv^2H, vH, xH, xvH, and v^2H.

2. Observation 1 leads me to view each coset rep in two parts:

   (a) The **pre-coset rep** attached to a hyperplane is either x, v, xv, v^2, or xv^2 and each difference set will have exactly one of each appear as a post-coset. From observation one, we know the coset reps must come from xv^2H, vH, xH, xvH, and v^2H so each coset rep must have x, v, xv, v^2, or xv^2 in order to be a coset representative for one of these cosets. Looking at Example 12, we can see this property holds.

   (b) the **post-coset rep** is the rest of the coset rep that comes from H. If you look at the same hyperplane in all four difference sets you will notice that the post-coset reps either forms a 2-

dimensional subgroup of H or are three out of four generators for H which are x, y, z and w. For instance in example 12, the first hyperplane listed in the four difference sets is $< y, z >$ and respectively xv^2w, xv^2, xv^2wu, and xv^2u are the coset representatives attached. Note that all the coset representatives are from the coset xv^2H and the post-cosets are $w, 1, wu$, and u respectively. These post-cosets form the 2-d space $< w, u >$.

2.1.3 Unique Properties

We now must consider what makes these three groups unique from the other 228 groups of order 96. The better we can understand what properties are contributing to the success of this partition, the more likely we can take this idea and generalize it further to groups of other orders.

First, all three groups are nonabelian. Suppose an order 96 abelian group G can be partitioned in the way we hope. Let $D = S_1 \cup vS_2 \cup v^2S_3$ where each S_i is a set such that $S_i \subseteq < x, y, z, w, u >$ and v is an order three element. We know $D^{(-1)} = S_1^{-1} \cup S_2^{-1}w^{-1} \cup S_3^{-1}w^{-2}$. If G is abelian then $D^{(-1)} = S_1 \cup w^2S_2 \cup wS_3$. In order for $D = D^{(-1)}$, we know $S_2 = S_3$. This means each of these sets can have at most four elements which is impossible. Therefore, we cannot have the partition we are looking for if G is abelian.

All three groups also have similar relations. First, all the groups have four generators of order two such that the subgroup H generated by those four generators is isomorphic to $\mathbb{Z}_2^4$. These groups also have two other generators (one of order 2 x and one of order 3 v) that do not commute with the other elements. In all the groups, we choose H to be the subgroup that the hyperplanes will live. Thus, the cosets of H in G become H, xH,vH, xvH, v^2H, and xv^2H. As discussed in the previous section, a coset rep will never be chosen from H, so our coset reps must be x, v, xv, v^2, and xv^2 multiplied by some element in H. As shown in Examples 9 and 10, we cannot arbitrarily pick and attach coset reps to hyperplanes because the groups we are working with are nonabelian. We must check if D is a difference set by calculating $DD^{(-1)}$ and checking that $DD^{(-1)} = n1_G + \lambda G$ where $n = k - \lambda$. When working with nonabelian groups, we run into problems when calculating $g_iH_iH_ig_i^{-1}$ because, unlike abelian groups, $g_iH_iH_ig_i^{-1}$ does not necessarily equal H_i. Thus, it is possible that some hyperplanes will not be produced in the product $DD^{(-1)}$ meaning that there exists some element that is not the result of any difference of two elements in D meaning D cannot be a difference set. My goal is to determine for each hyperplane H_i, what hyperplane is produced by $g_iH_iH_ig_i^{-1}$ for each coset where g_i is the coset rep. For instance, I know $< y, z >$ is a hyperplane of $H =< y, w, z, u >$ from the group $G = [96, 70]$. I want to calculate $x < y, z >< y, z > x, xv < y, z >< y, z > xv^2, v < y, z >< y, z > v^2, v^2 < y, z >< y, z > v$, and $xv^2 < y, z >< y, z > xv$ and see what hyperplanes are produced.

Note that I just need to pick one coset rep for each coset because $g_iH_iH_ig_i^{-1} = g_jH_iH_ig_j^{-1}$ where $g_i \neq g_j$, but g_i and g_j are from the same coset. The reason I want to do this calculation is so that I know what hyperplanes must appear together in a difference set. For instance, $x < y, z >< y, z > x =< zu, yw >$. So if I use $< y, z >$ as a hyperplane and I attach a coset rep from xH to $< y, z >$ then I must also use $< zu, yw >$ as a hyperplane, so that $DD^{(-1)} = n1_G + \lambda G$. There are 35 hyperplanes and five coset reps for each hyperplane, so there are a total of 175 combinations of hyperplanes and coset reps. Example 13 shows the 175 combinations of hyperplanes and coset reps for $G = [96, 70]$. Also in Example 13, we will begin to observe that "self contained" sets of hyperplanes.

Definition 2.2. *Let G be a group and H a subgroup of G. Let S be a set of hyperplanes. The set S is called* ***self contained*** *if for each H_i in the set, $gH_iH_ig^{-1}$ is also in the set where g is a coset rep from each coset of H in G.*

Example 13 will show all the self contained sets of hyperplanes for the group $[96, 70]$.

Example 13. *Let G be the group $[96, 70]$, and $H =< y, z, w, u >$ be a subgroup of G such that $H \cong \mathbb{Z}_2^4$. The hyperplanes of H are all the subgroups of H isomorphic to $\mathbb{Z}_2^2$. Thus, there are 35 hyperplanes that can be used to construct a difference set. I label the hyperplanes as follows:*

$H_1 =< y, z >$	$H_2 =< z, u >$	$H_3 =< z, w >$	$H_4 =< z, yu >$	$H_5 =< z, yw >$
$H_6 =< z, wu >$	$H_7 =< z, ywu >$	$H_8 =< y, u >$	$H_9 =< y, w >$	$H_{10} =< y, zu >$
$H_{11} =< y, zw >$	$H_{12} =< y, wu >$	$H_{13} =< y, zwu >$	$H_{14} =< u, w >$	$H_{15} =< u, yz >$
$H_{16} =< u, zw >$	$H_{17} =< u, yw >$	$H_{18} =< u, yzw >$	$H_{19} =< w, yz >$	$H_{20} =< w, zu >$
$H_{21} =< w, yu >$	$H_{22} =< w, yzu >$	$H_{23} =< yz, zu >$	$H_{24} =< yz, zw >$	$H_{25} =< yz, zwu >$
$H_{26} =< yz, zwu >$	$H_{27} =< zu, zw >$	$H_{28} =< zu, yw >$	$H_{29} =< zu, zyw >$	$H_{30} =< zw, yu >$
$H_{31} =< zw, yzu >$	$H_{32} =< yu, yw >$	$H_{33} =< yu, yzw >$	$H_{34} =< yw, zyu >$	$H_{35} =< wu, yzw >$

Using a computer program, I first find all the hyperplanes which are labeled H_1 through H_{35}. The program then takes each hyperplane and calculates $xH_iH_ix^{-1}$, $vH_iH_iv^{-1}$, $xvH_iH_ixv^{-1}$, $v^2H_iH_i(v^2)^{-1}$, and $xv^2H_iH_i(xv^2)^{-1}$. By lemma 1.7, each of these calculations will form one of the 35 hyperplanes. Note that each coset representative comes from a unique coset and that we are not attaching a coset representative from the coset H, because as discussed earlier, we will never attach a coset representative from H to a hyperplane. Table 3, organizes this information by labeling the vertical columns by the hyperplanes, and the rows by the coset rep you are attaching to the hyperplane. For instance, the hyperplane stored in the cell under the

column H_2 and row v represents the hyperplane generated by $vH_2H_2v^2$.

Table 3: Finding $g_iH_iH_ig_i^{-1}$ for each hyperplane

	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8	H_9	H_{10}	H_{11}	H_{12}	H_{13}	...	H_{35}
x	H_{28}	H_2	H_{20}	H_{29}	H_{10}	H_{27}	H_{23}	H_{17}	H_9	H_5	H_{34}	H_{32}	H_{24}	...	H_{35}
v	H_1	H_{25}	H_{12}	H_{11}	H_{13}	H_8	H_{10}	H_{19}	H_{25}	H_{24}	H_{26}	H_{15}	H_{23}	...	H_{16}
xv	H_{28}	H_{25}	H_{32}	H_{34}	H_{24}	H_{17}	H_5	H_{22}	H_{25}	H_{13}	H_{30}	H_{18}	H_7	...	H_{16}
v^2	H_1	H_9	H_{15}	H_{26}	H_{23}	H_{19}	H_{24}	H_6	H_2	H_7	H_4	H_3	H_5	...	H_{21}
xv^2	H_{28}	H_9	H_{18}	H_{30}	H_7	H_{22}	H_{13}	H_{27}	H_2	H_{23}	H_{29}	H_{20}	H_{10}	...	H_{21}

Table 3 holds some interesting properties. First, note if a hyperplane H_i generates H_j then H_j will also generate H_i. From the table, we can find nine "self contained" sets of hyperplanes which are listed below:

- H_1, H_{28}
- H_2, H_{25}, H_9
- $H_3, H_{20}, H_{15}, H_{18}, H_{12}, H_{32}$
- $H_4, H_{29}, H_{26}, H_{30}, H_{11}, H_{34}$
- $H_5, H_7, H_{10}, H_{24}, H_{13}, H_{23}$
- $H_6, H_{27}, H_{19}, H_{22}, H_8, H_{17}$
- H_{14}
- H_{16}, H_{35}, H_{21}
- H_{31}, H_{33}

For the self contained sets of 6 hyperplanes we know we cannot pick any of these hyperplanes to be in a difference set because then $DD^{(-1)}$ cannot have one of each hyperplane.

Therefore, we can only use self contained sets of 1,2 or 3. The two sets of hyperplanes we use for our construction are $H_1, H_{28}, H_{16}, H_{35}, H_{21}$ and $H_2, H_{25}, H_9, H_{31}, H_{33}$. In each case it is a combination of a two element self contained set and a three element self contained set.

If you repeat this algorithm on both [96,195] and [96,227] then you will find that the hyperplanes we use in our construction all contain a three element self contained set. Note that if we were working with an abelian group everything would be one element self contained sets and we could pick 5 one element self contained sets to construct a difference set. If we did this though, we would not be able to have the property that $D_1^{(-1)} = D_1, D_2^{(-1)} = D_2, D_3^{(-1)} = D_4$, and $D_4^{(-1)} = D_3$. So even though you can use any combination of one,two, or three element self contained sets to create a difference set, we hypothesize that we must have a three element self contained set for the property $D_1^{(-1)} = D_1, D_2^{(-1)} = D_2, D_3^{(-1)} = D_4$, and $D_4^{(-1)} = D_3$ to hold.

We next look through all groups of order 96 with a normal subgroup isomorphic to $\mathbb{Z}_2^4$ to see if they have three element self contained sets of hyperplanes. We found that six other order 96 groups have these sets of hyperplanes (specifically Gap groups [96,194], [96,196], [96,197], [96,226], [96,228], and [96,229]); however, in these six groups the hyperplanes in the three element self contained sets overlap in more than just the origin so they cannot be used together to form a difference set. Therefore, only index 70,195, and 227 have self contained sets of three elements that can be used in the hyperplane construction. This leads us to hypothesize that these three element self contained sets are what are allowing for the property $D_1^{(-1)} = D_1, D_2^{(-1)} = D_2, D_3^{(-1)} = D_4$, and $D_4^{(-1)} = D_3$ to hold. Moving forward, we want to generalize this property.

2.2 Groups of order larger than 96

The first thing to consider is if only nonabelian groups are able to be partitioned into some set of McFarland difference sets and a subgroup such that this partition can be mapped to an association scheme. Consider the example below.

Example 14. *Let $G = \mathbb{Z}_2^5 \times \mathbb{Z}_5^3$. Let the hyperplanes come from $\mathbb{Z}_3^5$ meaning there are $\frac{125-1}{5-1} = 31$ hyperplanes defined as H_1 through H_{31}. Let the coset reps come from $\mathbb{Z}_2^5$ and define them as $g_0, ..., g_{31}$ where g_0 is the identity. Define $D_0 = \cup_{i=1}^{31} g_i H_i$. We can show that D_0 is a $(4000, 775, 150)$ reversible McFarland difference set meaning the inverse of D_0 is itself. For each H_i, let $x_i \in \mathbb{Z}_5^3 \backslash H_i$ and define $D_j = \cup_{i=1}^{3} 1 g_i x_i^j H_i$ for $1 \leq j \leq 4$. Note that $\cup_{j=0}^{4} D_j \cup \{(0, x) | x \in \mathbb{Z}_5^3\} = G$. Therefore G can be partitioned and this partitioning can be mapped to an association scheme.*

Example 14 shows an abelian group that can be partitioned in such a way that $D_1 = D_1^{(-1)}, D_2^{(-1)} = D_2, D_3^{(-1)} = D_4$, and $D_4^{(-1)} = D_3$; however, this is believed to be a sporadic example meaning it is the only

example of this kind. This example relies on the number of hyperplanes being one less than a power of two. There are no other known McFarland groups that hold this property.

Therefore, moving forward we focused on nonabelian groups. We also wanted to look for groups that can have groups of hyperplanes that work like the three element self contained sets in order 96. This led us to explore groups of order 640. Because $640 = 2^7 \times 5$, we will be looking for groups of order 640 that have a normal subgroup H that is isomorphic to $\mathbb{Z}_2^6$ and groups that have five element self contained sets that operate similar to three element self contained sets. The hyperplanes of H are all the normal subgroups of H isomorphic to $\mathbb{Z}_2^3$. There will be 1395 hyperplanes of H, but only 9 will be used in a difference set. The algorithm used in Example 13, can also be used for this group to show that there exist groups of order 640 that contain five element self contained sets of hyperplanes. Now that we know there exist groups of order 640 that contain five element self contained sets of hyperplanes, we must consider how to arrange the hyperplanes and coset reps so that we can partition the group into eight $(640, 72, 8)$ difference sets and a subgroup isomorphic to $\mathbb{Z}_2^6$ so that $D_1^{(-1)} = D_1, D_2^{(-1)} = D_2, D_3^{(-1)} = D_3, D_4^{(-1)} = D_4, D_5^{(-1)} = D_6, D_7^{(-1)} = D_8$, and $D_8^{(-1)} = D_7$. We do this by first finding a difference set D in a group with a five element self contained cycle such that $D = D^{(-1)}$. The algorithm used to find such a partition is computationally intensive, thus a computer program must be used in order to complete the process.

3 GAP

As we work with larger groups, it becomes harder to find difference sets by hand. This leads us to automate this process. We do this by generating programs in a computational discrete algebra programming language called GAP, which is short for Groups Algorithm Programming. We use GAP because the GAP library already contains implementations of many algebraic algorithms as well as an extensive data library of algebraic objects, including all the groups of order less than 2000.

Specifically, we will be using GAP to find groups with a difference set D such that $D^{(-1)} = D$. I will outline the logic used to write this code using pseudocode. Specifics for how to use and write code in GAP are provided in the appendix.

Example 15. *In this example, we will provide pseudocode to find a difference set in group* $[96, 70]$ *such that* $D = D^{(-1)}$.

```
G := the group [96,70];
For each normal subgroup in G
```

```
    if the normal subgroup is isomorphic to Z_2^4  then
        H := normal subgroup
        break out of loop

If H has a value then (the next statements execute if G has a normal subgroup isomorphic to Z_2^4)
    find some generators for H call them [x,y,z,w]

    g := an element of order 3 from G
    cosetreps := coset reps from each coset of H in G

    hyperplanes := find all the hyperplanes of H (should be 35 of these)

    for each hyperplane in hyperplanes
        set1 :=  hyperplane;
        set2 := g*hyperplane*g^(-1);
        set3 := g2*hyperplane*g2^(-1);
        sets := [set1,set2,set3];
        if the three sets are disjoint everywhere except the identity element then
            use elements in sets to create embedding from H to GF(4)^2
                if the embedding works then
                    the five hyperplanes are picked and now look at all permutations
                    of hyperplanes and coset reps --> apply the hyperplane construction
                        for each construction check if D=D^(-1)
                            if D=D^(-1) then check if D is a difference set
                                if you make it here you found a difference set so that D=D^(-1)
```

Example 15 gives the general logic that needs to happen in order to iterate through all possible difference sets in G and find a difference set such that $D = D^{(-1)}$. Through our work, we believe that McFarland groups that have difference sets such that $D = D^{(-1)}$ can be partitioned in a way that there will be four difference sets and a subgroup of $\mathbb{Z}_2^4$. This code can be easily modified for working with groups of order 640, the next size group we are working with. Instead, we will look for normal subgroups isomorphic to $\mathbb{Z}_2^6$, g will be an element of order 5, there will be 5 sets being made for each hyperplane, and H will be embedded

into $(GF(8))^2$.

4 Appendix

Creating programs in GAP played a fundamental part in my research. In this appendix, I dive into the specifics of the syntax and functionality of GAP that I used in my work.

In Gap, the most common data structure used is a list. A list stores a collection of objects in a particular order where each item can be located in the list by an index value. The structure for a list is:

```
lists := [item1,item2,...,itemn];
```

Note that the indexing of a list begins at 1 and to add another item to a list you simply write:

```
add(lists,newItem);
```

For-loops are control statements that allow for a designated chunk of code to execute repeatedly. The idea is that the loop will stop when some control statement is met. For instance, you could say for each item in a list do this chunk of code and when the code has been run for each item in the list then the execution of the for loop is complete and the program moves to the next line of code past the for loop. The structure for a for loop is:

```
for i in list do
    # repeated code
od;
```

Note that beginning a line with # indicates a comment.

Another important element of a programming language is conditional statements specifically an if-statement where some conditional is given and the code associated with the if statement only excecutes if the conditional is true. The syntax of the if-statement is:

```
if conditional then
    #conditional code
fi;
```

Data structures such as lists and logical flow operations such as an if-statement or a for-loop are common in all programming languages, but what makes GAP unique is its built in functionality. For instance GAP has numerous methods dealing with groups such as: NormalSubgroups(Group), StructureDescription(G), Size(G), Elements(G), GroupsWithGenerators(lists), etc . More details about these methods and others are in the GAP documentation.

The most useful tool of GAP is the rds library where rds means relative difference sets. This package was created in 2008 by Leonard Soicher. He created this package in order to help complete searches for relative difference sets in non-abelian groups. The package still contains abelian groups, but some of the functionality of the package is reserved for nonabelian groups. A full manual of the functionality of the rds package can be found online, but we mainly used rds because the package contains the definition and structure of all the groups of order 2000 and less. Thus, when we are looking for difference sets in a specific order, we can iterate through all the groups of the order and run some search on each group. Through an exhaustive search we can find all the groups of a specific order that have the property we are looking for. In order to use this package, the program must start with:

```
LoadPackage("rds");
```

For each group of order up to 2000, the rds library has a list of all the groups with that order. To access one group of a specific size you would right SmallGroup(i,j) where i is the order of the group and j is the index of the specific group in the list.

Now that we have some background of the syntax and functionality of GAP, I will give the GAP code used when working with groups of order 96. Much of this code was initially presented as pseudocode in the GAP section.

One way to use the above ideas is to take a group and determine if this group has some specific subgroup. Below is an example of iterating through all the groups of order 96 and printing out the group indices that have a normal subgroup isomorphic to $\mathbb{Z}_2^4$.

Example 16. *Example of finding groups with a specific subgroup.*

```
LoadPackage("rds");              #allows us to use built in groups
ListOfIndices := [];
for i in [1..231] do             #there are 231 groups of order 96
    G := SmallGroup(96,i);       #G stores the ith group of order 96
    NS := NormalSubgroups(G);    #NS stores the normal subgroups of G
    for sub in NS do             # iterate through all elements in NS
        if (Size(sub) = 16) then #entered if sub has 16 elements
            if (StructureDescription(sub) = "C2 x C2 x C2 x C2")  then
                Add(ListsOfIndices,i);
                break;
            fi;
        fi;
    od;
od;
```

When this code is executed, the list called `ListsOfIndices` *will store the Gap indices for all the groups that have a normal subgroup isomorphic to* $\mathbb{Z}_2^4$. `ListsOfIndices` *= [70, 159, 160, 162, 167, 194, 195, 196,*

197, 197, 218, 219, 220, 221, 221, 226, 227, 228, 228, 228, 228, 228, 228, 228, 229, 230, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231, 231]

For each group G that has a normal subgroup H which is isomorphic to $\mathbb{Z}_2^4$, we can also find an embedding for the subgroup H by picking four nonidentity elements in H such that they are all order 2 elements (meaning $e^2 = 1, 2^1 \neq 1$), and that there exist no linear combination of a subset of 2 or 3 of the elements that forms one of the four elements. An example of how this would be coded in GAP is provided below.

Example 17. *In this example, we are taking a subgroup H of the group G where H is isomorphic to $\mathbb{Z}_2^4$ and finding a set of generators for the subgroup H.*

```
x := 0;
y := 0;
z := 0;
w := 0;
Els := Elements(H);
spaceFound := false;
for i in Elements(H) do
    if Order(i)=2 and spaceFound=false then
        for j in Elements(H) do
            if Order(j)=2 and (not j=i) and (spaceFound=false) then
                for k in Elements(H) do
                    if ( (not k=j) and (not k=i) and (not k=i*j)) and (spaceFound=false) then
                        for l in Elements(H) do
                            if (not l=k) and (not l=j) and (not l=i) and
                            (spaceFound=false) and (not l=k*j) and
                            (not l=k*i) and (not l=i*j) and (not l=i*j*k) then
                                if (GroupWithGenerators([i,j,k,l]) = H) then
                                    x := i;
                                    y := j;
                                    z := k;
                                    w := l;
                                fi;
                            fi;
                        od;
                    fi;
                od;
            fi;
        od;
    fi;
od;
```

Once we have a subgroup and a generator for the subgroup, we can now form hyperplanes of the subgroup. Remember when dealing with order 96 McFarland difference sets, we embed the subgroup into $GF(4)^2$. Thus the hyperplanes of H have dimension one over $GF(4)$. Note that there are 15 nonidentity elements in $GF(4)^2$ and each hyperplane will have 3 nonzero elements so there are $\frac{15}{3} = 5$ hyperplanes since you

can pick any of the three elements of the fifteen to form a hyperplane. The hyperplanes of $GF(4)^2$ are $< (0,1) >, < (1,0) >, < (1,1) >, < (1,\alpha) >$, and $< (1,\alpha+1) >$. I am going to use the mapping θ from H into $(GF(4))^2$ where $\theta(y) = (1,0), \theta(z) = (\alpha,0), \theta(u) = (0,1)$, and $\theta(zw) = (0,\alpha)$. Note that you could have chosen any embedding at this step not just $< y, z, u, zw >$. From this embedding we find that the five hyperplanes of $(GF(4))^2$ $< (1,0) >, < (0,1) >, < (1,1) >, < (1,\alpha) >$, and $< (1,\alpha^2) >$ are mapped to $H_1 =< y, z >, H_2 =< u, zw >, H_3 =< w, yu >, H_4 =< wu, yzw >$, and $H_5 =< yw, zu >$ respectively.

In this example, I first manually enter the hyperplanes with the mapping θ applied, but I could automate this process by iterating through the elements of H and finding appropriate mappings from H to $GF(4)$ and then applying the mapping to the 5 hyperplanes $< (0,1) >, < (1,0) >, < (1,1) >, < (1,\alpha) >$, and $< (1,\alpha+1) >$.

Example 18. *This example builds off example 17 where we pick the four generators-x, y, z, and w-for the subgroup H in G. In this example we first manually enter the hyperplanes with a mapping from H to $GF(4)^2$.*

```
H := GroupByGenerators([y,z,w,u]);
e := Elements(H)[1];

cosets := CosetDecomposition(G, H);
H1 := Elements(GroupByGenerators([y,z]));
H2 := Elements(GroupByGenerators([w,y*u]));
H3 := Elements(GroupByGenerators([u,z*w]));
H4 := Elements(GroupByGenerators([y*w,z*u]));
H5 := Elements(GroupByGenerators([w*u,y*z*w]));
Planes := [H1,H2,H3,H4,H5];
cosetReps := [cosets[1][1], cosets[2][1], cosets[3][1], cosets[4][1], cosets[5][1]];
```

After example 18, we have five hyperplanes, and the coset reps. Now we want to apply the hyperplane construction to form (96,20,4) difference sets. Because G is nonabelian, not every combination of cosets and hyperplanes will form a difference set. When programming, it is best to try all the permutations of hyerplanes and coset reps and then just check to see if a difference set is formed. The code to do this is provided in example 19.

Example 19. *This example relies on the above examples in this section. The code finds a difference set in the group* $[96, 70]$.

```
differenceSets := [];          #will store the valid difference sets in G
count := 0;                    #count permutations
diffset := [];                 #stores a potential difference set
ds := [];                      #stores potential ds without the identity element
complete := false;             #true when permutations are complete
maxPerms := 719;               #maximum permutations considered.
```

```
while (complete = false) do
    #apply the hyperplane construction
    #diffset will store 20 elements that could be a ds
    for planeNumber in [1..Length(Planes)] do
        for elementInPlane in Planes[planeNumber] do
            Add(diffset, cosetReps[p[planeNumber]]*elementInPlane);
        od;
    od;

    #iterates through potential ds and removes the identity element
    #we must remove this element in order to use the IsDiffSet method on the set

    for diffElement in [2..Length(diffset)] do
    x := diffset[diffElement]*(diffset[1]^(-1));
    if not( x = Elements(G)[1]) then
        Add(ds,x);
   fi;
   od;

    #check to see that the identity element is removed
    if Length(ds) = 19 then
        #use GAP function that checks if ds is a difference set
        if IsDiffset(ds,G,4) then
            # if ds is a difference then add ds to the total collection of difference sets
            Add(differenceSets, ds);
        fi;
    fi;

    #increase permutation count up by one
    count := count + 1;

# if you have done max permutations then the loop is complete
if count > maxPerms then
    complete := true;
    break;
fi;

    #if not complete, we compute the next permutation of the order of the hyperplanes.
    if complete=false then
        a:= 7;
        b:= a-2;
        while p[b]>p[b+1] do
            b:=b-1;
        od;

        c:= a-1;
        while p[b]>p[c] do
            c:=c-1;
        od;

        temp:= p[b];
```

```
            p[b]:=p[c];
            p[c]:=temp;

            d:= a-1;
            e:= b+1;

            while d>e do
                temp:= p[d];
                p[d]:=p[e];
                p[e]:=temp;
                d:=d-1;
                e:=e+1;
            od;
        fi;
od;
```

One property we are looking for specifically in our difference sets is if $D = D^{(-1)}$. Now that we have a set of the differences sets of G with the specific hyperplanes given, we can check if any of the difference sets have the property that $D = D^{(-1)}$. If a difference set does have this property, we can continue to explore if these hyperplanes allow for a partition of a group that can be viewed as an association scheme. This code can then be modified for groups of other orders that fit the Mcfarland constrains such as order 640 which is the current ordered group we exploring.

5 Conclusion

The goal of our work was to explore if McFarland groups could be partitioned into some number of McFarland difference sets and a subgroup such that this partition can map over to an association scheme. We began our search with the order 96 case. We found three groups of order 96 that can be partitioned into four difference sets and a subgroup isomorphic to $\mathbb{Z}_2^4$ with the additional property that $D_1^{(-1)} = D_1, D_2^{(-1)} = D_2, D_3^{(-1)} = D_4$, and $D_4^{(-1)} = D_3$. This partition with this final property can be mapped into an association scheme. We then tried to find patterns in these three groups of order 96 that could be generalized to other groups. We began to see the importance of three element self contained sets of hyperplanes.

Moving forward, we focused our attention on nonabelian groups. Though there does exist an abelian group that can be partitioned in the way we want, this seems to be a sporadic example. Specifically, we focus our attention on groups of order 640. With these groups, we hope to partition the group into eight $(640, 72, 8)$ difference sets and a subgroup isomorphic to $\mathbb{Z}_2^6$ so that $D_1^{(-1)} = D_1, D_2^{(-1)} = D_2, D_3^{(-1)} = D_3, D_4^{(-1)} = D_4, D_5^{(-1)} = D_6, D_7^{(-1)} = D_8$, and $D_8^{(-1)} = D_7$. Because 640 has a prime factor of 5 rather than 3, we will be looking for five element self contained sets of hyperplanes rather than three element sets.

We have already shown the existence of such groups. We also know of groups of order 640 that have a difference set such that $D = D^{(-1)}$. We are still working on finding the exact partition that corresponds to an association scheme.

Moving forward, we hope to generalize these results beyond just order 96 and order 640 groups and prove why these self contained cycles are so important to our construction.

References

[1] E.H Moore, H.S Pollatsek, *Difference Sets: Connecting Algebra, Combinatorics, and Geometry* , *American Math Society* **67** (2013), 1-26.

[2] J.A. Davis, J. Polhill, "Difference Set Construction of DRADs and Association Schemes", *Journal of Combinatorial Theory Series A* **117** (2010), 598-605.

[3] O.A. AbuGhneim, K.W. Smith "All (96,20,4) difference sets and related structures", *American Math Society* (2013).

[4] J. Dillion,"A Survey of Bent Functions", *NSA Technical Journal* (1972) 191-215