5-2-1997

On some new constructions of difference sets

Sarah Agnes Spence

University of Richmond

On some new constructions of difference sets

Sarah Agnes Spence
Honors Thesis under the direction of Dr. James A. Davis
Department of Mathematics and Computer Science
University of Richmond
Richmond, VA 23173

May 2, 1997

Abstract

Difference sets are mathematical structures which arise in algebra and combinatorics, with applications in coding theory. The fundamental question is when and how one can construct difference sets. This largely expository paper looks at standard construction methods and describes recent findings that resulted in new families of difference sets. This paper provides explicit examples of difference sets that arise from the recent constructions. By gaining a thorough understanding of these new techniques, it may be possible to generalize the results to find additional new families of difference sets. The paper also introduces partial and relative difference sets and discusses how the three types of difference sets relate to other combinatorial structures such as block designs and certain strongly regular graphs.

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 Sarah A. Spence has met all the requirements needed to receive honors in mathematics.

James A Davis

(advisor)

Gary R. Greenfield

(reader)

(honors committee representative)

1 Introduction

We introduce difference sets by showing their connections to mathematical designs. We describe known construction techniques and examine recent results that produced new families of difference sets. In Section 2, we introduce incidence structures, balanced incomplete block designs, and symmetric designs. In Section 3, we define difference sets and show how they relate to designs through the development of a difference set. Some tools from character theory are explained in Section 4, and the results presented therein are used for the balance of the paper. We focus on existence and construction methods in Section 5: We explain the group ring equation and McFarland's construction. An equivalence between partial difference sets and certain strongly regular graphs is presented in Section 6. The equivalence is important because it allows new results in one area to be applied to the other areas. We describe Hadamard matrices, designs, and difference sets in Section 7. The recent results of Wilson and Xiang are examined in Section 8. Section 9 shows how Chen built on Wilson and Xiang's results to form a new family of difference sets known as generalized Hadamard difference sets.

2 Designs

Problems in combinatorics often involve arranging objects into a given number of sets, with various constraints governing how the objects are assigned to the sets. Incidence systems are the combinatorial structures that formalize this problem. Design theory is an area of discrete mathematics that is fundamentally concerned with questions relating to such incidence structures. Design theory has applications in Communications, Engineering, Optimization, Statistical Planning, Computer Science, and Signal Processing [1].

We begin this section with a general definition of an incidence structure.

Definition 2.1 *[1] An* incidence structure *is an ordered triple* $(V, \mathbf{B}, I)$ *where* V *and* $\mathbf{B}$ *are two disjoint sets and* I *is a binary relation between* V *and* $\mathbf{B}$*.*

In general, we call the elements of V points and call the elements of $\mathbf{B}$ blocks. The relation I can be interpreted as a set of ordered pairs (p, B) where point p is then said to be incident with block B. Alternatively, say that point p lies on the block B. Therefore, incidence structures are arrays of points (or objects) and blocks, along with an incidence relation that describes which points belong to which blocks.

Our first example of an incidence structure will prove important for the balance of this paper.

Example 2.1 *Let* $V = \{0, 1, 2, 3, 4, 5, 6\}$ *be the set of points and* $\mathbf{B}$=$\{\{0, 1, 3\}$, $\{1, 2, 4\}$, $\{2, 3, 5\}$, $\{3, 4, 6\}$, $\{4, 5, 0\}$, $\{5, 6, 1\}$, $\{6, 0, 2\}\}$ *be the set of seven blocks. The incidence relation* I *is membership in a block.*

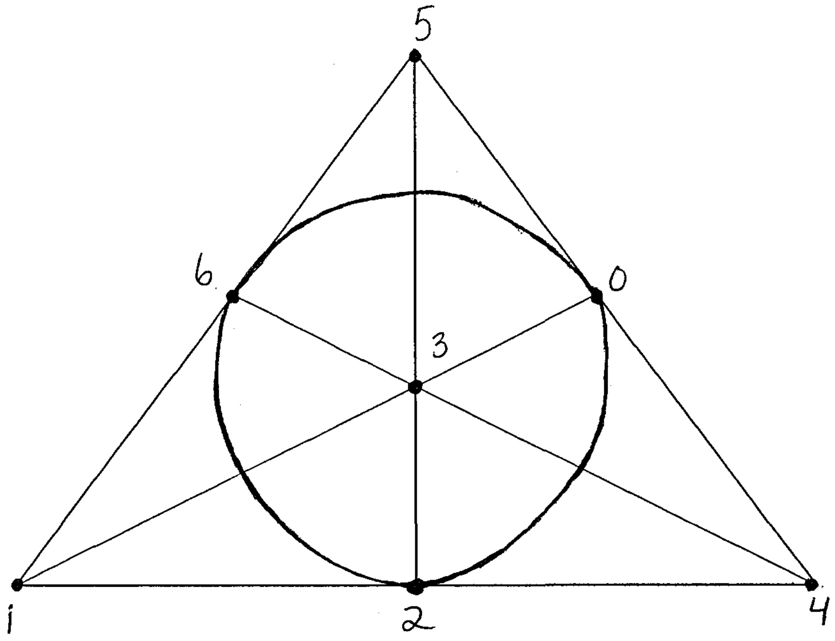
While incidence structures are the building blocks for many combinatorial problems, imposing additional constraints on the points and blocks usually yields more interesting results. One of the fundamental incidence systems is the balanced incomplete block design.

Definition 2.2 *A* balanced incomplete block design (BIBD) *is an arrangement of v distinct points into b blocks such that each block contains exactly k distinct points, each point occurs in exactly r different blocks. Furthermore, every pair of distinct points occurs together in exactly λ blocks.*

Clearly, the incidence structure in Example 2.1 is also a BIBD with parameters $v = 7$, $b = 7$, $k = 3$, $r = 3$, $\lambda = 1$. There are seven points and seven blocks. Each block contains three points. Each point lies in exactly three blocks. Every pair of points is found in exactly one block. For example, the pair of points 0 and 1 is found only in the first block.

This example is commonly known the *Fano plane* drawn in Figure 1. In this interpretation, V consists of the seven points labelled 0 through 6, and **B** consists of the six straight lines together with the circle. This geometric illustration clearly shows that each point is incident with three lines (where the circle is interpreted as a "line"), and each line is incident with three points.

Figure 1.



In a BIBD (b, v, r, k, λ), $bk = vr$ and $r(k-1)=\lambda(v-1)$. BIBD's are called *symmetric* (v, k, λ)-designs when $v = b$ and $k = r$. The Fano plane represents a symmetric design.

3 Difference sets

Difference sets are mathematical structures that are closely related to symmetric designs.

Definition 3.1 *Let G be an additive group of order v. A k-subset $D \subset G$ is a (v, k, λ)-difference set if the set differences $\{d_1 - d_2 = g \mid d_1, d_2 \in D, \text{ and } g \in G\}$ contains each non-identity element $g \in G$ exactly λ times and contains the identity element $g = 0$ exactly k times.*

An analogous definition exists for multiplicative groups. Clearly, $\lambda(v - 1) = k(k-1)$, and to avoid trivial difference sets, we require that $1 < k < v - 1$.

Example 3.1 *The 3-set $\{1, 2, 4\}$ in Z_7 forms a $(7, 3, 1)$-difference set. To see that this indeed forms a difference set, we write out the differences explicitly.* $2 - 1 \equiv 1,\ 4 - 2 \equiv 2,\ 4 - 1 \equiv 3,\ 1 - 4 \equiv 4,\ 2 - 4 \equiv 5,\ 1 - 2 \equiv 6$

The above example is related to the symmetric $(7, 3, 1)$-design represented by the Fano plane of Figure 1. The difference set D is equivalent to one of the blocks in this design. In general, any block of a symmetric (v, k, λ)-design is a (v, k, λ)-difference set in the group consisting of the points of the design.

Example 3.2 *The 15-set*

$$\{(1,1), (2,2), (3,3), (4,4), (5,5),$$

$$(0,1), (0,2), (0,3), (0,4), (0,5),$$

$$(1,0), (2,0), (3,0), (4,0), (5,0)\}$$

is a $(36, 15, 6)$-difference set in $Z_6 \times Z_6$.

Example 3.3 *Let G be the group of order 21 defined by $a^3 \equiv b^7 \equiv 1$, and $a^{-1}ba \equiv b^4$. Then the set $\{a, a^2, b, b^2, b^4\}$ is a $(21, 5, 1)$-difference set.*

Example 3.3 above shows that G need not be abelian, however this paper will focus on difference sets in abelian groups.

3.1 The Development of D

The concept of the development of a difference set is fundamental for understanding the connection between difference sets and symmetric designs.

Definition 3.2 *Let G be a group of order v. For any subset $S \subset G$, and for any $g \in G$, we denote the* translate, *or* shift, *of S by g as $S+g = \{x+g | x \in S\}$.*

In other words, the translate of a subset S is obtained by adding a particular element of the group G to each element in S.

Definition 3.3 *[1] Let G be any finite group and D be a non-empty subset of G. Then, the incidence structure $devD = (G, \mathbf{B}, \in)$ with $\mathbf{B} = \{D+x : x \in G\}$ and $\in$ the set membership relation is called the* development of D.

Obviously, $devD = dev(D+a)$ for any $a \in G$. The development of D has points that are elements of a group G, blocks that are the translates of D, and the incidence relation is membership of a group element in a translate.

Example 3.4 *Let $G = Z_7$ and $D = \{1, 2, 4\}$. Choose $g = 1$, and look at the translates of D. We list them beginning with D:*

$$\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 0\}, \{5, 6, 1\}, \{6, 0, 2\}, \{0, 1, 3\}.$$

This list is equal to the dev$D$.

Notice that the $dev(D)$ in Example 3.4 is equivalent to the design in Example 2.1 which is represented by the Fano plane of Figure 1. We have seen that the line in the Fano plane containing points $\{1, 2, 4\}$ forms a difference set. Now, we see that the other lines are the translates of this difference set, and it is easy to verify that each is a difference set. In fact, a subset D of a group G is a difference set if and only if every translate of D is a difference set. We can now view this symmetric (v, k, λ)-design as the development of $D = \{1, 2, 4\}$ and it is clear that difference sets are the building blocks of symmetric designs. In general, if the development of D forms a symmetric (v, k, λ)-design, then D is a (v, k, λ)-difference set.

We note that using difference sets to represent symmetric designs is often preferable due to the simplicity of required notation. Instead of listing each block in a symmetric design, we need only give the group G and one block. The reader can then take translates of the block to form the design.

4 Character Theory

Character theory is a branch of mathematics that has applications in finite geometry, and its tools are particularly useful when working with difference sets.

Definition 4.1 *A* character χ *is a homomorphism from an additive abelian group G of order m to the cyclotomic field $Q(\psi)$, where ψ is an m-th root of unity. The principal character χ_0 is the homomorphism that maps all elements to the identity.*

Key results from character theory that are used when working with difference sets are stated below as theorems.

For any set A, let $\chi(A) = \sum_{a \in A} \chi(a)$.

Theorem 4.1 *Let A be some set in a group G. Then $\chi(A) = 0$ for all nonprincipal characters if and only if $A = G$.*

Let $\overline{\chi(D)} = \sum_{d \in D} \overline{\chi(d)}$, where $\overline{\chi(d)}$ represents the complex conjugate of $\chi(d)$.

Theorem 4.2 *For all nonprincipal characters χ, $|\chi(D)| = \sqrt{k - \lambda}$ if and only if D is a (v, k, λ)-difference set.*

Since χ is a homomorphism, $\chi(-g) = \overline{\chi(g)}$, and thus it follows from the above theorem that

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

when D is a difference set. For large examples, computing characters is much quicker than other methods used to verify difference sets.

Example 4.1 *The set $D =< x^2 > \cup x < y^2 > \cup y < x^2y^2 >$ is a $(16, 6, 2)$-difference set in $Z_4 \times Z_4 = \{x, y| \ x^4 = y^4 = xyx^{-1}y^{-1} = 1\}$.*

We must show that $|\chi(DD^{-1})| = k - \lambda$. If suffices to compute $\chi(\{1, x^2, x, xy^2, y \ , \ x^2y^3\})$. Since χ is a homomorphism, $(\chi(x))^4 = \chi(x^4) = 1$. So, x and y must each get mapped to 1, -1, i, or $-i$. In other words, all χ take $x \to i^j$ and $y \to i^k$. We consider the following four cases.

1. *j odd, k odd*

2. *j even, k odd*

3. *j odd, k even*

4. *j even, k even*

We work through the first case. Suppose $\chi(x) = i^{2n+1}$ and $\chi(y) = i^{2m+1}$. Consider the character sum over the first subgroup:

$$\begin{aligned}\chi(< x^2 >) &= \chi(1) + \chi(x^2) \\ &= 1 + (i^{2n+1})^2 \\ &= 1 + i^{4n+2} \\ &= 1 - 1 \\ &= 0.\end{aligned}$$

Consider the character sum on the second coset:

$$\begin{aligned}
\chi(x < y^2 >) &= \chi(x) + \chi(xy^2) \\
&= i^{2n+1} + i^{2n+1}(i^{2m+1})^2 \\
&= i^{2n+1}(1 + i^{4m+2}) \\
&= i^{2n+1}(1 - 1) \\
&= 0.
\end{aligned}$$

Finally, the character sum on the third coset yields:

$$\begin{aligned}
\chi(y < x^2y^2 >) &= \chi(y) + \chi(x^2y^3) \\
&= i^{2m+1} + (i^{2n+1})^2(i^{2m+1})^2(i^{2m+1}) \\
&= i^{2m+1}(1 + (-1)(-1)) \\
&= 2i^{2m+1} \\
&= \pm 2i.
\end{aligned}$$

In total, we see that all characters in Case 1 will act on the set $D =< x^2 > \cup x < y^2 > \cup y < x^2y^2 >$ *to give character sum with absolute value 2.*

The other three cases are similar, but note that in Case 4 if x *and* y *both get mapped to 1, then this is the principal character, and the character sum is* $|D|$.

This example show that when considering a large set D, we can check many characters at once by using cases. This method proves preferable for sets D with large order.

5 Constructing Difference Sets

Until this point, the examples of difference sets have been fairly simple, because with groups of such small order, brute force methods may produce difference sets. However, when looking at groups of large order, it is necessary to have organized methods for constructing difference sets. Recall the fundamental question: When and how can we construct a difference set? Methods exist for checking if a difference set can exist within a group and for extracting the appropriate subset from the group. We now examine some established methods, and we later describe recent results that uncover new families of difference sets.

5.1 The group ring equation

The existence of a difference set is equivalent to the existence of a solution to a certain algebraic equation in a group ring. Throughout this section, we use the notation of [5] which is appropriate for abelian groups and highlights the analogy with polynomials.

Let R be a commutative ring with unity and G be a finite abelian group, written additively. The group ring $R[G]$ consists of all formal sums

$$A = \sum_{g \in G} (a_g x^g),$$

where $a_g \in R$ for each $g \in G$. Note that x is simply a place holder. From the identification of $g \in G$ with $a_g \in R$, it follows that the elements of the group ring are in one-to-one correspondence with mappings $G \to R$.

Addition and scalar multiplication are defined in the natural way [5].

$$\sum_{g\in G}(a_g x^g) + \sum_{g\in G}(b_g x^g) = \sum_{g\in G}((a_g + b_g)x^g),$$

$$c\sum_{g\in G}(a_g x^g) = \sum_{g\in G}(ca_g)x^g).$$

Multiplication in the group ring $R[G]$ is defined by [5]

$$\sum_{g\in G}(a_g x^g)\sum_{g\in G}(b_g x^g) = \sum_{g\in G}(\sum_{h+h'=g}((a_h b_{h'})x^g).$$

Example 5.1 *Let G be the additive group Z_v. The elements of the group ring $R[Z_v]$ are the formal sums $\sum_{i=0}^{v-1}(r_i x^i)$ where exponents are modulo v. The group ring is therefore isomorphic to the factor ring $R[x]/(x^v - 1)$ of the polynomial ring $R[x]$.*

When using group rings as a tool for difference sets, we are primarily interested in group rings over the integers $Z[G]$. For a subset $A \subset G$, we define an element $A(x)$ of $Z[G]$ by

$$A(x) = \sum_{g\in A}(x^g).$$

Clearly, $G(x) = \sum_{g\in G}(x^g)$. Alternatively, we write $A(x) \in Z[G]$ as

$$A(x) = \sum_{g\in G}(a_g x^g),$$

where $a_g = 0$ when $a_g \notin A$, and $a_g = 1$ otherwise. We now define $A(x^{-1})$ by

$$A(x^{-1}) = \sum_{g\in G}(a_g x^{-g}).$$

Theorem 5.1 *For a k-subset D of a group G of order v, D is a (v, k, λ)-difference set in G if and only if the equation*

$$D(x)D(x^{-1}) = (k - \lambda) + \lambda G(x)$$

has a solution in the group ring $Z(G)$.

Example 5.2 *We return to our familiar (7,3,1) difference set in Z_7. We will write out the factors of the group ring equation separately, and then show that there is indeed a solution to this equation. We have, $G = Z_7$ and $D = \{1, 2, 4\}$.*
$D(x) = x^1 + x^2 + x^4$
$D(x^{-1}) = x^{-1} + x^{-2} + x^{-4} = x^6 + x^5 + x^3$ (exponents modulo 7)
Clearly $D(x)D(x^{-1}) = 2x^0 + (x^0 + x^1 + x^2 + x^3 + x^4 + x^5 + x^6) = 2 + 1G(x)$. So, $D(x)$ satisfies the group ring equation, confirming our earlier computations that $\{1, 2, 4\}$ forms a $(7, 3, 1)$-difference set in Z_7.

This method is clearly more efficient than writing out a list of differences. Choosing between the use of the group ring equation and the use of character theory depends on the given problem.

5.2 Hyperplanes and Normal Subgroups

So far, we have focused on difference sets in cyclic or elementary abelian groups. There are also construction methods and existence theorems specifically for groups that are neither elementary abelian nor cyclic. We present a family of difference sets due to R. McFarland, who proved their existence in 1973. McFarland difference set are constructed using cosets of hyperplanes of elementary abelian p-groups (groups which are isomorphic to $Z_p \times Z_p \times \cdots \times Z_p$). We will think of a hyperplane of an elementary abelian group of order p^{d+1} as a subgroup of order p^d.

Theorem 5.2 *[1] Let q be a prime power, r a natural number, and K* any *group of order $1 + (q^{r+1} - 1)/(q - 1) = q^r + q^{r-1} + \ldots + q + 2$. Then there exists a (v, k, λ) difference set D where*

$$\begin{aligned} v &= q^{r+1}|K| \\ k &= q^r(|K| - 1) \text{ and} \\ \lambda &= q^r(q^r - 1)/(q - 1) \end{aligned}$$

in $G = EA(q^{r+1}) \times K$, where $EA(q^{r+1})$ denotes the elementary abelian subgroup of order q^{r+1}.

Some examples of McFarland parameters are $(16, 6, 2)$, $(45, 12, 3)$, and $(441, 56, 7)$.

Lemma 5.1 *Let G be a group with a normal elementary abelian subgroup $N \cong Z_2 \times Z_2 \times \ldots \times Z_2$ where $|N| = 2^{r+1}$. Then G/N has a $(|G/N|, |G/N| - 1, |G/N| - 2)$- difference set.*

We will prove McFarland's construction with the help of Lemma 5.1 for the case where $q = 2$. The proof generalizes for q equal to any prime power.

We now restate Theorem 5.2 with $q = 2$, using the fact that $EA(2^{r+1}) \equiv Z_2^{r+1}$.

Theorem 5.3 *Let K be a group of order 2^{r+1}, and let $N \lhd G$ be an elementary abelian subgroup of order 2^{r+1}. Then there exists a $(2^{2r+2}, 2^{2r+1}-2^r, 2^{2r}-2^r)$-difference set D in $G = Z_2^{r+1} \times K$.*

Proof: We first remark that $|G/N| = 2^{r+1}$. Let $K = \{k_1, k_2, \ldots, k_{2^{r+1}}\}$ so $\{k_1N, k_2N, \ldots, k_{2^{r+1}}N\}$ are the distinct cosets of N. Let $\{k_1N, k_2N, \ldots, k_{2^{r+1}-1}N\}$ be the cosets whose leaders we arbitrarily chose to form $D = \sum_{i=1}^{2^{r+1}-1} k_iH_i$, where H_i , for each i, denotes a hyperplane.

Performing group ring computations on D gives the following.

$$D(x)D(x^{-1}) = \sum_{i=1}^{2^{r+1}-1} (x^{k_i} \sum_{h_s \in H_i} x^{h_s}) \sum_{j=1}^{2^{r+1}-1} (x^{k_j^{-1}} \sum_{h_s \in H_i} (x^{-h_s}))$$

For notational convenience, let the group ring element $\sum_{h_s \in H_i} x^{h_s}$ be represented by $H_i(x)$. We can break this into two pieces, the first piece deals with the case $i = j$ for i between 1 and $2^{r+1} - 1$, and the second piece deals with the case $i \neq j$ for i between 1 and $2^{r+1} - 1$. In the first sum, we have taken advantage of the fact that $H_i(x)H_i(x^{-1}) = |H_i|H_i(x)$. In the second sum, we have used the fact that $H_i(x)H_j(x) = \frac{1}{2}|H_i|N(x)$.

$$D(x)D(x^{-1}) = |H_i| \sum_{i=1}^{2^{r+1}-1} k_iH_i(x)k_i^{-1} + \frac{|H_i|}{2} \sum_{i \neq j} k_iN(x)k_j^{-1}.$$

Now, substituting for the given values and using the fact that N is normal, we get:

$$D(x)D(x^{-1}) = 2^r \sum_{i=1}^{2^{r+1}-1} H_i(x) + 2^{r-1} \sum_{i \neq j} a_i a_j^{-1} N(x).$$

Consider the first sum. By a counting argument, every non-identity element of N appears in $2^r - 1$ hyperplanes, and so the first sum gives every non-identity element of N $2^r - 1$ times. Further, this sum gives the identity element $2^{r+1} - 1$ times since the identity is contained in each hyperplane. The first sum gives $2^r\{(2^r - 1)(N - 1_G) + (1_G)(2^{r+1} - 1)\}$, where 1_G denotes the identity element.

Now, consider the second sum. Since $\{k_1N, k_2N, \ldots, k_{2^{r+1}-1}N\}$ forms a $(2^{r+1}, 2^{r+1} - 1, 2^{r+1} - 2)$-difference set D' in $G/N = \{k_1N, k_2N, \ldots, k_{2^{r+1}}N\}$ (by Lemma 5.1), $k_i k_j^{-1} N$ gives each element $kN \in G/N$, (for $k \notin N$ since $i \neq j$ and inverses are unique), $2^{r+1} - 2$ times, using the multiplicative definition of a difference set.

So, the second sum reduces to $2^{r-1}(2^{r+1} - 2)(k_1N + k_2N + \cdots + k_{2^{r+1}-1})N$, where $k_i \notin N$. Consider the union of these cosets. Since a disjoint union of all cosets of normal subgroup is the whole group, and since this union is lacking only the coset equivalent to N, we are left with $G \setminus N$. The second sum gives $2^{r-1}(2^{r+1} - 2)(G \setminus N)$.

Putting the two sums together gives

$$2^{2r}N(x) - 2^rN(x) - 2^{2r} + 2^r + 2^{2r+1} - 2^r + 2^{2r}G(x) - 2^{2r}N(x) - 2^rG(x) + 2^rN(x).$$

This reduces to:

$$2^{2r+1} - 2^{2r} + (2^{2r} - 2^r)G(x),$$

which is clearly equivalent to

$$(k - \lambda) + \lambda G(x),$$

implying that $D(x)$ satisfies the group ring equation. Thus D is a difference set. $\square$

Now, we provide a character theory proof of Theorem 5.2 when q is equal to any prime.

PROOF: We again consider the group $G = K \times Z_q^{r+1}$ where $|K| = \frac{q^{r+1}-1}{q-1} + 1$. There are $\frac{q^{r+1}-1}{q-1}$ hyperplanes H_i. Let

$$D = \sum_{i=1}^{\frac{q^{r+1}-1}{q-1}} k_i H_i.$$

Notice that one coset leader, $k_{\frac{q^{r+1}-1}{q-1}+1}$ is not associated with a hyperplane. Let χ be a nonprincipal character and calculate $\chi(D)$.

First, suppose that χ is nonprincipal on Z_q^{r+1}. Then, we have the following.

- $H_{i'} \subset Ker(\chi)$ for some specific hyperplane $H_{i'}$.
- $\chi(H_i) = 0$ for $i \neq i'$ by Theorem 4.1 since H_i is itself a group.
- $\chi(H_{i'}) = |H_{i'}| = q^r$

Calculating $\chi(D)$ is now greatly simplified and we have

$$|\chi(D)| = |\chi(k_{i'})\chi(H_{i'})| = q^r$$

Next, suppose that χ is principal on Z_q^{r+1} and nonprincipal on K. Then

$$|\chi(D)| = q^r \mid \sum_{i=0}^{\frac{q^{r+1}-1}{q-1}} \chi(k_i)| = q^r \mid(-\chi(k_{\frac{q^{r+1}-1}{q-1}+1}))| = q^r$$

By Theorem 4.2, since

$$|\chi(D)| = q^r = \sqrt{q^d(|G|-1) - q^d(q^d-1)/(q-1)}$$

which is equal to $\sqrt{k-\lambda}$, we have proven that D is a difference set. □

By applying a result of John Dillon, we see that McFarland difference sets need not be inside $EA(q^{r+1}) \times K$, but rather can be inside a group Γ with some normal subgroup N isomorphic to $EA(q^{r+1})$ where $\frac{|\Gamma|}{|N|} = 1 + \frac{q^{r+1}-1}{q-1}$.

The next example demonstrates the McFarland construction.

Example 5.3 *Find a $(16, 6, 2)$-McFarland difference set in $G = Z_4 \times Z_4$.*

This group has a normal subgroup isomorphic to the elementary abelian subgroup $Z_2 \times Z_2$, namely $N =< (0,2), (2,0) >$. Since N has order $2^2 = 4$, we will be looking for subgroups of order 2. Let's explicitly write out all possibilities.

$$H_1 =< (2,0) >= \{(0,0), (2,0)\}$$

$$H_2 =< (0,2) >= \{(0,0),(0,2)\}$$

$$H_3 =< (2,2) >= \{(0,0),(2,2)\}$$

Since our goal is to construct a 6-set, we now attach a coset representative to each of the three hyperplanes. One choice is to let $D = ((0,0)+ < (2,0) >) \cup ((1,0)+ < (0,2) >) \cup ((0,1)+ < (2,2) >)$. *Of course, the coset representative are chosen arbitrarily from the elements in* G.

This method can be extended to construct difference sets with parameters different from McFarland's parameters. We follow essentially the same procedure, but we attach a coset leader to the complement of a hyperplane in addition to attaching coset leaders to the remaining hyperplanes. We work through an example to demonstrate how this extension of the McFarland construction works.

Example 5.4 *Find a (36,15,6)-difference set in* $G = Z_6 \times Z_6$.

The group G *has a normal subgroup isomorphic to* $Z_3 \times Z_3$. *Specifically,* $N =< (0,2),(2,0) >$. *Hyperplanes of this group are subgroups of order 3. We write out the four hyperplanes.*

$$H_1 =< (2,0) >= \{(0,0),(2,0),(4,0)\}$$

$$H_2 =< (0,2) >= \{(0,0),(0,2),(0,4)\}$$

$$H_3 =< (2,2) >= \{(0,0),(2,2),(4,4)\}$$

$$H_4 =< (2,4) >= \{(0,0),(2,4),(4,2)\}$$

Notice that we need a difference set with 15 elements, but we have only 12 elements in the above hyperplanes. We choose to take a coset of the complement of hyperplane H_1. Since $N \equiv Z_2 \times Z_2$, the complement of H_1 has order six. The complement of order six can be written as the union of two cosets of H_1 since N can be written as the union of three distinct cosets of H_1. Thus, one choice for D is

$$((2,0) + (((0,0) + < (0,2) >) \ \cup \ ((4,0) + < 0,2 >)))$$

$$\cup \ ((1,0) + < (2,2) >)$$

$$\cup \ ((0,1) + < (2,4) >)$$

$$\cup \ ((1,1) + < (2,0) >)$$

Similar techniques for finding the complement of a hyperplane in groups other than $Z_3 \times Z_3$ are also known.

6 Partial Difference Sets and Strongly Regular Graphs

Definition 6.1 *Let D be a subset of a group G. The subset D is a partial difference set (or $\{\lambda_1, \lambda_2\}$-difference set) if the differences $x - y = v$, for $x, y \in D$ occur λ_1 times for $v \in D$ and λ_2 times for $v \notin D$, and $v \neq 0$.*

Example 6.1 *The set $D = \{1,4,9,3,12,10\}$ is a $(13,5,2,3)$-partial difference set in Z_{13}.*

When $\lambda_1 = \lambda_2$, a partial difference set reduces to an ordinary difference set, which we have already shown to be related to other combinatorial structures such as BIBD's and symmetric designs. We will now see that partial difference sets are related to combinatorial structures known as graphs.

Definition 6.2 *A* graph *is a set of points V and a set of edges E along with an incidence relation between the points and edges.*

We will call the points of a graph vertices. Edges begin and end at vertices. The incidence relation is adjacency, which describes how the vertices and edges are connected. The number of edges that are incident with a given vertex is called the *degree* of the vertex. For our purposes, all graphs are *connected*, which means that there are no isolated vertices.

Definition 6.3 *A* regular graph *is a graph where each vertex has the same degree, say r.*

Definition 6.4 *[5] A* strongly regular graph *with parameters (v, r, h_1, h_2) is a regular graph with v vertices of degree r, such that for any pair of adjacent vertices x and y, there are exactly h_1 vertices adjacent to x and to y, and for any pair of non-adjacent vertices, there are exactly h_2 vertices adjacent to x and to y.*

It is easy to see that a pentagon is a strongly regular graph with parameters (5,2,0,1). A more interesting (and quite famous) example of a strongly regular graph is the Peterson graph. This strongly regular graph has parameters (10,3,0,1).

Partial difference sets are related to ordinary difference sets in a manner analogous to the way regular graphs are related to strongly regular graphs. Furthermore, partial difference sets are equivalent to certain strongly regular graphs [2].

7 Hadamard matrices, designs, and difference sets

J. Hadamard (1865-1963) started a long line of research when he pondered what could be done with matrices whose entries were real, with absolute value at most one. The matrices that intrigued him naturally took his name, and they have become building blocks for other combinatorial structures.

Definition 7.1 *[1] A Hadamard matrix H_m is an $m \times m$ matrix with entries chosen from $\{1, -1\}$ such that*

$$HH^T = mI,$$

and thus also

$$H^T H = mI.$$

For any given Hadamard matrix, there is an equivalent one for which the first row and the first column consist entirely of +1's, and this is known as a *normalized* Hadamard difference set. Although there are many known construction methods for finding Hadamard matrices, the conjecture that a Hadamard matrix of order m exists for all $m \equiv 0 \pmod 4$ remains open.

There is a continued interest in constructing Hadamard matrices because of their applications in error-correcting codes. This important part of coding theory is concerned with transmitting data that passes through a noisy channel.

Hadamard designs, defined below, are a family of symmetric designs that have applications in coding theory and relate to difference sets.

Definition 7.2 *[6] Let H_{4k} be a normalized Hadamard matrix. Delete the first row and the first column. A* Hadamard 2-design *is constructed by letting the rows of this matrix be the points, and letting each column define a block. Each column defines a subset of the rows (points), namely those rows for which there is a +1 in the column. Any pair of points is contained in exactly* $k-1$ *blocks and each block has size* $2k-1$*. A Hadamard 2-design is then a symmetric* $(4k-1, 2k-1, k-1)$*-design.*

Hadamard-Paley difference sets have the same parameters as these designs. In certain groups, these difference sets are easily constructed using the following theorem by Paley and Todd.

Theorem 7.1 *[5] Let* $q = 4n-1$ *be a prime power. Then the set D of non-zero squares in F_q is a* $(4n-1, 2n-1, n-1)$*-Hadamard-Paley difference set in the additive group of F_q.*

The existence of another family of Hadamard-Paley difference sets was proved by Stanton and Sprott in 1958.

Theorem 7.2 *[5] If q and $q+2$ are both odd prime powers, then with $4n-1$ $= q(q+2)$, there exists a $(4n-1, 2n-1, n-1)$-Hadamard-Paley difference set in the additive group of the ring $R = F_q \times F_{q+2}$.*

Recall that the above combinatorial structures are based on Hadamard matrices that have the first row and column deleted. There is another group of combinatorial structures based on "full order" Hadamard matrices.

Definition 7.3 *A Hadamard difference set has parameters $(4m^2, 2m^2-m, m^2-m)$.*

There is a family of designs, presented in the theorem below, that has the same parameters as Hadamard difference sets. We first define the incidence matrix of a design.

Definition 7.4 *Given an incidence structure $(P, \mathbf{B}, I)$, with v points and k points per block, an* incidence matrix *N is the V by k matrix with rows indexed by the points p of P, columns indexed by the blocks B of $\mathbf{B}$, and the entry $N(p, B) = 1$ if p is incident with B, and $N(p, B) = 0$ otherwise.*

Theorem 7.3 *[1] If a symmetric design with $v = 4(k-\lambda) \geq 2k$ exists, then it has parameters $(4m^2, 2m^2-m, m^2-m)$, and its $(-1,1)$-incidence matrix is a Hadamard matrix.*

Recently there has been much research focusing on Hadamard difference sets. Sections 8 and 9 present some of the new families of Hadamard difference sets, as well as the constructions used to form them.

Before we present the new construction techniques, we would like to stress the importance of these new results. The study of difference sets is complicated by many facts. For example, Theorems 7.1 and 7.2 each identify a family of Hadamard-Paley difference sets, but the constructions used in each case turn out to be quite different. Discovering a family of (v, k, λ)- difference sets in one group G does not usually lead to the discovery of (v, k, λ)-difference sets in some other group Γ. Even if a difference set with these parameters can be found in Γ, it is probable that a different construction will be necessary to form it. Furthermore, construction techniques change as the desired parameters change. For example, the McFarland construction yields difference sets only with McFarland parameters. It is a bonus that the McFarland construction can be extended by using complements of hyperplanes to produce difference sets with parameters different from McFarland's parameters. This extension makes the McFarland construction exceedingly interesting. So far, we have introduced difference sets with McFarland, Hadamard-Paley, and Hadamard parameters. In Section 9, we present a family of difference sets with new parameters. Including this new family, there are only approximately seven different classifications of difference set parameters. It is rare and exciting when a new family of parameters is found.

8 Wilson and Xiang

Wilson and Xiang recently announced results from their study of $(4m^2, 2m^2 - m, m^2 - m)$-Hadamard difference sets [6]. Problems in this area focus on the study of which groups of order $4m^2$ contain a Hadamard difference set. They present a new construction producing a family of Hadamard difference sets where $m = 2^a 3^b 5^{2c_1} 13^{2c_2} 17^{2c_3} p_1^2 p_1^2 \dots p_1^2$ with a, b, c_1, c_2, c_3 positive integers, and with each p_i a prime congruent to 3 modulo 4, for $1 \leq i \leq t$. Their construction relies on a clever choice of projective sets and spreads.

8.1 Projective Sets and Spreads

A projective geometry of dimension $k - 1$ and order q, which we denote by $PG(k-1, q)$, is fundamentally connected to a k dimensional vector space over $GF(q)$, which we denote by $W = V^k(q)$. The points of $PG(k-1, q)$ are the 1-dimensional (linear) subspaces of $V^k(q)$, and so there are $\frac{q^{k+1}-1}{k-1}$ projective points of $PG(k-1, q)$. The hyperplanes of $PG(k-1, q)$ are the $k - 1$-dimensional subspaces of $V^k(q)$. For more information on projective geometries, please see [5].

Definition 8.1 *A* projective (n, k, h_1, h_2) set *O is a proper, non-empty set of n points of the projective space $PG(k-1, q)$ (where q is a power of prime p) with the property that every hyperplane meets O in h_1 points or h_2 points.*

Projective (n, k, h_1, h_2) sets are equivalent to certain strongly regular graphs, which, as seen in Section 6, are also equivalent to partial difference sets.

Definition 8.2 *A* spread *is a family of j-dimensional subspaces of a vector space that partition the 1-dimensional subspaces, i.e. every 1-dimensional subspace is contained in exactly one member of the family.*

In other words, a spread is a family of j-dimensional subspaces such that any two j-dimensional subspaces intersect only at the 0-subspace, but such that their union is the entire k-dimensional vector space.

Let $\Sigma_3 = PG(3,p)$ denote projective 3-space over $GF(p)$, where p is an odd prime. A spread of Σ_3 is any collection of p^2+1 pairwise disjoint lines (2-subspaces) of Σ_3 which partition the points (1-subspaces) of Σ_3.

Definition 8.3 *A* partial spread *in Σ_3 is a set of mutually non-intersecting lines.*

For convenience, Wilson and Xiang call a subset of Σ_3 "type Q" if it is a projective $(\frac{(p^4-1}{4(p-1)}, 4, \frac{(p-1)^2}{4}, \frac{(p+1)^2}{4})$ set.

Wilson and Xiang's fundamental theorem follows:

Theorem 8.1 *[6] Assume that $S = (L_1, L_2, \ldots, L_{p^2+1}\}$ is a spread of Σ_3. If there exist two subsets C_0, C_1 of type Q in Σ_3 such that $|C_0 \cap L_i| = \frac{p+1}{2}$, $1 \leq i \leq s$, and $|C_1 \cap L_j| = \frac{p+1}{2}$, $(s+1) \leq j \leq 2s$, where $s = \frac{p^2+1}{2}$, then there exists a Hadamard difference set in $H \times (Z_p)^4$, where H is either the Klein 4-group or the cyclic group of order 4.*

We state without proof that $C_2 = (L_1 \cup \ L_2 \cup \cdots \cup \ L_s) \setminus C_0$ and $C_3 = (L_{s+1} \cup \ L_{s+2} \cup \cdots \cup \ L_{2s}) \setminus C_1$ are also sets of type Q. Following Wilson and Xiang, A is the partial spread formed by taking the union of any $\frac{p^2-1}{4}$ lines from $L_{s+1}, L_{s+2}, \ldots, L_{2s}$, and B is the partial spread formed by taking the union of any $\frac{p^2-1}{4}$ lines from $L_1, L_2, \ldots, L_s$, where L_i for $1 \leq i \leq s$ are the lines that form the spread of Σ_3. Define

$$D_0 = C_0 \ \cup \ A,$$

$$D_1 = C_1 \ \cup \ B,$$

$$D_2 = C_2 \ \cup \ A,$$

$$D_3 = C_3 \ \cup \ B.$$

Corollary 8.1 *Let $K = \{k_0, k_1, k_2, k_3\}$ be either group of order 4. Then*

$$D = k_0(V^4(p) \setminus D_0) \cup \ k_1 D_1 \cup \ k_2 D_2 \cup \ k_3 D_3$$

is a $(4p^4, 2p^4 - p^2, p^4 - p^2)$-Hadamard difference set in $H \times (Z_4)^p$.

The points in the sets used in Corollary 8.1 are written additively. In general, changing from multiplicative to additive notation requires a chart. For example, the conversion chart used for the case $PG(3, 5)$ is given at the end of this section.

Notice that the construction in Corollary 8.1 is similar to the extension of the McFarland construction which uses the complement of one hyperplane unioned with cosets of the remaining hyperplanes. (See Example 5.4.) Here, the D_i's, for $0 \leq i \leq 3$ are analogous to the hyperplanes.

With the help of Theorem 8.1, in order to construct Hadamard difference sets in $H \times Z_p^4$, where $|H| = 4$ and p a prime with $p \equiv 3 \pmod 4$, we need only construct a spread in Σ_3 and sets C_0, C_1 of type Q that satisfy the technical requirements. Wilson and Xiang provide algorithms that work only in special cases.

We will first present a construction for the special case where p is a prime with $p \equiv 3 \pmod 4$. Let β be a primitive element of $GF(p^4)$. Here, we interpret Σ_3 by viewing $GF(p^4)$ as a 4-dimensional vector space over $GF(p)$. In this context, the points of Σ_3 can be represented by $< 1 >$, $< \beta >$, $\ldots$, $< \beta^{(p^2+1)(p+1)-1} >$. Let $L_i = \{< \beta^i >, < \beta^{(p^2+1)+i} >, \ldots, < \beta^{p(p^2+1)+i} >\}$ for $0 \leq i \leq p^2$. The collection of "lines" $S = \{L_0, L_1, \ldots, L_{p^2}\}$ forms a spread in Σ_3. Appropriate sets C_0 and C_1 are chosen as:

$$C_0 = \{< 1 >, < \beta^4 >, < \beta^8 >, \ldots, < \beta^{(p^2+1)(p+1)-4} >\}$$

$$C_1 = \{< \beta >, < \beta^5 >, < \beta^9 >, \ldots, < \beta^{(p^2+1)(p+1)-3} >\}$$

These sets are proved to be of type Q by uniform cyclotomy, and quick counting will show that the other constraints are satisfied.

Wilson and Xiang also provide a method to construct sets of type Q in $\Sigma_3 = PG(3, p)$ for the special case $p \equiv 1 \pmod 4$. We will rely on Σ_3's association with $W = V^4(p)$, the 4-dimensional vector space over $GF(p)$. The key to this construction depends on viewing W as 2-dimensional over

$GF(p^2) \times GF(p^2)$. We will work through the construction for the case $PG(3,5)$.

Our first step in constructing a difference set in $PG(3,5)$ is to find a spread. As in the case above, we begin by forming lines. Let $L_\infty = \{0\} \times GF(25)$ be a line, or two-dimensional subspace. For all $d \in GF(25)$, let $L_d = \{(x, dx^5) | x \in GF(25)\}$. The set $S = L_\infty U \{L_d\}_{d \in GF(25)}$ is a spread of Σ_3 that consists of 26 lines with 25 points on each line. The points of the lines L_d are disjoint two-dimensional subspaces over $GF(5)$ and one-dimensional subspaces over $GF(25)$.

The next step is to construct sets C_0 and C_1 of type Q. Wilson and Xiang define a map T to facilitate the construction of these sets.

Let g be a primitive element of $GF(25)$. Consider the action of the mapping $T = \begin{pmatrix} g^2 & 0 \\ 0 & g^{-2} \end{pmatrix}$ on the points of Σ_3, which we are viewing as one-dimensional subspaces of $GF(25) \times GF(25)$, which in turn we viewed as a vector space over $GF(5)$. Constructing sets of type Q depends on the orbits of the action of T on Σ_3. These orbits fall into two categories.

In $PG(3,p)$:

1. There are four short orbits, each of length $(p+1)/2$. For $PG(3,5)$, choices for the representatives of these 4 orbits are (0,1), (0,g), (1,0), and (g,0). Each short orbit clearly consists of points from L_0 or L_∞.

2. There are $4(p+1)$ long orbits, each of length $(p^2-1)/4$. Representatives of these orbits are

$$(1,1),(1,g),(1,g^2),\ldots,(1,g^{2*p+1})$$

$$(g,1),(g,g),(g,g^2),\ldots,(g,g^{2*p+1})$$

Each long orbit consists of $(p+1)/2$ points of $(p-1)/2$ lines from the set $\{L_d | d \neq 0, d \in GF(p^2)\}$.

Continuing with the example $PG(3,5)$, we first write the elements of each orbit so that each column consists of three points on some line L_d, $d \neq 0$, $d \in GF(25)$. For the orbit of $(1,g)$, we get:

$$\begin{array}{rcl} (1,g) & \to & (g^2,g^{23}) \\ (g^4,g^{21}) & \to & (g^6,g^{19}) \\ (g^8,g^{17}) & \to & (g^{10},g^{15}) \end{array}$$

The first column consists of points on L_g, while the second column consists of three points on the line $L_{g^{13}}$. For $PG(3,5)$, we noticed that the orbit represented by $(1,g^i)$ will consist of 3 projective points on L_{g^i} and 3 projective points on $L_{g^{i+12}}$. Recall that each such line contained 6 projective points. We remark that orbits consist of combinations of "half-lines."

Wilson and Xiang discovered by computer search that taking unions of certain orbits forms projective sets C_0, C_1 in $PG(3,5)$ of type Q.

In $PG(3,5)$, if g is a root of $x^2+x+2 \in GF(5)[x]$, then C_0 consists of orbits of

$$(1,g),(1,g^2),(1,g^9),(1,g^{11}),(g,1),(g,g^8),(1,0)$$

where the first six orbits are long, and the last orbit is short. Thus, C_0 consists of 39 projective points in Σ_3.

We will write out all of the orbits, showing which lines contribute to each orbit.

orbit $(1,g)$:	From L_g :	From $L_{g^{13}}$
	$(1,g)$	(g^2,g^{23})
	(g^4,g^{21})	(g^6,g^{19})
	(g^8,g^{17})	(g^{10},g^{15})
orbit $(1,g^2)$:	From L_{g^2} :	From $L_{g^{14}}$
	$(1,g^2)$	(g^2,g^{24})
	(g^4,g^{22})	(g^6,g^{19})
	(g^8,g^{18})	(g^{10},g^{16})
orbit $(1,g^9)$:	From L_{g^9} :	From $L_{g^{21}}$
	$(1,g^9)$	(g^2,g^7)
	(g^4,g^5)	(g^6,g^3)
	(g^8,g^1)	(g^{10},g^{23})
orbit $(1,g^{11})$:	From $L_{g^{11}}$:	From $L_{g^{23}}$
	$(1,g^{11})$	(g^2,g^9)
	(g^4,g^7)	(g^6,g^5)

	(g^8, g^3)	(g^{10}, g^1)
orbit $(g, 1)$:	From $L_{g^{19}}$:	From L_{g^7}
	$(g, 1)$	(g^3, g^{22})
	(g^5, g^{20})	(g^7, g^{18})
	(g^9, g^{16})	(g^{11}, g^{14})
orbit (g, g^8):	From L_{g^3} :	From $L_{g^{15}}$
	(g, g^8)	(g^3, g^6)
	(g^5, g^4)	(g^7, g^2)
	(g^9, g^0)	(g^{11}, g^{22})
orbit $(1, 0)$:	From L_0 :	
	$(1, 0)$	
	$(g^2, 0)$	
	$(g^4, 0)$	

Note that the short orbit terminates after three elements because $(g^6, 0) \equiv (1, 0)$ in projective space since g^6 is viewed additively as the scalar 2.

This table is useful for interpreting how the points and lines contribute to C_0. C_0 consists of points on lines L_{g^i} where $i \in \{1, 2, 3, 7, 9, 11, 13, 14, 15, 19, 21, 23\}$ L_0.

C_1 consists of points on lines L_{g^i} where $i \in \{4, 5, 6, 8, 10, 12, 16, 17, 18, 20, 22, 24{=}0\}$ and L_∞.

This construction technique has relied on multiplicative computations performed on the multiplicative group inside $GF(25)$, but we now must make use of the additive structure of the field since Corollary 8.1 uses the sets D_i, $0 \leq i \leq 3$, written additively. Understanding the structure of the resulting difference set requires understanding the relationship between the multiplicative and additive groups inside $GF(25)$. The conversion table at the end of this section uses a primitive element $g \in GF(25)$ that satisfies $x^2 + x + 2 = 0$. In order to construct the difference set described in Corollary 8.1 for $p = 5$, we look at the $4(39) = 156$ affine points in Z_5^4 that are associated with the 39 projective points in C_0, and similarly for the 39 projective points in each of C_1, C_2, and C_3 the 36 projective points in each of partial spreads A and B. By examining the table at the end of this section, we note that there are 4 constants in $GF(25)$ when elements are viewed additively: $g^{24} = 1$, $g^6 = 2$, $g^{18} = 3$, and $g^{12} = 4$. We can essentially multiply each of the 39 projective points in C_0 by each of the 4 constants to get 156 affine points. We view the 39 projective points in each set C_1, C_2, and C_3 and the 36 projective points on each partial spread A and B in the same way. We now see that each D_i, $0 \leq i \leq 3$, consists of 300 affine points. Corollary 8.1 forms the difference set by taking the complement of D_0, which contains $(625 - 300) = 325$ affine points, unioned with the remaining three D_i's, for a total of $325 + 3(300) = 1225$ affine points. Thus, as expected, we have constructed a difference set with parameters $(2500, 1225, 600)$.

$g^1 = g$	$g^9 = 4+3g$	$g^{17} = 1+g$
$g^2 = 3+4g$	$g^{10} = 4+g$	$g^{18} = 3$
$g^3 = 2+4g$	$g^{11} = 3+3g$	$g^{19} = 3g$
$g^4 = 2+3g$	$g^{12} = 4$	$g^{20} = 4+2g$
$g^5 = 4+4g$	$g^{13} = 4g$	$g^{21} = 1+2g$
$g^6 = 2$	$g^{14} = 2+g$	$g^{22} = 1+4g$
$g^7 = 2g$	$g^{15} = 3+g$	$g^{23} = 2+2g$
$g^8 = 1+3g$	$g^{16} = 3+2g$	$g^{24} = 1$

9 Chen

Chen recently introduced a construction method for finding $(4m^2, 2m^2 - m, m^2 - m)$ Hadamard difference sets in abelian groups of order $4m^2$, whose Sylow p-subgroups are elementary abelian. Chen's work is based on the ideas set forth by Wilson and Xiang regarding spreads and subsets of type Q. Above, we described how Wilson and Xiang used the orbits of a mapping T to find sets of type Q. Chen was able to generalize their results and provide formulae for building these sets without the need for a mapping like T or a computer search. Instead, Chen forms projective sets of type Q from relative $(q+1, 2, q, \frac{q-1}{2})$-difference sets.

Chen's spread in $PG(3,q)$ is composed in the same way used by Wilson and Xiang. Chen uses slightly differently notation, and we present it now since it is related to the notation used for the type Q sets that we explain below.

For each $d \in GF(q^2)$, let

$$L_d = \{(\beta, d\beta) \mid \beta \in GF(q^2)^*\}$$

and define

$$L_\infty = \{(0, \beta) \mid \beta \in GF(q^2)^*\}$$

The collection of these 26 lines forms a spread in Σ_3.

9.1 Relative Difference Sets

This section presents some of the results related to relative difference sets that are needed for the construction method in [3].

Definition 9.1 *[3] Let G be a group and H a subgroup of G. A subset $R \subset G$ is called a* relative $(G/H, H, R, \lambda)$-difference set of G relative to H *if the differences $r - r' = g$ for $r, r' \in R$ occur λ times for $g \in G \setminus H$ and zero times when g is any nonidentity element in H.*

There is an analogous group ring equation to check for the existence of relative difference sets.

Theorem 9.1 *A subset $R \subset G$ is a relative $(G/H, H, R, \lambda)$-difference set of G relative to a subgroup $H \subset G$ if and only if*

$$R(x)R(x^{-1}) = |R| + \lambda(G \setminus H).$$

When $H = 1$, the relative difference set is also a "ordinary" difference set.

An alternative way to describe relative difference sets follows:

$$|gR \cap R| = \lambda, \text{ if } g \in G \setminus H$$

$$|gR \cap R| = 0, \text{ if } g \in H \setminus \{1\}.$$

The construction techniques of Chen use relative difference sets and a trace map [3].

Definition 9.2 *The* relative trace $Tr_{q^n} : GF(q^n) \to GF(q)$ *the map defined by* $Tr_{q^n}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}$.

Theorem 9.2 *[3]*

$$R = \{\alpha \in GF(q^n)^* | Tr_{q^n/q}(\alpha) = 1\}$$

is a relative $(\frac{q^n-1}{q-1},\ q-1,\ q^{n-1},\ q^{n-2})$*-difference set in* $GF(q^n)^*$ *relative to* $GF(q)^*$.

Following Chen, let S_q denote the set of nonzero squares of $GF(q)$ and N_q denote the set of nonsquares of $GF(q)$.

Theorem 9.3 *[3]*

$$\overline{R} = \{\overline{\alpha} \in GF(q^2)^*/S_q \mid Tr_{q^2/q}(\alpha) \in S_q\}$$

is a relative $(q+1, 2, q, (q-1)/2)$*-difference set in* $GF(q^2)^*/S_q$.

9.2 Chen's Hadamard Construction

Chen defines π to be the natural surjection from $GF(q^2)^*$ to $GF(q^2)^*/S_q$. Let X be the preimage of $\overline{R}$ in $GF(q^2)^*$, or in other words, $X = \{\alpha \in GF(q^2)^* | Tr_{q^n}(\alpha) \in S_q\}$. Chen defines $X^g = \pi^{-1}(\overline{gR})$ for every $g \in GF(q^2)^*$, and we can write $X^g = \{g\alpha | \alpha \in X\}$ for every $g \in GF(q^2)^*$. The sets X and X^g are used to construct sets X_1, X_2, X_3, and X_4 that form a spread in $GF(q^2)^*$.

$$\begin{aligned} X_1 &= X - (X \cap X^g), \\ X_2 &= X^g - (X \cap X^g), \\ X_3 &= X \cap X^g, \\ X_4 &= GF(q^2)^+ - (X \cup X^g) = GF(q^2)^+ - X_1 - X_2 - X_3. \end{aligned}$$

Chen defines projective $(\frac{q^4-1}{4(q-1)}, 4, \frac{(q-1)^2}{4}, \frac{(q+1)^2}{4})$ sets C_0, C_1, C_2, and C_3 using the sets X_i as well as the sets of nonsquares and squares of $GF(q^2)$. Let $P_{q^2} \in \{S_{q^2}, N_{q^2}\}$ and let Q_{q^2} be the other choice. Set

$$\begin{aligned} C_0 &= \{(\beta, d\beta) \mid \beta \in S_{q^2}, d \in X_1\} \ \cup \\ &\quad \{(\beta, d\beta) \mid \beta \in N_{q^2}, d \in X_2\} \ \cup \\ &\quad \{(0, \beta) \mid \beta \in Q_{q^2}\}, \end{aligned}$$

$$\begin{aligned} C_1 &= \{(\beta, d\beta) \mid \beta \in S_{q^2}, d \in X_3\} \ \cup \\ &\quad \{(\beta, d\beta) \mid \beta \in N_{q^2}, d \in X_4\}, \end{aligned}$$

$$\begin{aligned} C_2 &= \{(\beta, d\beta) \mid \beta \in N_{q^2}, d \in X_1\} \ \cup \\ &\quad \{(\beta, d\beta) \mid \beta \in S_{q^2}, d \in X_2\} \ \cup \\ &\quad \{(0, \beta) \mid \beta \in P_{q^2}\}, \end{aligned}$$

$$\begin{aligned} C_3 &= \{(\beta, d\beta) \mid \beta \in N_{q^2}, d \in X_3\} \ \cup \\ &\quad \{(\beta, d\beta) \mid \beta \in S_{q^2}, d \in X_4\}. \end{aligned}$$

Recall that for each $d \in GF(q^2)$, $L_d = \{(\beta, d\beta) \mid \beta \in GF(q^2)^*\}$. Notice that the above sets of type Q consist of subsets of projective points on these lines. In fact, the way that Chen uses S_{q^2} and N_{q^2} means that each set of type Q consists of a collection of "half-lines." Of course, we are reminded that the orbits of the map T that were used to form the sets of type Q in Section 8 also consisted of "half-lines." Clearly, there is a connection between Wilson and Xiang's method that requires a mapping and a computer search and Chen's method that uses these explicit formulae. Understanding the correspondence between the two methods is non-trivial.

Chen uses his spread and sets of type Q to construct new $(4q^4, 2q^4-q^2, q^4-q^2)$-Hadamard difference sets. Chen proves that his construction yields such Hadamard difference sets by describing how to form the difference set, and then applying character theory to the result. Let $K = \{k_0, k_1, k_2, k_3\}$, and let $V^4(q)$ denote a 4-dimensional vector space over $GF(q)$. Similar to the Xiang-Wilson construction, A is any union of $\frac{q^2-1}{4}$ lines from $\{L_{1+\frac{q^2+1}{2}} \cup L_{2+\frac{q^2+1}{2}} \cup \ldots \cup L_{q^2+1}\}$ and B is any union of of $\frac{q^2-1}{4}$ lines from $\{L_1, L_2, \ldots, L_{\frac{q^2+1}{2}}\}$.

Again, define the following four sets:

$$D_0 = C_0 \cup \ A,$$

$$D_1 = C_1 \cup \ B,$$

$$D_2 = C_2 \cup \ A,$$

$$D_3 = C_3 \cup \ B.$$

Corollary 9.1 *The set*

$$D = k_0(V^4(q) - D_0) + k_1 D_1 + k_2 D_2 + k_3 D_3$$

is a $(4q^2, 2q^2 - q^2, q^4 - q^2)$*-Hadamard difference set in* $G = K \times V^4(q)$.

Again, notice that the construction for D is related to the extension of the McFarland construction.

9.3 Chen's Generalized Hadamard Difference Sets

The above results do more than produce a new family of Hadamard difference sets: Chen was able to generalize his technique to produce (non-Hadamard) difference sets with parameters $(4m^{2n}\frac{m^{2n}-1}{m^2-1},\ m^{2n-1}(\frac{2(m^{2n}-1)}{m+1}+1),\ (m^{2n}-m^{2n-1})\frac{m^{2n-1}+1}{m+1})$, for $m = q^2$, where q is an odd prime power, and for $m = 36t$ where t is a positive integer. Chen calls this new family generalized Hadamard difference sets [3]. Notice that in the case $n = 1$, generalized Hadamard difference sets reduce to "ordinary" Hadamard difference sets.

Chen uses sets D_0, D_1, D_2, and D_3 and applies the above results in the group $GF(q^4)$ rather than in $GF(q^2) \times GF(q^2)$.

Consider the vector space $V^n(q^4) = (GF(q^4))^n$, which has $\frac{q^{4n}-1}{q^4-1}$ hyperplanes. For each hyperplane H_i in this vector space, look at the natural surjection

$$\Phi_i : V^n(q^4) \rightarrow V^n(q^4)/H_i \cong GF(q^4).$$

In relation to Chen's previous work, his sets D_j, $0 \leq j \leq 3$, are found in $GF(q^4)$. If we look at the pre-images $\Phi_i^{-1}(D_j)$ for $1 \leq i \leq \frac{q^{4n}-1}{q^4-1}$ and $1 \leq j \leq 3$, we get $t = \frac{4(q^{4n}-1)}{q^4-1}$ subsets $U_1, U_2, \ldots, U_t$ of size $\frac{q^{4n}-q^{4n-2}}{2}$ inside $V^n(q^4)$.

Theorem 9.4 *Let $K = \{k_1, k_2, \ldots, k_t\}$ where $t = |K| = \frac{4(q^{4n}-1)}{q^4-1}$. Let U_k be sets obtained as described above. Then*

$$D = k_1(V^n(q^2) - U_1) + \sum_{i=2}^{m} k_i U_i$$

is a $(4q^{2n}\frac{q^{2n}-1}{q^2-1},\ q^{2n-1}(\frac{2(q^{2n}-1)}{q+1}+1),\ (q^{2n}-q^{2n-1})\frac{q^{2n-1}+1}{q+1})$-generalized Hadamard difference set in the group $G = K \times V^n(q^2)$.

This generalized Hadamard difference set contains a coset of the complement of a hyperplane unioned with cosets of the remaining hyperplanes, which again mimics the extension of the McFarland construction. We remark that the sets U_i play the same role in constructing generalized Hadamard difference sets that their images, the sets D_i, play in constructing Hadamard difference sets. The generalized Hadamard difference sets are obtained by *lifting* the pieces involved with Chen's Hadamard construction.

10 Combinatorial Analysis

The majority of results surveyed in this paper are proved using character theory. Looking at the recent Hadamard and generalized Hadamard constructions from a combinatorial view may prove beneficial. Combinatorial analysis of the individual pieces that form the difference set may provide a better understanding of the final results that character theory proves as a collective unit. The goal is to fully comprehend why the construction method works in order to generalize it. For example, it may be possible to use a similar construction method to produce difference sets in groups other than $GF(q^2) \times GF(q^2)$ or $GF(q^4)$.

Proving that Chen's D is a difference set involves looking at $D(x)D(x^{-1})$ in order to check if $D(x)$ satisfies the group ring equation. By the definition of D, we see that this computation will involve pieces of the form $D_i(x)D_i(x^{-1})$ and $D_i(x)D_j(x^{-1})$. Our work involves combinatorial analysis of these pieces.

First we notice that by the nature of these sets, $D_i^{-1} = D_i$. We analyzed the product

$$D_0D_1 = (C_0 \cup \ A)(C_1 \cup \ B)$$

for the example in $PG(3,5)$. From character theory, we know that this product yields $144Z_5^4$. We were interested in obtaining a combinatorial proof using the component pieces AB, C_0C_1, C_0B, and C_1A.

Computing AB deals with multiplying full lines by full lines. Using the group ring, we found that

$$AB = 36Z_5^4 - 36(0,0) - 6A - 6B.$$

Computing C_0C_1 deals with multiplying half-lines by other distinct half-lines. Here, we must introduce new notation. Recall that L_d consists of 6 projective points, and C_i, for $0 \leq i \leq 3$, consists of the union of halves of these lines. We use $l_d^{(1)}$ to denote the half of L_d that is found in C_i, and we use $l_d^{(2)}$ to denote the half of L_d that is not found in C_i. We found that

$$\begin{aligned} C_0C_1 &= 169Z_5^4 - 169(0,0) - \\ &\quad 13(L_0 \cup L_1 \cup \ldots \cup L_{12}) - \\ &\quad 13(L_{13} \cup L_{14} \cup \ldots \cup L_{25}) - \\ &\quad l_i^{(2)} L_j \text{ for } i \in \{0,1,\ldots,12\} - \\ &\quad l_i^{(1)} l_j^{(2)} \text{ for } j \in \{13,14,\ldots,25\}. \end{aligned}$$

The remaining two products are more difficult because they involve multiplying half-lines by full lines. Let $\overline{A}$ be the lines in $\{L_{13}, L_{14}, \ldots, L_{25}\}$ that were not chosen to be in A.

We found that

$$\begin{aligned} AC_1 &= 72Z_5^4 + 72(0,0) + 6A - 6(\overline{A}) - \\ &\quad L_i l_j^{(2)} \text{ (where } L_i \in A \text{ and } l_j^{(2)} \in A) - \end{aligned}$$

$$L_i l_j^{(2)} \text{ (where } L_i \in A \text{ and } l_j^{(2)} \in \overline{A}.)$$

An analogous result holds for BC_0.

The four individual products should combine to give $144Z_5^4$, but it is not obvious how to manipulate the products for a clear comparison. In a recent paper, Wilson and Xiang remark that it appears difficult to prove this result in this manner [7]. This problem merits further investigation.

11 Acknowledgments

I thank Dr. James Davis for guiding me down the path from learning simple definitions to analyzing the most recent developments in the study of difference sets. I also thank Dr. Gary Greenfield for his beneficial help in editing previous versions of this paper. Their suggestions have been invaluable.

References

[1] T.Beth, D.Jungnickel, H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 1986.

[2] R. Calderbank and W.M.Kantor, "The geometry of two-weight codes," Bull. Lond Math. Soc. **18** (1986), 97-122.

[3] Y. Q. Chen, "On the existence of abelian Hadamard difference sets and generalized Hadamard difference sets," pre-print, 1996.

[4] M. Hall, *Combinatorial Theory*, Blaisdell Publishing Company, Waltham, MA, 1967.

[5] J. H. van Lint and R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press, New York, NY, 1994.

[6] R. M. Wilson and Q. Xiang, "Constructions of Hadamard difference sets," J. Combin. Theory (A), 77, 148-160, 1997.

[7] R. M. Wilson and Q. Xiang, "Cyclotomy, Half Ovoids, and two-weight codes," pre-print, 1997.