4-30-1993

Symmetric designs, difference sets, and a new way to look at MacFarland difference sets

John Bowen Polhill Jr.

University of Richmond

Symmetric Designs, Difference Sets, and a New Way to Look at MacFarland Difference Sets

John Bowen Polhill,Jr.
Honors thesis[1]
Department of Mathematics
University of Richmond

April 30,1993

[1] Under the direction of Dr. James A. Davis

Abstract

In this paper, the topics of symmetric designs and difference sets are discussed both separately and in relation to each other. Then an approach to MacFarland Difference Sets using the theory behind homomorphisms from groups into the complex numbers is introduced. This method is contrasted with the method of finding this type of difference set used by E.S. Lander in his book Symmetric Designs: An Algebraic Approach.

This paper is part of the requirements for honors in mathematics. The signatures below, by the advisor, a departmental reader, and a representative of the departmental honors committee, demonstrate that John Polhill has met all the requirements needed to receive honors in mathematics.

James A Davis

(advisor)

Gary R. Greenfield

(reader)

(honors committee representative)

1 Symmetric Designs

1.1 Definitions

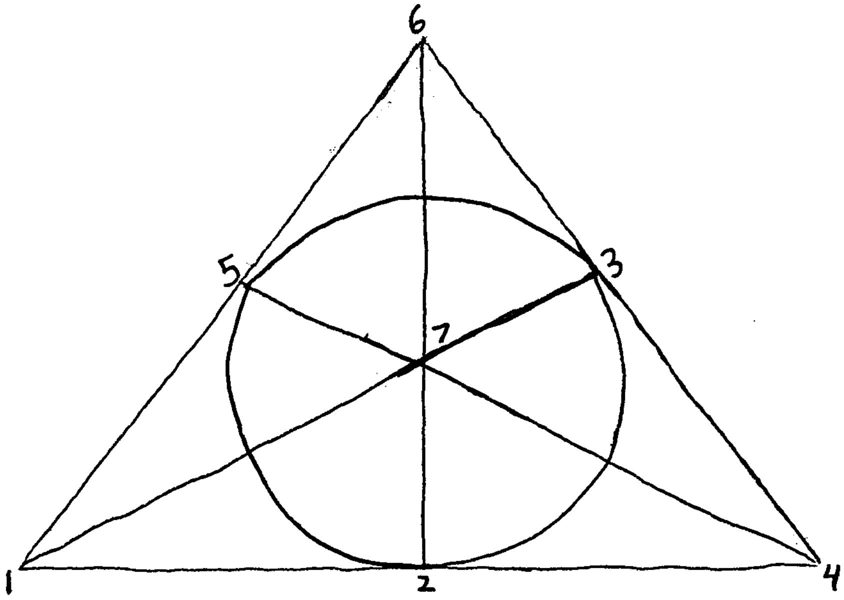
Definition 1.1 *An* incidence structure *consists of a set of points P and a set of blocks B, along with some relation of incidence.*

This definition is extremely general, and one finds that incidence structures appear in all branches of mathematics. A symmetric design is a specific type of incidence structure, and it is to these designs that this chapter is devoted.

Definition 1.2 *A* symmetric (v, k, λ) design *is an incidence structure with the following properties: (i) There are v points. (ii) There are v blocks. (iii) Any block is incident with k points. (iv) Any point is incident with k blocks. (v) Any two blocks are incident with λ points. (vi) Any two points are incident with λ blocks. Note that $k > \lambda$, so that degenerate cases are excluded. The order of a symmetric design is $n = k - \lambda$. The order is an important parameter (see Theorem 4.1).*

The following are simple examples of symmetric designs:

Example 1.1 *The Fano Plane (on the following page) is a symmetric design with parameters (7,3,1). Notice that the 7 points are the numbers 1-7, while the blocks are the six lines together with the circle. There are clearly 3 points on each "line," and each point is on exactly 3 lines. Also any two "lines" have one point in common, while any two points can be found together on one "line."*



Example 1.2 *Let the set of points P be the sixteen squares in the diagram below. To each point is associated a block → the block consists of the six points in the same row or column as that point (so the point is not actually in its associated block). This is a symmetric (16,6,2) design.*

	X X X X X	X X X X X	X X X X X
X X X X X			
X X X X X			
X X X X X			

From symmetric designs one can form an incidence matrix. This matrix is a useful way to describe the design.

Definition 1.3 *The* incidence matrix *of a symmetric (v, k, λ) design is the $v \times v$ matrix whose rows are indexed by the blocks and whose columns are indexed by the points. If a point is incident with a block, then the corresponding entry has a 1. Otherwise, the position has a 0.*

Note that for such an incidence matrix A, $AA^T = (k - \lambda)I + \lambda J$ where I is the identity matrix and J is the square matrix with entries of 1 in every position.

The incidence matrix for the Fano Plane is the matrix shown below.

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Certain relationships between the parameters of a symmetric design always exist. The following lemma reveals them.

Lemma 1.1 *For any symmetric (v, k, λ) design, the following two restrictions always apply:*

$$(i)\ (v - 1)\lambda = k(k - 1),$$

$$(ii)\ k^2 - v\lambda = k - \lambda.$$

Proof: To prove (i) let p' be any point in the design and count the number of pairs (p, B), where p is a point other than p' and B is a block incident with both p and p'. If we sum over the points, there are $(v - 1)$ points other than p' and each is incident with a block to which p' is incident λ times. If we sum over the blocks, p' is on k blocks, while there are $(k - 1)$ points other than p' on each block. The number of pairs must be the same, so $(v-1)\lambda = k(k-1)$. (ii) is just an algebraic rearrangement of the first, but is written in a useful fashion. □

1.2 Automorphisms of a Symmetric Design

Definition 1.4 *An* automorphism *of a symmetric design is an isomorphism of the design onto itself, so that it permutes the blocks to blocks and points to points while preserving incidence.*

The collection of all the automorphisms of a symmetric design forms a group under function composition. This collection is the full automorphism group for the symmetric design. Any subgroup of this full automorphism group is called an automorphism group for the symmetric design. The following defines an important type of automorphism group.

Definition 1.5 *A* regular automorphism group *for a symmetric* (v, k, λ) *design is an automorphism group which for any two points* p, p' *of the design contain a unique group element* g *so that* $gp = p'$. *The size of this automorphism group must hence be of size* v.

For example, for the symmetric $(16, 6, 2)$ design of Example 1.2, $Z_4 \times Z_4$ is a regular automorphism group.

2 Difference Sets

Symmetric designs have a direct relationship to difference sets, the subject of this chapter.

Definition 2.1 *Let G be a group of order v. A (v, k, λ)*-difference set *in G is a subset D of order k such that the list of "differences"*

$$xy^{-1} \quad \textit{with } x, y \in D$$

contains every nonidentity element of G exactly λ times. Note that $k > \lambda$ to exclude trivial difference sets. The order of the difference set is $n = k - \lambda$, analogous to the symmetric design.

Example 2.1 *The set $\{1, 2, 4\}$ in the additive group of integers modulo 7 forms a (7,3,1)-difference set. Notice:*

$$1 - 2 \equiv 6;\ 1 - 4 \equiv 4;\ 2 - 1 \equiv 1;\ 2 - 4 \equiv 5;\ 4 - 1 \equiv 3;\ 4 - 2 \equiv 2.$$

As one might suspect, there does exist a relationship between this example and the symmetric (7,3,1) design (Fano Plane) of chapter 1.

Example 2.2 *The set $\{(0, 1), (0, 2), (0, 3), (1, 0), (2, 0), (3, 0)\}$ is a (16,6,2)-difference set in the group $Z_4 \times Z_4$. We can use this difference set (along with* *its translations, which also will be difference sets in $Z_4 \times Z_4$) to generate the symmetric* $(16, 6, 2)$ *design of example 1.2. Notice that we can also find the following (16,6,2)-difference sets in other groups: in* $G = Z_8 \times Z_2$ *we have* $D = \{(2,0),(6,0),(1,1),(3,1),(5,0),(3,0)\}$; *in* $G = Z_4 \times Z_2 \times Z_2$ *we have* $D = \{(0,1,0),(0,0,1),(0,1,1),(1,0,0),(2,0,0),(3,0,0)\}$; *and in* $G = Z_2^4$ *we have* $D = \{(0,0,0,1),(0,0,1,0),(0,0,1,1),(1,0,0,0),(0,1,0,0),(1,1,0,0)\}$. *(Note that these are not the only difference sets in these groups.) These three difference sets are not equivalent to the design in Example 1.2 because the group of which they are in is not a regular automorphism group for that design. But in general, several groups of the same order may have difference sets with the same parameters.*

The following theorem reveals that symmetric designs with regular automorphism groups and difference sets can be treated as the same notion.

Theorem 2.1 *Let D be a (v, k, λ)-difference set in a group G. Form an incidence structure I_D (the development of D) with the points being the group elements in G and the blocks being the left translates of D,*

$$gD = \{gx | x \in D\} \ \forall g \in G.$$

Then I_D is a symmetric (v, k, λ) design. Also, left multiplication by G on points induces a regular automorphism group of I_D.

Proof: I_D clearly has v points, since the points are the elements of G. Also, I_D has v blocks since the blocks are the translates of the difference set, one each for each different group element in G. In addition, there are k points on a block since the difference set has k elements. To see that every point will be on k blocks, let $h \in G$ and $D = \{d_1, d_2, \ldots, d_k\}$. Then h will be in each left translation of, call it gD, for $g \in G$ whenever $g = hd_i^{-1}$ for $i = 1$ to k. Notice that each $g = hd_i^{-1}$ yields a different translation gD so that there are exactly k blocks which contain any given point.

Now to show that any two distinct blocks contain λ points in common, let gD and hD ($g \neq h$) be any two left translations of the difference set D, so gD and hD are distinct blocks of the incidence structure. Let $x, y \in D$. We want the number of solutions (x, y) to the equation

$$gx = hy.$$

This value is the same as the number of points in common between gD and hD. Multiplication on the right by g^{-1} and on the left by y^{-1} yields the equation

$$xy^{-1} = g^{-1}h.$$

Notice that $g^{-1}h$ is a unique fixed number in G, and not equal to the identity since $g \neq h$. In the list of "differences" xy^{-1} of the difference set D, every non-identity element is contained exactly λ times by definition. So there are λ solutions (x, y) which fit the equation $gx = hy$, so that any two distinct blocks contain exactly λ points in common.

Now to see that any two points are on λ blocks let $g_1, g_2 \in G$. $g_1, g_2 \in gD$ for some $g \in G$ if and only if there exists $d_1, d_2 \in D$ so that $g_1 = gd_1 \; and \; g_2 =$

gd_2. We know by definition that the number $g_2^{-1}g_1$ has exactly λ solutions $d_1d_2^{-1}$. We also know that $g_1 = gd_1$ for a unique $g \in G$. So we have:

$$g_2^{-1}g_1 = d_2^{-1}d_1.$$

Substitution for g_1 yields:

$$g_2^{-1}gd_1 = d_2^{-1}d_1.$$

$$g_2 = gd_2.$$

Since there are λ solutions $d_2^{-1}d_1$, and we get a distinct gD for each solution, we find that any two points are on λ blocks. Therefore, the incidence structure I_D is a symmetric (v,k,λ) design. □

For example, look at the difference set $D = \{1, 2, 4\}$ in Z_7 of Example 2.1. We can form the Fano Plane of Example 1.1 by making the blocks be the left translations of D: $\{g + D \mid g \in Z_7\}$, so there are 7 translations ($\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}$, etc.). Note that these do correspond to the blocks ("lines") of the Fano Plane, while the elements of Z_7 correspond to the points of the design (where $0 \to 7$). A point is on a block if it is in that translation. With this construction, the symmetric $(7, 3, 1)$ design is generated. A similar argument shows that the $(16, 6, 2)$ difference set in $Z_4 \times Z_4$ can be used to generate the symmetric $(16, 6, 2)$ design of example 1.2.

The following Theorem shows that we can also view a symmetric (v, k, λ) design D with a regular automorphism group G as the development of a (v, k, λ)-difference set in G. To form the difference set choose some point x_0.

$\forall\, g \in G$ identify the point gx_0 with the element g, so that x_0 is the identity element. (Notice that any point can be chosen as the x_0, but once the choice is made it serves as the identity element and the identification of the set is completely determined.) With this identification, the elements of G incident with any block of D form a difference set in G. Hence the following result:

Theorem 2.2 *Let I_D be a symmetric (v, k, λ) design with a regular automorphism group G such that $x_0 \in I_D$. For any block B of I_D, the set*

$$D_B = \{g \in G | gx_0 \in B\}$$

is a (v, k, λ)-difference set in B. The development of D_B is isomorphic to D.

Proof: Clearly there are v elements in the group G because there are v points in the design. D_B consists of all $g \in G$ so that $gx_0 = x_i$ for some x_i in the block B. But each block contains k distinct points, so there are k elements $g_i \in G$ so that $g_ix_0 = x_i$ (for $i = 1$ to k). Thus D_B contains k elements.

Now observe a set D_B and a translation D'_B (for distinct blocks B and B'). Since G is the regular automorphism group of the design, we know $D_B = aD'_B$ for some $a \in G$. By definition, B and B' have λ points in common, so there are λ points h_i (for i = 1 to k) such that for $g, h_i \in D_B$ and $h_i \in D'_B$,

$$gx_0 = ah_ix_0 \ or \ a = gh_i^{-1}.$$

Since each group element $a \in G$ ($a \neq$ identity) yields a translation of the block B, and any two blocks have λ points in common, each a can be produced λ times by the list of "differences" xy^{-1} for $x, y \in D = D_B$. Thus the set D_B is a $(v, k, \lambda)-$difference set. □

With this construction, we can treat symmetric designs with regular automorphism groups and difference sets interchangeably.

3 A Difficult Approach to MacFarland Difference Sets

In his book Symmetric Designs: An Algebraic Approach, E.S. Lander describes the following method of finding a specific type of difference set known as a MacFarland Difference Set. Using this method one can produce (for any prime power $q = p^f$) a $(q^{d+1}(q^d + \cdots + q + 2), q^d(q^d + \cdots + q + 1), q^d(q^{d-1} + \cdots + q + 1))-$ difference set in $(Z_p)^{f(d+1)} \times K$, where K is any group with order $(q^d + \cdots + q + 2)$.

3.1 Affine Geometries

In order to produce the theorem necessary to construct the difference set we need some discussion of affine geometries and designs.

Definition 3.1 *An affine geometry, denoted $AG(m, q)$, consists of the following: the points are the elements in the m-dimensional vector space over F_q where q is a power of a prime and the blocks are the translates of the* *hyperplanes (or $(m-1)-$dimensional subspaces).*

The following lemma yields the number of hyperplanes which exist for an m-dimensional vector space over F_q. This result will be used in proving the main theorem in Chapter 5.

Lemma 3.1 *For an m-dimensional vector space V over F_q there are exactly $(q^m-1)/(q-1) = q^{m-1}+q^{m-2}+\cdots+q+1$ hyperplanes ($(m-1)-$dimensional subspaces).*

Proof: We completely determine a subspace by chosing an ordered basis from the elements of V. For our first element, we can choose any of the non-zero elements of V, so there are $q^m - 1$ possibilities. For the second choice we must choose an element not in the 1-dimensional subspace of the first choice, so we have $q^m - q$ choices. For the third element, we can pick from any of the elements not in the 2-dimensional space spanned by the first two elements, so there are $q^m - q^2$ choices. We continue to choose like this until for the last ($(m-1)-$th) element, for which we have $q^m - q^{m-2}$ choices. So the total number of ways we can form a basis for a hyperplane is:

$$(q^m-1)(q^m-q)(q^m-q^2)\cdots(q^m-q^{(m-2)}).$$

But within each hyperplane there are different bases for the space. For the first choice we can choose any non-zero element in the hyperplane, so there are $q^{(m-1)} - 1$ choices. The next choice can be any element of the hyperplane not in the 1-dimensional subspace defined by the first, so there are $q^{(m-1)} - q$ possibilities. We continue to choose until the final element for which there are $q^{(m-1)} - q^{(m-2)}$ options, so that for any hyperplane there are

$$(q^{(m-1)} - 1)(q^{(m-1)} - q)\cdots(q^{(m-1)} - q^{(m-2)})$$

ways to construct the basis. So the total number of hyperplanes in V is:

$$N = [(q^m-1)(q^m-q)(q^m-q^2)\cdots(q^m-q^{(m-2)})]/[(q^{(m-1)}-1)(q^{(m-1)}-q)\cdots(q^{(m-1)}-q^{(m-2)})]$$

Now we can simplify algebraically:

$$N = [(q^m - 1)/(q^{(m-1)} - q^{(m-2)})]\times$$

$$[(q^m-q)(q^m-q^2)\cdots(q^m-q^{(m-2)})]/[(q^{(m-1)}-1)(q^{(m-1)}-q)\cdots(q^{(m-1)}-q^{(m-3)})]$$

$$= [(q^m - 1)/(q^{(m-2)}(q - 1))]\times$$

$$[(q[q^{(m-1)}-1])(q[q^{(m-1)}-q])\cdots(q[q^{(m-1)}-q^{(m-3)}])]/[(q^{(m-1)}-1)(q^{(m-1)}-q)\cdots(q^{(m-1)}-q^{(m-3)})]$$

Now cancellation yields:

$$N = q^{(m-2)}(q^m - 1)/(q^{(m-2)}(q - 1)) = (q^m - 1)/(q - 1)$$

$$= q^{m-1} + q^{m-2} + \cdots + q + 1.$$

□

Affine geometries are an example of an affine design, which is what we will use to produce the MacFarland Difference Sets.

Definition 3.2 *An* affine (v, k, λ) design *is a design for which there exist integers s and μ such that the blocks can be placed into "parallel classes" of size s with the following properties: (i) blocks in the same parallel class are disjoint; (ii) blocks in different parallel classes meet in μ points.*

Note that an affine design is not a symmetric design, as the number of blocks and the number of points in an affine design are not the same. v is the number of points, k is the number of points per block, and λ is the number of blocks which contain any two points. The number of blocks we call b, and the number of blocks which contain a point we call r. For an affine design the restraints on the parameters given by the following lemma must be satisfied.

Lemma 3.2 *For an affine design, (i) $s = v/k$ and (ii) $\mu = v/s^2 = k^2/v$.*

Proof: To show (i), notice that each parallel class of an affine design contains all the points of the design. The blocks of the parallel classes are disjoint, so the number of blocks in each parallel class is s = (number of points)/ (number of points on each block)$=v/k$.

To show (ii), let B be any fixed block in the affine design. Now I count in two ways the number of pairs (x, B') where B' is a block other than B and x is a point on both B and B'. There are k points on B, and each of these points is on r blocks, or $(r - 1)$ blocks other than B. So there are $k(r - 1)$ pairs. Alternatively, there are $(b - s)$ blocks in a distinct parallel class from B, while each of these blocks share μ points with B. So there are $(b - s)\mu$

pairs. We then have

$$\mu = [k(r-1)]/[b-s]$$

But each point is in each parallel class exactly once, and each point is on r blocks, so there are r parallel classes, and each consists of s blocks. So $b = rs$, so substitution for b and $k = v/s$ yields:

$$\mu = [k(r-1)]/[rs-s] = k/s = v/s^2 = k^2/v. \quad \square$$

The following is a simple example of an affine design.

Example 3.1 *$AG(2,3)$ is the affine geometry whose points are the elements of Z_3^2. The blocks B are the 4 1-dimensional subspaces of this group and their cosets. The following shows the design construction with parallel classes P:*

$P_1 : B_{1.1} = \{(0,0),(1,0),(2,0)\};\ B_{1.2} = \{(0,1),(1,1),(2,1)\};\ B_{1.3} = \{(0,2),(1,2),(2,2)\}$

$P_2 : B_{2.1} = \{(0,0),(1,1),(2,2)\};\ B_{2.2} = \{(0,1),(1,2),(2,0)\};\ B_{2.3} = \{(1,0),(2,1),(0,2)\}$

$P_3 : B_{3.1} = \{(0,0),(0,1),(0,2)\};\ B_{3.2} = \{(1,0),(1,1),(1,2)\};\ B_{3.3} = \{(2,0),(2,1),(2,2)\}$

$P_4 : B_{4.1} = \{(0,0),(1,2),(2,1)\};\ B_{4.2} = \{(1,0),(0,1),(2,2)\};\ B_{4.3} = \{(2,0),(0,2),(1,1)\}$

So we have $v = 9$ points, $b = 12$ blocks, $k = 3$ points on a block, $r = 4$ blocks which contain each point, and $\lambda = 1$ block which contains any two points. The parallel classes are of size $s = 3$ (one class for each 1-dimensional subspace), and any two blocks in distinct parallel classes meet in $\mu = 1$ points.

3.2 The Theorem Behind the Construction

The material presented in the previous sections provides the basis for the following theorem, which can be used to form symmetric designs which are analogous to the MacFarland Difference Sets.

Theorem 3.1 *Let there be an affine design with parameters v, b, r, k, and λ. Then there exists a symmetric (v^*, k^*, λ^*) design, where*

$$v^* = (r+1)v, \; k^* = kr, \; and \; \lambda^* = k\lambda.$$

Proof: Let Σ be the affine design. The blocks are placed into parallel classes of size s blocks each. The number of parallel classes is, then, $b/s = b/(v/k) = bk/v = r$. Denote these parallel classes by $\Pi_1, \Pi_2, \ldots, \Pi_r$. Let the points be $p_1, \ldots, p_v$. To each parallel class Π_h we associate a $v \times v$ matrix $M_h = (m_{ij}^h)$ by the rule: $m_{ij}^h = 1$ if p_i and p_j lie on some block in Π_h or $m_{ij}^h = 0$ otherwise. First notice that the matrix points are indexed by the points of the affine design while the rows are indexed by the blocks. Now we make the following three observations about M_h. (i) $M_h = (M_h)^T$, since incidence is reflexive; (ii) $M_h M_h^T = kM_h$ since the blocks are the rows (to see this, and any distinct blocks are disjoint in a parallel class so that the off-diagonal entries are 0, while any row contains k 1's (because there are k points per block) so the dot product of a row with itself is k; (iii) $M_g M_h^T = \mu J \; for \; g \neq h$, since each entry consists of a row representing a block of Π_g dotted with a column representing a block of $\Pi_h \Longrightarrow$ each time the blocks share a point a contribution of 1 to the entry sum is added, and this happens μ times since any two blocks in different parallel classes share μ points (Recall that J is the square matrix with 1 in each position). Now also notice that

$$\sum_{h=1}^{r} M_h = (r - \lambda)I + \lambda J,$$

since each point is on r blocks so the diagonal positions must have an entry of r, while any two distinct points are on λ blocks so that the off-diagonal positions must have an entry of λ. Combining this fact with (ii) above yields:

$$\sum_{h=1}^{r} (M_h M_h^T) = k(r - \lambda)I + k\lambda J.$$

Now we construct the $(r+1)v \times (r+1)v$ matrix L by

$$L = \begin{pmatrix} 0 & M_1 & M_2 & \cdots & M_r \\ M_r & 0 & M_1 & \cdots & M_{r-1} \\ \vdots & & & & \vdots \\ M_1 & M_2 & M_3 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} L_0 \\ L_1 \\ \vdots \\ L_r \end{pmatrix}$$

where each L_i is a $v \times (r+1)v$ matrix. Now using the information above shows that $L_i L_j^T = (r-1)\mu J$ (for $i \neq j$) since any row of L_i represents r blocks of the design, and each row is multiplied with r blocks represented in L_j each of which is in a different parallel class from the block it is dotted with; this is by construction of L as the parallel classes are never matched up in distinct L_i. Now we have that $M_g M_h^T = \mu J \ for \ g \neq h$, and $r+1$ separate block products in the overall dot product, but two of these involve 0's so that the total is $(r-1)\mu J$. Also we have $L_i L_i^T = k(r-\lambda)I + k\lambda J$; this comes directly from the statement $\sum_{h=1}^{r}(M_h M_h^T) = k(r-\lambda)I + k\lambda J$, since $L_i L_i^T$ is exactly this calculation. Finally we can substitute $(r-1)\mu = (r-1)k^2/v = k/\lambda$, so we get

$$LL^T = k(r-\lambda)I + k\lambda J.$$

If we recall the definition of incidence matrices, we find that L is the incidence matrix of the desired symmetric design. □

3.3 Using the Design Theory to Get MacFarland Difference Sets

If we apply the preceding theorem to the affine design $AG(d+1,q)$ we can construct the desired difference sets.

Theorem 3.2 *Let G be an abelian group with order $q^{d+1}(q^d + q^{d-1} + \cdots + q + 2)$, where $q = p^f$ is a power of a prime p. Then if G contains a subgroup isomorphic to ${Z_p}^{f(d+1)}$, then G has a $(q^{d+1}(q^d + \cdots + q + 2), q^d(q^d + \cdots + q + 1), q^d(q^{d-1} + \cdots + q + 1))$-difference set D.*

Proof: The method of construction is a direct application of Theorem 3.1. The rows and columns of the parallel-class matrices are indexed by the group elements in $AG(d+1,q)$; these elements are simply the elements in the vector space $V = F_q^{d+1}$. Since translation by any vector $v \in V$ preserves the parallel classes, the matrices $M_0, \ldots, M_r$ are each left unaltered if we permute the rows and columns according to translation by v (this means that we send the column indexed by the element x to the column indexed by $x+v$, and likewise for rows). Thus the translation group T of V acts as a regular group permuting the rows and columns of the matrices M_i and preserving each of them. Note that if $q = p^f$ for a prime p, then $T \cong (Z_p)^{f(d+1)}$.

Now assume that in forming the matrix L we use the group multiplication table of the group K, with order $r + 1$. The group K has a regular action on the rows and columns of L. For an element $k \in K$, send the row in the position indexed by $g \in K$ to the position indexed by gk and send the column indexed by $h \in K$ to the position indexed by $k^{-1}h$; this preserves the multiplication table since $gh = gkk^{-1}h$. Now the rows and columns of the incidence matrix are indexed by the ordered pairs (v, k) where $v \in V$ and $k \in K$. If we combine the action of T and K, we find that $T \times K$ acts regularly on the rows and columns of the matrix L, thus preserving it. The symmetric design can thus be viewed as a difference set in $T \times K$. Therefore, for a prime power $q = p^f$, we can find a

$$(q^{d+1}(q^d + \cdots + q + 2), q^d(q^d + \cdots + q + 1), q^d(q^{d-1} + \cdots + q + 1))-$$

difference set in $(Z_p)^{f(d+1)} \times K$, where K is a group of order $(q^d + \cdots + q + 2)$.

□

By this method we can find for $q = 3$ and $d = 1$ a $(45, 12, 3)-$difference set in $(Z_3)^2 \times Z_5$ (here $K = Z_5$ and $T = (Z_3)^2$) and for $q = 4$ and $d = 1$ we can identify a $(96, 20, 4)-$difference set in $(Z_2)^5 \times Z_3$ (where $K = Z_2 \times Z_3$ and $T = (Z_2 \times Z_2)^2$).

One can improve this result by a modification so that a difference set can be found in any group G which contains in its center a subgroup isomorphic to $T = (Z_p)^{f(d+1)}$, such that $G/T \cong K$. Using this method we will also find another $(96, 20, 4)-$difference set, now in $(Z_2)^3 \times Z_4 \times Z_3$.

3.4 An Example

Example 3.2 *The following process produces a* $(96, 20, 4)-$*difference set in* $(Z_2)^5 \times Z_3$. *T is the additive subgroup isomorphic to* $F_4^2 \cong (Z_2 \times Z_2)^2$ *(let* $F_4 = \{0, 1, \alpha, \alpha + 1\}$*), so K is the group* $Z_6 \cong Z_2 \times Z_3$. *The matrix L is given by*

$$L = \begin{pmatrix} 0 & M_1 & M_2 & M_3 & M_4 & M_5 \\ M_5 & 0 & M_1 & M_2 & M_3 & M_4 \\ M_4 & M_5 & 0 & M_1 & M_2 & M_3 \\ M_3 & M_4 & M_5 & 0 & M_1 & M_2 \\ M_2 & M_3 & M_4 & M_5 & 0 & M_1 \\ M_1 & M_2 & M_3 & M_4 & M_5 & 0 \end{pmatrix}$$

where the M_i are the matrices defined by the parallel classes of the affine design: each parallel class consists of a 1-dimensional subgroup of F_4^2 *along with the cosets of that subgroup. Note that the five subgroups (hyperplanes) are:*

(1) $(0,0), (0,1), (0,\alpha), (0,\alpha+1)$

(2) $(0,0), (1,0), (\alpha,0), (\alpha+1,0)$

(3) $(0,0), (1,1), (\alpha,\alpha), (\alpha+1,\alpha+1)$

(4) $(0,0), (1,\alpha), (\alpha,\alpha+1), (\alpha+1,1)$

(5) $(0,0), (1,\alpha+1), (\alpha,1), (\alpha+1,\alpha)$

For the first subgroup along with the cosets we have the following parallel class matrix M_1. Note that each other parallel class has such a matrix.

$$M_1 = \begin{array}{c} (0,0) \\ (0,1) \\ (0,\alpha) \\ (0,\alpha+1) \\ (1,0) \\ (1,1) \\ (1,\alpha) \\ (1,\alpha+1) \\ (\alpha,0) \\ (\alpha,1) \\ (\alpha,\alpha) \\ (\alpha,\alpha+1) \\ (\alpha+1,0) \\ (\alpha+1,1) \\ (\alpha+1,\alpha) \\ (\alpha+1,\alpha+1) \end{array} \begin{pmatrix} 1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \end{pmatrix}.$$

Note that the row and column indexes are the same. Now since $F_4 \cong Z_2 \times Z_2$ as additive groups, let $0 = (0,0), 1 = (1,0), \alpha = (0,1), \alpha+1 = (1,1)$ to change the elements into $Z_2 \times Z_2$ Also, $Z_6 \cong Z_2 \times Z_3$, so we map from Z_6 into $Z_2 \times Z_3$ by $0 \rightarrow (0,0), 1 \rightarrow (1,2), 2 \rightarrow (0,1), 3 \rightarrow (1,0), 4 \rightarrow (0,2), 5 \rightarrow (1,1)$. When we finish constructing L (the incidence matrix for the design, a 96×96 matrix), we can then pull the following $(96,20,4)-$difference set in $Z_2^5 \times Z_3$ (from any of the rows will result such a difference set):

$\{(0,0,0,0,1,2),(1,0,1,1,1,2),(0,1,1,0,1,2),(1,1,0,1,1,2),(0,0,0,0,0,1)$

$(1,0,0,1,0,1),(0,1,1,1,0,1),(1,1,1,0,0,1),(0,0,0,0,1,0),(1,0,1,0,1,0)$

$(0,1,0,1,1,0),(1,1,1,1,1,0),(0,0,0,0,0,2),(1,0,0,0,0,2),(0,1,0,0,0,2)$

$(1,1,0,0,0,2),(0,0,0,0,1,1),(0,0,1,0,1,1),(0,0,0,1,1,1),(0,0,1,1,1,1)\}.$

4 Homomorphisms from an Abelian Group to the Complex Numbers

4.1 Defining the Group of Homomorphisms from $G \rightarrow$ C

Lemma 4.1 *For an abelian group G of order ν, there exist ν homomorphisms from G into the complex numbers under multiplication.*

Proof: From the properties of homomorphisms, we know the identity, e, of G must be mapped to 1, the identity of **C** under multiplication. Now let g be a generator of G which is of order n. Then notice that:

$$[\phi(g)]^n = \phi(g^n) = \phi(e) = 1$$

Therefore, $\phi(g)$ must be an nth root of unity. The order of an abelian group is the product of the orders of elements in a generating set, and since for each generator of order m there are m choices for an mth root of unity, then the number of automorphisms from G to **C** is the order of G. □

Example 4.1 *As a simple example, in the group $Z_4 \times Z_2$, (1,0) can be sent to +1, -1, i, or -i while (0,1) can be sent to +1 or -1. Once we determine where to send these two generators of the group, we have determined the ho-*

momorphism. So there are 8 homomorphisms of this group into the complex numbers.

Theorem 4.1 *Let G be an abelian group of order ν. Then the set of homomorphisms $\{\phi : G \to \boldsymbol{C} | \phi$ is a homomorphism $\}$ forms a group under multiplication.*

Proof: $\phi_0(g) = 1 \; \forall g \in G$ is an identity element for the set under multiplication. Associativity is inherited from multiplication in $\boldsymbol{C}$. So if the set contains inverses, then it is a group. Define

$$\phi^{-1}(g) = \phi(g^{-1});$$

this is possible since G is a group and contains all its inverses. Notice that

$$\phi(g)\phi^{-1}(g) = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = 1 = \phi_0(g), \quad \forall\, g \in G.$$

Now to show that ϕ^{-1} is a homomorphism from G to $\boldsymbol{C}$, let $g_1, g_2 \in G$. Then

$$\phi^{-1}(g_1)\phi^{-1}(g_2) = \phi(g_1^{-1})\phi(g_2^{-1}) = \phi(g_1^{-1}g_2^{-1}) = \phi(g_2{}^{-1}g_1{}^{-1}) = \phi^{-1}(g_1g_2)$$

Therefore, if ϕ is a homomorphism from G to $\boldsymbol{C}$, then our ϕ^{-1} is a homomorphism from G to $\boldsymbol{C}$ so that $\phi\phi^{-1} = \phi_0$. So the set is a group. □

We also note that $\phi^{-1} = \overline{\phi}$. This fact is crucial in proving the lemmas and theorems that follow. It is true because for any group G, $|\phi(g)| = 1 \; \forall\, g \in G$. So $\phi\overline{\phi} = \phi_0$.

4.2 Properties of the Homomorphism Group

In this section we will collect a few of the properties of the group of homomorphisms introduced above. In order to prove the lemmas that follow we need the following proposition.

Proposition 4.1 *The sum of the nth roots of unity for $n > 1$ is 0.*

Proof: The nth roots of unity are solutions to the equation $x^n - 1 = 0$. Let α be an nth root of unity, then the nth roots of unity are $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. So the sum of the nth roots of unity is $1+\alpha+\alpha^2+\cdots+\alpha^{n-1} = (1-\alpha^n)/(1-\alpha) = 0$ since $\alpha^n = 1$. □

Lemma 4.2 *Let G be a group of order ν. If ϕ is not the identity homomorphism (equivalent to saying ϕ is nontrivial), then $\sum_{g\in G}\phi(g) = 0$.*

Proof: Let $h \in G$ so that $\phi(h) \neq 1$. Such an h exists since ϕ is nontrivial. We know that h will generate a unique cyclic subgroup in G, call it $\langle h\rangle$. Observe that:

$$\sum_{g\in\langle h\rangle} \phi(g) = \phi(h^1) + \phi(h^2) + \cdots + \phi(h^n),$$

where n is the order of h in G. Now since $\phi(h^n) = \phi(e) = 1$, then $\phi(h)$ must be an nth root of unity. Now $\phi(h)$ may not be a primitive nth root of unity, so let it be a primitive mth root of unity where $m|n$ (note that m $\neq$ 1 since $\phi(h) \neq 1$). So continuing from the equation above we have:

$$\sum_{g\in\langle h\rangle} \phi(g) = ([\phi(h)]^1+[\phi(h)]^2+\cdots+[\phi(h)]^m)+([\phi(h)]^{m+1}+\cdots+[\phi(h)]^{2m})+\cdots$$

$$+([\phi(h)]^{n-m+1} + \cdots + [\phi(h)]^n)$$

Notice that if $m = n$ then we stop after the first parenthesis, or if $n = 2m$ we stop after the second set. Now since $[\phi(h)]^m = 1$, the equation simplifies to:

$$= (n/m)[\phi(h) + \phi^2(h) + \cdots + \phi^m(h)]$$

Now we have a constant times the mth roots of unity. But the sum of the mth roots of unity ($m \neq 1$) is 0 by Proposition 4.1, so we now have:

$$\sum_{g\in\langle h\rangle} \phi(g) = (n/m)(0) = 0.$$

Every $g \in G$ is in some coset of $\langle h\rangle$. Let $a\langle h\rangle$ be one such coset ($a \in G$). We have

$$\sum_{g\in a\langle h\rangle} \phi(g) = \sum_{g\in\langle h\rangle} \phi(ag) = \sum_{g\in\langle h\rangle} \phi(a)\phi(g)$$
$$= \phi(a) \sum_{g\in\langle h\rangle} \phi(g) = \phi(a)(0) = 0$$

Now we can break up G into the cosets of $\langle h\rangle$:

$$\sum_{g\in G} \phi(g) = \sum_{g\in\langle h\rangle} \phi(g) + \sum_{g\in a_1\langle h\rangle} \phi(g) + \cdots + \sum_{g\in a_k\langle h\rangle} \phi(g) = 0 + 0 + \cdots + 0 = 0.$$

Note that by LaGrange's Theorem $k = \nu/n$. □

Lemma 4.3 *For an abelian group G of order ν with identity e and homomorphism group $\Phi = \{\phi : G \to \mathbf{C} | \phi$ is a homomorphism $\}$, $\sum_{\phi\in\Phi} \phi(e) = \nu$ and $\sum_{\phi\in\Phi} \phi(g) = 0$ $\forall g \in G,\ g \neq e$.*

Proof: We know $\phi(e) = 1 \; \forall \; \phi \in \Phi$, so we have $\sum_{\phi\in\Phi} \phi(e) = \sum_{\phi\in\Phi} 1 = \nu$. So let $g \in G$, $g \neq e$. Choose some ϕ_g such that $\phi_g(g) \neq 1$. Such a homomorphism exists because otherwise g would have to be of order 1 in G, and hence the identity, but $g \neq e$. Now let $\langle\phi_g\rangle$ be the cyclic subgroup of Φ generated by ϕ_g. We have, then,

$$\sum_{\phi\in\langle\phi_g\rangle} \phi(g) = \phi_g(g) + \phi_g^2(g) + \cdots + \phi_g^n(g),$$

where n is the order of ϕ_g in Φ. Since $\phi_g^n(g) = \phi_0(g) = 1$, $\phi_g(g)$ must be an nth root of unity. Then we know ϕ_g is a primitive mth root of unity for $m|n$, and that $m \neq 1$ since then $\phi_g = 1$. We have then:

$$\sum_{\phi\in\langle\phi_g\rangle} \phi(g) = ([\phi_g(g)]^1 + [\phi_g(g)]^2 + \cdots + [\phi_g(g)]^m) + ([\phi_g(g)]^{m+1} + \cdots + [\phi_g(g)]^{2m}) + \cdots$$

$$+([\phi_g(g)]^{n-m+1} + \cdots + [\phi_g(g)]^n).$$

Notice that if $n = m$ we stop after the first parenthesis or if $n = 2m$ we stop after the second set. Now since $[\phi_g(g)]^m = 1$, this equation simplifies to:

$$= (n/m)[\phi_g(g) + {\phi_g}^2(g) + \cdots + {\phi_g}^m(g)].$$

So we have a constant times the mth roots of unity. But the sum of the mth roots of unity ($m \neq 1$) is 0 by Proposition 4.1, so we now have:

$$\sum_{\phi\in\langle\phi_g\rangle} \phi(g) = (n/m)(0) = 0.$$

We know every $\phi \in \Phi$ is in a unique coset of $\langle \phi_g \rangle$. Let $a\langle \phi_g \rangle$ be one such coset ($a \in \Phi$). We have:

$$\sum_{\phi \in a\langle \phi_g \rangle} \phi(g) = \sum_{\phi \in \langle \phi_g \rangle} a(g)\phi(g) = a(g) \sum_{\phi \in \langle \phi_g \rangle} \phi(g) = a(g)(0) = 0.$$

Now we break up Φ into the cosets of $\langle \phi_g \rangle$:

$$\sum_{\phi \in \Phi} \phi(g) = \sum_{\phi \in \langle \phi_g \rangle} \phi(g) + \sum_{\phi \in a_1\langle \phi_g \rangle} \phi(g) + \cdots + \sum_{\phi \in a_k\langle \phi_g \rangle} \phi(g) = 0 + 0 + \cdots + 0 = 0.$$

Note that $k = \nu/n$. □

4.3 Extending the Homomorphism Group to the Group Ring *Z[G]*

It is possible to extend a homomorphism $\phi \in \Phi$ from $\phi : G \to C$ to $\phi : Z[G] \to C$. This is very useful in defining difference sets.

Definition 4.1 *Let G be a group. Then define* $\phi(\sum_{g \in G} a_g g) = \sum_{g \in G} a_g \phi(g)$. *Note that* $a_g \in Z$.

With this definition $\phi : Z[G] \to$ C is a homomorphism, since if we have sets $A = \sum_{a \in A} a$ and $B = \sum_{b \in B} b$, it is clear that $\phi(A+B) = \phi(A) + \phi(B)$. I point out that this is abusive notation to write these sets of elements as sums in this manner. With this definition we can prove the following lemma which is instrumental in proving our main theorems.

Lemma 4.4 (Fourier Inversion Formula) *Let G be a group of order* ν *with homomorphism group* Φ *into the complex numbers. If* $A = \sum_{g \in G} a_g g$, *then* $a_h = (1/\nu) \sum_{\phi \in \Phi} \phi(A)\overline{\phi(h)}$.

Proof: First I simplify $\sum_{\phi\in\Phi}\phi(A)\overline{\phi(h)}$.

$$\sum_{\phi\in\Phi}\phi(A)\overline{\phi(h)}=\sum_{\phi\in\Phi}\phi(\sum_{g_i\in G}a_{g_i}g_i)\overline{\phi(h)}=\sum_{\phi\in\Phi}[\sum_{g_i\in G}a_{g_i}\phi(g_i)]\overline{\phi(h)}.$$

Now we can separate h from the sum of other group elements in G:

$$=\sum_{\phi\in\Phi}a_h\phi(h)\overline{\phi(h)}+\sum_{\phi\in\Phi}\sum_{g_i\in G,\ g_i\neq h}a_{g_i}\phi(g_i)\overline{\phi(h)}$$

$$=a_h\sum_{\phi\in\Phi}\phi(h)\overline{\phi(h)}+a_h\sum_{\phi\in\Phi}\sum_{g_i\in G,\ g_i\neq h}\phi(g_ih^{-1})$$

Now in the first addend, since $|\phi(g)|=1$ for every $\phi\in\Phi$ and $g\in G$, we can simplify $\phi(h)\overline{\phi(h)}=1$. In the second addend, we see that the element g_ih^{-1} will be a non-identity element since $g_i\neq h$. So by lemma 4.3, we find that $\sum_{\phi\in\Phi}\phi(g_ih^{-1})=0$. So the equation simplifies to:

$$=a_h\sum_{\phi\in\Phi}1+a_h\sum_{g_i\in G,\ g_i\neq h}0=a_h\nu+0=a_h\nu.$$

So in this string of equalities we have $\sum_{\phi\in\Phi}\phi(A)\overline{\phi(h)}=a_h\nu$. Therefore, $a_h=(1/\nu)\sum_{\phi\in\Phi}\phi(A)\overline{\phi(h)}$. □

4.4 Main Homomorphism Theorem

The above lemma gives us what we need in order to prove the following theorem, which is at the heart of this method to identify difference sets.

Theorem 4.2 *D is a difference set of k elements in G (of order ν) if and only if $|\phi(D)|=\sqrt{n}$ for every nontrivial homomorphism ($\forall\ \phi\in\Phi,\ \phi\neq\phi_0$).*

Proof: First recall that $n = k-\lambda$. For the difference set D, write $D = \sum_{d\in D} d$. For example we can write the (7,3,1) difference set $\{1, 2, 4\}$ as $D = x^1 + x^2 + x^4$. The group $G = Z_7$ can then be written as $G = 1+x^1+x^2+x^3+x^4+x^5+x^6$. Note that 1 = identity element. Now by definition of a difference set, if we take D (with parameters (v, k, λ)) and multiply by $D^{(-1)}$ ($D^{(-1)}$ is not the inverse of D in $Z[G]$, but the sum of inverses of elements in D written as a polynomial), we get each non-identity element λ times and the identity element k times. So we have the following relationship:

$$DD^{(-1)} = (k-\lambda)1 + \lambda G.$$

Notice that 1 =identity and G is the group written as a polynomial as in the Z_7 example above.

($\Longrightarrow$) Let D be a difference set, and let ϕ be a nontrivial homomorphism. We have

$$|\phi(DD^{(-1)})| = |\phi[(k-\lambda)1+\lambda G]| = |\phi[(k-\lambda)1]+\phi(\lambda G)| = |\phi[(k-\lambda)1+\lambda\phi(G)]|$$

But we know that $\phi(G) = \sum_{g\in G} \phi(g) = 0$ for any nontrivial homomorphism ϕ by lemma 4.2. So substitution yields:

$$= |\phi[(k-\lambda)1] + \lambda(0)| = |\phi[(k-\lambda)1]| = |k-\lambda||\phi(1)|$$

But $\phi(1) = 1$, $\forall\ \phi \in \Phi$ so we have:

$$|k-\lambda|(1) = |k-\lambda| = n.$$

So now we have the equality $|\phi(DD^{(-1)})| = n$, so observe:

$$n = |\phi(DD^{(-1)})| = |\phi(D)||\phi(D^{(-1)})| = |\phi(D)||\overline{\phi(D)}| = |\phi(D)|^2.$$

Therefore, $|\phi(D)| = \sqrt{n}$.

($\Longleftarrow$) Let $|\phi(D)| = \sqrt{n} \, \forall \, \phi \neq \phi_0$. If we can show that $DD^{(-1)} = (k-\lambda)1+\lambda G$, then D is a difference set. Using the Fourier Inversion Formula, I need to show that for the set $DD^{(-1)}$, $a_1 = k$ and $a_g = \lambda$, $\forall \, g \in G$ such that $g \neq 1$.

$$a_1 = (1/\nu) \sum_{\phi \in \Phi} \phi(DD^{(-1)})\overline{\phi(1)} = (1/\nu)[\phi_0(DD^{(-1)}) + \sum_{\phi \neq \phi_0} \phi(DD^{(-1)})]$$

There are $k \cdot k$ differences $DD^{(-1)}$, and $\phi_0(g) = 1 \; \forall \; g$, so $\phi_0(DD^{(-1)}) = k^2$. We also know that for all nontrivial homomorphisms ϕ, that $|\phi(D)| = \sqrt{n}$, so $\phi(DD^{(-1)}) = \phi(D)\overline{\phi(D)} = n$. With these substitutions we get:

$$a_1 = (1/\nu)[k^2 + \sum_{\phi \neq \phi_0} n]$$

There are $\nu - 1$ nontrivial homomorphisms, and $n = k - \lambda$, so we get:

$$a_1 = (1/\nu)[k^2 + (k-\lambda)(\nu - 1)] = (1/\nu)[k^2 + k\nu - v\lambda - k + \lambda]$$

Finally, we can use lemma 1.1 to substitute for $v\lambda$:

$$a_1 = (1/\nu)[k^2 + k\nu - k^2 + k - \lambda - k + \lambda] = k.$$

Now we solve for a_g, $g \neq 1$.

$$a_g = (1/\nu) \sum_{\phi \in \Phi} \phi(DD^{(-1)})\overline{\phi}(g) = (1/\nu)[\phi_0(DD^{(-1)})\overline{\phi_0(g)} + \sum_{\phi \neq \phi_0} (k-\lambda)\overline{\phi(g)}]$$

We know $\overline{\phi_0(g)} = 1$ and $\phi_0(DD^{(-1)}) = k^2$ as above, so we have:

$$a_g = (1/\nu)[k^2 + (k - \lambda) \sum_{\phi \neq \phi_0} \overline{\phi(g)}]$$

But $\sum_{\phi \neq \phi_0} \overline{\phi(g)} = \sum_{\phi \in \Phi} \overline{\phi(g)} - \overline{\phi_0(g)}$. Since $g \neq 1$ we can use lemma 4.3 to substitute $\sum_{\phi \in \Phi} \overline{\phi(g)} = 0$, while $\overline{\phi_0(g)} = 1$. So we have:

$$a_g = (1/\nu)[k^2 + (k - \lambda)(-1)] = (1/\nu)[k^2 + \lambda - k]$$

Now we use lemma 1.1 to substitute for k^2 and get:

$$a_g = (1/\nu)[v\lambda + k - \lambda + \lambda - k] = \lambda.$$

So we have that $DD^{(-1)} = (k - \lambda)1 + \lambda G$, so D is a difference set. □

5 The Homomorphism Approach to MacFarland Difference Sets

With the results from the last chapter, we can now tackle the problem presented in chapter 3 in a simpler fashion. The following theorem is the main result.

Theorem 5.1 *Let G be an abelian group with order $q^{d+1}(q^d + q^{d-1} + \cdots + q + 2)$, where q is a prime. Then if G contains in its center a subgroup isomorphic to ${Z_q}^{d+1}$, then G has a $(q^{d+1}(q^d + \cdots + q + 2), q^d(q^d + \cdots + q + 1), q^d(q^{d-1} + \cdots + q + 1))$-difference set D.*

Proof: First notice that $n = k - \lambda = q^{2d}$. Let T be the subgroup isomorphic to $Z_q{}^{d+1}$. Then let $K = G/T$ so that K is of order $(q^d+\cdots+q+2)$, so now list the elements of K: $K = \{k_0, k_1, \ldots, k_r\}$, where $r = q^d + \cdots + q + 1$. Now we know there are $r = (q^{d+1} - 1)/(q-1) = q^d + \cdots + q + 1$ hyperplanes of $Z_q{}^{d+1}$, so let them be $H_1, \ldots, H_r$. Now we form a set $D = k_1H_1 \cup k_2H_2 \cup \cdots \cup k_rH_r$. Now let ϕ be any nontrivial homomorphism from G to $\mathbf{C}$. First assume ϕ is trivial on T, so that it must be nontrivial on K.

$$|\phi(D)| = |\phi(\sum_{i=1}^{r} k_iH_i)| = |\sum_{i=1}^{r} \phi(k_iH_i)| = |\sum_{i=1}^{r} \phi(H_i)\phi(k_i)|$$

Now we know that ϕ is trivial on T, so that it is trivial on each of the hyperplanes H_i. The hyperplanes are just the d-dimensional subspaces of T, so their size is q^d. Thus, $|\phi(H_i)| = |H_i| = q^d$. So we get then:

$$= |q^d \sum_{i=1}^{r} \phi(k_i)| = |q^d \sum_{i=0}^{r} \phi(k_i) - q^d\phi(k_0)|$$

But $\sum_{i=o}^{r} \phi(k_i) = 0$ by lemma 4.2, so that we get

$$= |q^d(0) - q^d\phi(k_0)| = q^d|\phi(k_0)| = q^d(1) = q^d = \sqrt{n}.$$

Now assume that ϕ is nontrivial on T.

$$|\phi(D)| = |\phi(\sum_{i=1}^{r} k_iH_i)| = |\sum_{i=1}^{r}[\phi(H_ik_i)]|$$

Now we have $\phi : T \rightarrow \mathbf{C}$, which is nontrivial. T has order q^{d+1}, while the size of $\phi(T)$ in $\mathbf{C}$ is q by construction. Therefore the kernel of ϕ, call it H_c is a subgroup of T of order $q^{d+1}/q = q^d$ so it is actually one of the hyperplanes.

Since the size of the kernel is q^d and ϕ is nontrivial on T, ϕ must be nontrivial on all hyperplanes other than H_e. So we have:

$$|\sum_{i=1}^{r}[\phi(H_i)\phi(k_i)]| = |\phi(H_e)\phi(k_e) + \sum_{i=1,i\neq e}^{r} [\phi(H_i)\phi(k_i)]|$$

Since ϕ is nontrivial on all other hyperplanes H_i, we know that $\sum_{h\in H_i} \phi(h) = 0$ by Lemma 4.2. So that $\sum_{i=1}^{r}[\phi(H_i)\phi(k_i)] = \sum_{i=1}^{r} \phi(k_i)[\sum_{h\in H_i} \phi(h)] = \sum_{i=1}^{r} \phi(k_i)(0) = 0$. So we have that:

$$= |\phi(H_e)\phi(k_e) + \sum_{i=1,i\neq e}^{r} [\phi(H_i)\phi(k_i)]| = |\phi(H_e)\phi(k_e)|$$

Now since ϕ is trivial on H_e and $|H_e| = q^d$, we have:

$$= q^d|\phi(k_e)| = q^d = \sqrt{n}.$$

So for $D = k_1H_1 \cup k_2H_2 \cup \cdots \cup k_rH_r$, we have $|\phi(D)| = \sqrt{n}$ for any nontrivial homomorphism ϕ. Thus, by Theorem 4.2, D is a difference set in G. □

This theorem applies also for q a power of a prime, but the proof is omitted. We have the following examples.

Example 5.1 *Using this method we can quickly find a $(16, 6, 2)-$difference set in $G = Z_4 \times Z_4$. G contains a subgroup isomorphic to $Z_2 \times Z_2$, namely the subgroup $T = \{(0,0),(0,2),(2,0),(2,2)\}$. The hyperplanes are the 1-dimensional subgroups of T: $\langle(0,2)\rangle$, $\langle(2,0)\rangle$ and $\langle(2,2)\rangle$. The group $K \cong$*

G/T is $(0,0)+T$, $(0,1)+T$, $(1,0)+T$, and $(1,1)+T$. Then we can form the difference set D by $D = k_1H_1 \cup k_2H_2 \cup k_3H_3 = (1,0)+\langle(0,2)\rangle \cup (0,1)+\langle(2,0)\rangle \cup (2,0)+\langle(2,2)\rangle$. Notice that $(2,0)$ is an element of T so that in K, $(2,0) \cong (0,0)$. So our difference set is $D = \{(0,1),(0,2),(0,3),(1,0),(2,0),(3,0)\}$.

Example 5.2 *We also can use this method to find a $(16,6,2)-$difference set in $G = Z_8 \times Z_2$. G contains in its center a subgroup isomorphic to $Z_2 \times Z_2$, namely the subgroup $T = \{(0,0),(4,0),(0,1),(4,1)\}$. The hyperplanes are the 1-dimensional subgroups of T: $\langle(4,0)\rangle$, $\langle(0,1)\rangle$ and $\langle(4,1)\rangle$. The group $K \cong G/T$ is $(0,0)+T$, $(1,0)+T$, $(2,0)+T$, and $(3,0)+T$. Then we can form the difference set D by $D = k_1H_1 \cup k_2H_2 \cup k_3H_3 = (0,0)+\langle(4,0)\rangle \cup (1,0)+\langle(0,1)\rangle \cup (2,0)+\langle(4,1)\rangle$. So our difference set is $D = \{(0,0),(4,0),(1,0),(1,1),(2,0),(6,1)\}$.*

Now this brings us to our main example, the $(96,20,4)-$difference set in $Z_4 \times Z_2^3 \times Z_3$. In section 3 we found a similar difference set in $Z_2^5 \times Z_3$ using the method of affine geometries and matrices. This example was less complicated than the following one. Yet this new process is far simpler to work with. Notice that this example is for a power of a prime (4); so this method does work for powers of primes as well.

Example 5.3 *We are looking for a $(96,20,4)-$difference set in $G = Z_4 \times Z_2^3 \times Z_3$ so that in the construction with Theorem 5.1 $q = 4$ (note that $F_4 \cong Z_2 \times Z_2$) and $d = 1$. G has a subgroup which is isomorphic to $F_4^2 \cong$*

$(Z_2 \times Z_2)^2$, *call it* $T = \langle (2,0,0,0,0),(0,1,0,0,0),(0,0,1,0,0),(0,0,0,1,0)\rangle$. *The five hyperplanes of* $F_4^2 \cong (Z_2 \times Z_2)^2$ *are:*

$$H_1 = \{(0,0,0,0,0),(0,0,1,0,0),(0,0,0,1,0),(0,0,1,1,0)\}$$

$$H_2 = \{(0,0,0,0,0),(2,0,0,0,0),(0,1,0,0,0),(2,1,0,0,0)\}$$

$$H_3 = \{(0,0,0,0,0),(2,0,1,0,0),(0,1,0,1,0),(2,1,1,1,0)\}$$

$$H_4 = \{(0,0,0,0,0),(2,0,0,1,0),(0,1,1,1,0),(2,1,1,0,0)\}$$

$$H_5 = \{(0,0,0,0,0),(2,0,1,1,0),(0,1,1,0,0),(2,1,0,1,0)\}$$

Now we know $K \cong G/T \cong Z_2 \times Z_3$, *so the list of elements in* K *is* $K = \{(0,0,0,0,0),(0,0,0,0,1),(0,0,0,0,2),(1,0,0,0,0),(1,0,0,0,1),(1,0,0,0,2)\}$. *Then we can form the difference set* $D = k_1H_1 \cup k_2H_2 \cup k_3H_3 \cup k_4H_4 \cup k_5H_5 =$

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

This is the difference set we want.

References

[1] Lander, E.S. *Symmetric Designs: An Algebraic Approach.* Cambridge University Press: Cambridge, 1983.

[2] Fraleigh, John B. *A First Course in Abstract Algebra.* Addison-Wesley: Reading, 1989.