DIFFERENCE SETS IN ABELIAN GROUPS AND THEIR GENERALIZATIONS

by

Gregory M. Trout

A thesis submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Master of Science in Mathematics

Summer 2017

DIFFERENCE SETS IN ABELIAN GROUPS

AND THEIR GENERALIZATIONS

by

Gregory M. Trout

Approved: _____

Qing Xiang, Ph.D.
Professor in charge of thesis on behalf of the Advisory Committee

Approved: _____

Louis Rossi, Ph.D.
Chair of the Department of Mathematics

Approved: _____

George Watson, Ph.D.
Dean of the College of Arts & Sciences

Approved: _____

Ann L. Ardis, Ph.D.
Senior Vice Provost for Graduate and Professional Education

ACKNOWLEDGMENTS

Thanks are due to Ben Nassau, Patrick Cesarz, Emily Bergman, and Kelvin Rivera-Lopez for the many valuable discussions I have had with them on this subject. I also appreciate very much the assistance of Sam Cogar, who read many rough drafts of my work and offered valuable corrections and improvements.

I thank Professor Harriet Pollatsek and Dr. John F Dillon for their thoughtful correspondence and assistance with several problems. Professor Mahya Ghandehari, Professor Felix Lazebnik, Professor Robert Coulter, and Professor Louis Rossi provided kind and encouraging words at many steps throughout the process, for which I thank them as well.

Ms. Deborah See deserves accolades for her ability to fix just about any logistical problem. Professor Francisco-Javier Sayas deserves similar accolades for his problem-solving skills related to my defense, and for being an ideal Graduate Director.

Of course, I thank my committee members: Professor Sebastian Cioaba and Professor Nayantara Bhatnagar, for their kindness, helpfulness, flexibility, and thoughtful insight.

Special thanks to Professor Qing Xiang, my advisor, for inspiring me, guiding me, believing in me, and encouraging me to continue studying mathematics. I also appreciate his willingness to take on this extra project to help me further my education.

This work is dedicated to my beautiful and brilliant wife-to-be, Hillary, for being a constant source of encouragement and joy, and for being my biggest champion.

TABLE OF CONTENTS

ABSTRACT

Difference sets exist at the intersection of algebra and combinatorics, and are motivated by a practical and efficient constructive method for symmetric block designs. Many of the seminal papers on the subject, such as those by Bose [10], Hall [40], Singer [83], and Bruck [13], deal with this explicitly. More specific uses include the construction of complex vector codes satisfying the Welch bound [93]. A short 1979 treatise by Camion [14] frames the entire study of difference sets in terms of linear projective codes, and entire books on this subject have since been written as well [32]. For uses of difference sets and combinatorial designs in computer science, the paper of Colbourn and van Oorschot [20] is fairly comprehensive, and difference sets have played a large role in the field of cosmology, where they are used for special kinds of imaging [103]. More recently, applications of difference sets to signal processing [101] and quantum information and computing [78] have become active areas of research. Moore and Pollatsek [72] note that member nations of the North Atlantic Treaty Organization (NATO) have sponsored advanced study on difference sets as well.

In this work we define difference sets, give several standard results on abelian difference sets, and discuss the uses of tools such as multipliers, the integral group rings, and characters to prove existence and nonexistence of various possible difference sets. We close with a brief survey of some recent work on some open conjectures (we take 'recent' to mean 'since the last major surveys were published', i.e., the 1990's) and new results in the last few years.

We assume a basic knowledge of some requisite algebra and comfort with combinatorial manipulation, but all results and terminology specifically connected to difference sets are made explicit, regardless of their level of sophistication. We prove results

which deal with difference sets explicitly or are particularly canonical, and provide sources for proofs in other cases.

Chapter 1

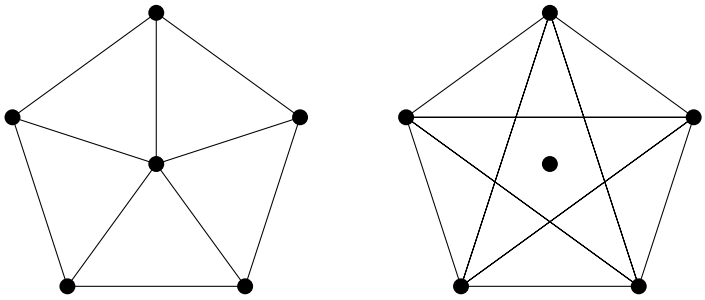
DESIGNS

While our discussion of difference sets (defined later) will mostly deal with a special kind of design, a slightly generalized introduction is helpful.

Definition 1.1. A *t-design* with parameters $t-(v,k,\lambda)$ is an incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, where $\mathcal{P}$ is a point set of size v and $\mathcal{B}$ is a set of k-subsets of $\mathcal{P}$ called *blocks* such that each t-subset of $\mathcal{P}$ is contained in exactly λ blocks.

Naturally, in the above definition, we require $\lambda \geq 1$ and $v > k$ so as to avoid trivialities.

Example 1.2. We will give an example of a $2-(6,3,2)$ design. We present this by distinguishing the two types of blocks on a pentagon with a vertex in the center.



Suppose the points are labeled with the first six natural numbers such that 1 is the uppermost vertex and the numbering continues counterclockwise, with 6 being the center vertex. Then the block set on the left is every triangle having the centroid as a vertex. The block set on the right is every isosceles triangle having just one side on the perimeter of the pentagon. Each such triangle in both figures is a block of size 3, and every pair of points occurs in exactly 2 triangles. The block set of the 2-$(6,3,2)$ design is the union of these two block sets. This is aesthetically satisfying, but obscures the

nature of the design, which could just as easily be presented using the first six natural numbers, as so:

$$[126], [236], [346], [456], [156], [124], [235], [134], [245], [135].$$

From the definition, we can immediately derive several well-known properties of t-designs.

Theorem 1.3. The number of blocks b in a $t-(v,k,\lambda)$ design is given by:

$$b = \lambda \binom{v}{t} \binom{k}{t}^{-1}.$$

Proof. We count pairs (T, B), where $T \subseteq B$ such that T runs through all t-subsets of $\mathcal{P}$ and B runs through all blocks of $\mathcal{B}$, in two ways. There are $\binom{v}{t}$ t-subsets and each is in λ blocks. On the other hand, each block, of which there are b, contains $\binom{k}{t}$ t-subsets. Hence, by double counting, we have $b\binom{k}{t} = \lambda\binom{v}{t}$. $\square$

Theorem 1.4. Let $\mathcal{D}$ be a $t-(v,k,\lambda)$ design and let S be an s-set, with $1 \leq s \leq t$. If λ_s denotes the number of blocks containing S, then we have:

$$\lambda_s = \lambda \binom{v-s}{t-s} \binom{k-s}{t-s}^{-1}.$$

Proof. The proof proceeds by reasoning identical to that of Theorem 1.3. $\square$

There is an important corollary to Theorem 1.4, the proof of which is obvious.

Corollary 1.5. Let λ_1 denote the number of blocks incident with any one point. Then:

$$\lambda_1 = \lambda \binom{v-1}{t-1} \binom{k-1}{t-1}^{-1}.$$

Note that λ_1 is sometimes denoted by r and is called the number of *replications* of a point in $\mathcal{D}$. We can use double counting to prove two more fundamental relations among the parameters of t-designs.

Theorem 1.6. For a $t-(v,k,\lambda)$ design, we have $vr = bk$.

Proof. Consider pairs $(x, B) \in (\mathcal{P}, \mathcal{B})$ such that $x \in B$. There are v points and each must be in r blocks. On the other hand, there are b blocks and each contains k points. By double counting, we have our result. $\square$

In the next chapter, we will study a special case of 2-designs called *symmetric* designs. It is natural to prove a particular relationship for 2-designs here.

Theorem 1.7. In a $2-(v, k, \lambda)$ design, we have $r(k-1) = \lambda(v-1)$.

Proof. Fix any point x in the point set of the design. We count the multiplicity of pairs (x, y) such that $x \neq y$ in two ways. There are $v-1$ points distinct from x, and since $t = 2$, any such pair must be in λ blocks. However, there are r blocks incident with x and there must be $k-1$ other points in such a block that form a pair with x. By double counting, we are done. $\square$

Interestingly, though perhaps not surprisingly, we can easily find an additional design from any initial t-design $\mathcal{D}$.

Definition 1.8. The *complement design* of a t-design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a design $\overline{\mathcal{D}} = (\mathcal{P}, \overline{\mathcal{B}})$, where $\overline{\mathcal{B}} = \{\mathcal{P} \backslash B : B \in \mathcal{B}\}$.

That is, the complement design $\overline{\mathcal{D}}$ has the same point set $\mathcal{P}$ as $\mathcal{D}$, and its block set $\overline{\mathcal{B}}$ is the complement set of blocks in $\mathcal{B}$. In other words, if B is a block in $\mathcal{D}$, then B^c is a block in $\overline{\mathcal{D}}$.

It remains to prove that $\overline{\mathcal{D}}$ is an s-design for some $s \in \mathbb{N}$, and to find the largest such s. Let λ^s denote the number of blocks in $\mathcal{D}$ disjoint from some fixed s-set S. To ensure that S is in at least one block, we will require that $0 \leq s \leq \min\{t, v-k\}$.

Theorem 1.9. Let $\mathcal{D}$ be a $t-(v, k, \lambda)$ design and let S be an s-subset of points such that $0 \leq s \leq \min\{t, v-k\}$. Then the number of blocks of $\mathcal{D}$ disjoint from S is independent of the choice of S and is given by:

$$\lambda^s = \lambda \binom{v-s}{k} \binom{v-t}{k-t}^{-1}.$$

Proof. We first show the independence. For any s-set, by inclusion-exclusion,

we have:

$$\lambda^s = b - s\lambda_1 + \binom{s}{2}\lambda_2 - ....$$

If we define $\lambda_0 = b$, we obtain:

$$\lambda^s = \sum_{i=0}^{s}(-1)^i\binom{s}{i}\lambda_i.$$

To prove the rest of the theorem, it is easier to proceed by double counting than to manipulate the expression obtained above. We count pairs (B, S), where B is a block of $\mathcal{D}$ and S is an s-set disjoint from B. If we first choose B from among the b blocks, there are then $\binom{v-k}{s}$ options for a disjoint s-set. On the other hand, we may first choose the s-set in $\binom{v}{s}$ ways, and then select from the λ^s blocks disjoint from the s-set. By double counting, we have:

$$b\binom{v-k}{s} = \lambda^s\binom{v}{s}.$$

Employing Theorem 1.3 and simplifying gives the desired result. □

Since we have already seen cases satisfying $b > v$ (see Example 1.2), it seems natural to ask whether or not we can have a 2-design for which $b < v$. It turns out that we cannot, provided we eliminate trivial cases by requiring the block sizes to be less than the size of the point set (indeed, this is a perfectly natural requirement). We prove this fact, known as Fisher's Inequality, using the method of van Lint and Wilson [86], but first require some new tools.

Consider a $b \times v$ binary matrix M with the columns labeled by points and the rows labelled by blocks of a (v, k, λ)-design $\mathcal{D}$. The entry m_{ij} is 1 if block i contains point j, and is 0 otherwise. This is the *incidence matrix* of $\mathcal{D}$, and we use it to prove Fisher's Inequality.

Theorem 1.10. Fisher's Inequality: For a non-trivial $2-(v, k, \lambda)$ design with b blocks, we have $b \geq v$.

Proof. Since the design is non-trivial, we have $v > k$, and hence $r > \lambda$ by

Theorem 1.7. Then the incidence matrix M for the design obeys $M^\top M = (r-\lambda)I+\lambda J$. To see this, we first consider the diagonal entries of $M^\top M$, which are just the result of dotting the incidence vectors of each point with themselves, and each point is incident with r blocks. For the non-diagonal entries, note that any two points must occur together in exactly λ blocks. The resulting matrix $M^\top M$ has determinant $rk(r-\lambda)^{v-1}$ (to see the reasoning behind this claim, see Proof A in Appendix B for a proof of a similar claim). Since $r > \lambda$, this determinant is nonzero, so M must have rank v, which implies that $b \geq v$ (recall that M is a $b \times v$ matrix). $\square$

We now turn our attention to a class of designs more specific to our eventual study of difference sets: symmetric designs, which are a special case of 2-designs, and satisfy the equivalence case of Fisher's Inequality (Theorem 1.10)

Definition 1.11. A *symmetric design* with parameters (v, k, λ) is a 2-design for which the additional condition that there are v blocks holds (that is, for which $b = v$).

As Example 1.2 shows, a 2-design need not be symmetric (in that example, the point and block sets have different sizes). It is immediate from Theorem 1.6 that a symmetric design also has the property that $r = k$. It is clear that the incidence matrix of a symmetric design is a square matrix of size v (and we note that it is not necessarily a symmetric matrix). We also have the following property.

Theorem 1.12. The $v \times v$ binary matrix M is the incidence matrix of a symmetric (v, k, λ)-design if and only if $MM^\top = M^\top M = (k - \lambda)I + \lambda J$, where I is the $v \times v$ identity matrix and J is the $v \times v$ matrix in which each entry is 1.

Proof. First, suppose $\mathcal{D}$ is a symmetric (v, k, λ) design. Multiplying row i of M by column j of $M^\top$ for $i \neq j$ is the same as taking the dot product of two distinct columns of M, and since any two points are in exactly λ blocks, the result is λ, so all the non-diagonal entries in $MM^\top$ are λ. If $i = j$, we see that the result will clearly be k. It is easy to apply the same reasoning to $M^\top M$ since any two distinct blocks coincide in exactly λ points, for example.

For the reverse assertion, suppose we have a $v \times v$ binary matrix M such that $MM^\top = M^\top M = (k - \lambda)I + \lambda J$. This immediately gives us the parameters (v, k, λ)

of a symmetric design. □

Note that the incidence matrix of a symmetric design is clearly full rank, and is thus invertible. For symmetric designs, we can replace Theorem 1.7, since for a symmetric design we have $r = k$.

Theorem 1.13. For a symmetric (v, k, λ)-design, we have $\lambda(v-1) = k(k-1)$.

We end this chapter by noting that in view of Definition 1.8, the following theorem is obvious:

Theorem 1.14. The complement design of a symmetric (v, k, λ)-design is a symmetric $(v, v-k, v-2k+\lambda)$-design.

Chapter 2

AUTOMORPHISMS OF DESIGNS

Before formalizing the concept of an automorphism on a structure, we first define and establish some preliminary material. We begin with the definition of a group action.

Definition 2.1. Let G be a group and X a set. We say that G *acts on* X if there exists a function $f : G \times X \to X$ such that the following hold (below, 1 denotes the group identity):

(i) $f(1, x) = x \ \forall x \in X$.

(ii) For all $g, h \in G$, $f(gh, x) = f(g, f(h, x)) \ \forall x \in X$.

Using the above language, we can define some notation. We can say that π_g is a permutation of X if we let $\pi_g(x) := f(g, x)$.

Suppose G is a group acting on a set X. Define $\sim$ to be the equivalence relation such that $x \sim y$ indicates that there exists $g \in G$ such that $y = \pi_g(x)$. For $x \in X$, this equivalence class containing x is called the *orbit* of x under G and is denoted $\text{orb}_G(x)$. The set $\{\text{orb}_G(x) : x \in X\}$ is the set of orbits of G on X. Furthermore, we call the set $\{g \in G : \pi_g(x) = x\}$ the *stabilizer* of x in G. This is the set of all group elements fixing x, and is denoted by $\text{stab}_G(x)$.

Our next theorem is one of the most important regarding group actions. Many shorter and more elegant proofs exist, but here we choose an explicit demonstration, eschewing more technical language in favor of a direct elementary approach.

Theorem 2.2. The Orbit-Stabilizer Theorem: If G is a finite group acting on a set X, then for all $x \in X$, we have $|G| = |\text{stab}_G(x)||\text{orb}_G(x)|$.

Proof. Fix $x \in X$. Suppose we have $\pi_1, \pi_2 \in \text{stab}_G(x)$. Then $\pi_2^{-1} \in \text{stab}_G(x)$, since if it is not, then $\pi_2^{-1}(x) \neq x$, so $\pi_2^{-1}\pi_2(x) \neq x$, and hence $\pi_2^{-1}\pi_2$ is not the identity

operation, a contradiction. Hence, $\pi_1\pi_2^{-1}(x) = x$, so $\pi_1\pi_2^{-1} \in \text{stab}_G(x)$, and by the one-step subgroup test, we have $\text{stab}_G(x) \leq G$. By Lagrange's theorem, then, we have $|G| = |\text{stab}_G(x)|[G : \text{stab}_G(x)]$.

Define a mapping $\phi : \text{orb}_G(x) \to \{\pi\text{stab}_G(x) : \pi \in G\}$ under which $\pi(x) \mapsto \pi\text{stab}_G(x)$. To see that ϕ is well-defined, let $\pi_1(x)$ and $\pi_2(x)$ be elements of $\text{orb}_G(x)$ such that $\pi_1(x) = \pi_2(x)$. Then $\pi_1^{-1}\pi_2(x) = x$, so $\pi_1^{-1}\pi_2 \in \text{stab}_G(x)$, therefore $\pi_2 \in \pi_1\text{stab}_G(x)$, and hence $\pi_2\text{stab}_G(x) = \pi_1\text{stab}_G(x)$.

Reversing this reasoning immediately gives that ϕ is injective, and, surjectivity is also immediate since the preimage of any coset $\pi\text{stab}_G(x)$ under ϕ is clearly $\pi(x)$. So ϕ is a well-defined bijection and hence we have $[G : \text{stab}_G(x)] = |\text{orb}_G(x)|$, and we are done. □

Definition 2.3. We say that the group G acts *transitively* on the set X if there is only one orbit of G on X.

Definition 2.4. We say that the group G acts *regularly* on the set X if G acts transitively and $\text{stab}_G(x) = \{1\}$ for all $x \in X$, where 1 is the identity in G. Note that some authors, such as Isaacs [50], use the term *sharply transitive* in place of *regular*.

Our next theorem is well-known and has many names, the most common of which are Burnside's Lemma and the Cauchy-Frobenius Theorem. We will use elementary language in our proof, but many more sophisticated proofs are known (e.g., see Isaacs [50]).

Theorem 2.5. Burnside's Lemma: The number $\mathcal{O}$ of orbits of G in X is given by:

$$\mathcal{O} = \frac{1}{|G|}\sum_{g\in G} |\{x \in X : \pi_g(x) = x\}|.$$

Proof. We will start by counting pairs $(g, y) \in G \times X$ such that $\pi_g(y) = y$ in two ways. On the one hand, for each $g \in G$, we have exactly $|\{x \in X : \pi_g(x) = x\}|$

such pairs, so:

$$|\{(g, y) \in G \times X : \pi_g(y) = y\}| = \sum_{g \in G} |\{x \in X : \pi_g(x) = x\}|.$$

On the other hand, there clearly must be exactly $\sum_{x \in X} |\text{stab}_G(x)|$ such pairs. It is obvious that if two elements of X are in the same orbit of G, then their respective orbits are the same. By Theorem 2.2, we know that their stabilizers in G have the same size. As such, for any $y \in X$, we have:

$$\sum_{t \in \text{orb}_G(y)} |\text{stab}_G(t)| = |G|.$$

Summing over all orbits, we obtain:

$$\sum_{x \in X} |\text{stab}_G(x)| = \mathcal{O}|G|.$$

By our double counting argument, this must also equal:

$$\sum_{g \in G} |\{x \in X : \pi_g(x) = x\}|,$$

completing the proof. □

Because we will later see that difference sets are intimately connected with symmetric designs, we now focus our study of automorphisms on those objects.

Definition 2.6. Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a symmetric design. An *automorphism of* $\mathcal{D}$ is a permutation of $\mathcal{P}$ that sends blocks to blocks and preserves incidence.

We could switch $\mathcal{P}$ and $\mathcal{B}$ in the definition above, as we shall see later. Note that Definition 2.6 is not meaningfully distinct from the usual definition of an automorphism as a mapping from some object to itself which preserves the structure of the object. Such an automorphism as that defined above also clearly permutes the blocks of $\mathcal{D}$. It is easy to check that the set of all automorphisms of a symmetric design is a group

with function composition as the group operation.

Theorem 2.7. An automorphism α of a symmetric design $\mathcal{D}$ fixes the same number of blocks as points.

Proof. Let A denote the incidence matrix for $\mathcal{D}$. The automorphism α corresponds to matrices P_B and P_p, which permute blocks and points, respectively, and $P_B A P_p = A$. We have $P_B A P_p = A$, and thus $P_B = A P_p^{-1} A^{-1}$. This is valid since permutations must have an inverse, and since incidence matrices for symmetric designs are non-singular. Noting that the inverse of a permutation matrix P is given by $P^\top$, we have $P_B = A P_p^\top A^{-1}$, from which it follows that P_B is similar to $P_p^\top$. Therefore, $\text{trace} P_B = \text{trace} P_p^\top = \text{trace} P_p$. But the trace of a permutation matrix is precisely the number of elements it fixes. Hence, P_B and P_p fix the same number of elements, and we are done. $\square$

Perhaps it is not too surprising, in light of Theorem 2.7, that we can say a little more regarding the behavior of automorphisms on symmetric designs.

Theorem 2.8. A group of automorphisms of a symmetric design has as many orbits on points as on blocks.

Proof. Writing Theorem 2.5 for the orbits of the block and point sets gives the result immediately. $\square$

The following two corollaries are then entirely self-evident:

Corollary 2.9. A group of automorphisms of a symmetric design is transitive on points if and only if it is transitive on blocks.

Corollary 2.10. The automorphism group of a symmetric design acts regularly on points if and only if it acts regularly on blocks.

Chapter 3

DIFFERENCE SETS

Definition 3.1. Let G be a group of size v written multiplicatively. A (v, k, λ)-*difference set* D in G is a k-subset of the elements of G such that for all $g \in G\backslash\{1\}$ there exist exactly λ pairs $(d_1, d_2) \in D \times D$ such that $d_1 d_2^{-1} = g$.

We note that some authors in early literature used the term "perfect difference set" in place of "difference set" [8]. A different but obviously equivalent definition of a difference set is given by de Launey and Flannery [27]: Let $\mathbb{1}_P(x)$ denote the indicator function, which equals 1 if P is true for x and equals 0 otherwise. Let G be a finite group of size v and let 1 be the identity in G. Then D is a (v, k, λ)-difference set in G if and only if:

$$\sum_{(a,b)\in D\times D} \mathbb{1}_{(ab^{-1}=x)}(x) = \begin{cases} k, & \text{if } x = 1, \\ \lambda, & \text{if } x \in G\backslash\{1\}. \end{cases}$$

It is helpful to begin with an example.

Example 3.2. Let $G = (GF(7), +)$ and define D to be the set of nonzero squares in $GF(7)$. Then $D = \{1, 2, 4\}$ and there is exactly one way to write each nonzero element of G as a difference of the elements of D. We list them here, though we will rarely do this going forward: $1 = 2 - 1$, $2 = 4 - 2$, $3 = 4 - 1$, $4 = 1 - 4$, $5 = 2 - 4$, $6 = 1 - 2$. Because $|G| = 7$, $|D| = 3$, and there is only 1 way to write each element of G as a difference (i.e., $\lambda = 1$), D is a $(7, 3, 1)$-difference set in G. In fact, this is an example of a Paley $(4n - 1, 2n - 1, n - 1)$-difference set, where $q = 4n - 1$ is a prime power and $G = (GF(q), +)$.

In the above example, because $\lambda = 1$, D is called *planar* or *simple* (and indeed, planar difference sets can be developed to give projective planes, as we shall see).

Similarly, D is said to inherit properties of G. That is, if G is abelian or cyclic, we say that D is as well. Notice also that in the above example, G is abelian with usual addition as the standard group operation. The ways to write each element of G are literal differences (subtractions) in this case, and it is from this observation that the term "difference set" originates. Indeed, early literature occasionally uses the outdated term "quotient set" when a group is written multiplicatively [8]. We now give a less obvious example.

Example 3.3. In the "twin prime power" difference set, we require q and $q+2$ to be prime powers. Let $G = (GF(q), +) \oplus (GF(q+2), +)$ and define
$D = \{(x, y) \in G : y = 0$ or x, y are both squares or x, y are both non-squares$\}$. Then D is a $\left(q^2 + 2q, \frac{q^2+2q-1}{2}, \frac{q^2+2q-3}{4}\right)$-difference set in G. For $q = 3$, we have:

$$D = \{(1,0), (2,0), (1,1), (1,4), (2,2), (2,3), (0,0)\},$$

and D is a $(15, 7, 3)$-difference set in G.

The following cyclotomic example can be found in Ionin and Shrikhande [48].

Example 3.4. Let $D = \{x^8 : x \in GF(q)\}$. Then D is a difference set in $(GF(q), +)$ if $(q - 49)/8$ is an odd square and $(q - 441)/64$ is an even square.

It is instructive to note that the difference sets in Example 3.3 and Example 3.4 contain the identity element, but that in Example 3.2 does not. We also caution the reader that difference sets as we have defined them are largely unrelated to the difference sets $A-B = \{a-b : a \in A, b \in B\}$ in additive combinatorics and information theory, though some connections exist (e.g., see Wallis [87])

We should establish immediately the so-called 'trivial' difference sets. These occur for $k \in \{0, 1, v-1, v\}$. In the first two cases, it is clear that $\lambda = 0$. In the third, we simply have $D = G\backslash\{1\}$. In the fourth case, $D = G$. These are not interesting situations, though they follow the usual rules and are perfectly valid as difference sets. As Davis and Jedwab [25] note, they are useful as the initial cases of recursive constructions of some families of difference sets. We now prove a lemma for difference

sets that is essentially a special case of Theorem 1.7 (and an exact duplicate of Theorem 1.13). It is insightful to state and prove the claim in a context specific to difference sets.

Lemma 3.5. Let D be a (v, k, λ)-difference set in a group G. Then we have $\lambda(v-1) = k(k-1)$.

Proof. We proceed by double counting. Define the multiset Δ as:

$$\Delta = \left[d_1 d_2^{-1} : d_1, d_2 \in D, d_1 \neq d_2\right].$$

There are $k(k-1)$ differences, so $|\Delta| = k(k-1)$. Because D is a difference set, there are $v-1$ non-identity elements of G that must each occur λ times in Δ, so $|\Delta| = \lambda(v-1)$. By double counting, we have our result. □

Definition 3.6. The *order*, n, of a (v, k, λ)-difference set is given by $n = k - \lambda$. As an example, the difference set D in Example 3.3 has order $n = 4$.

In view of the above definition, we could rephrase Lemma 3.5 to say that for a (v, k, λ)-difference set D in a group G, we have $\lambda v = k^2 - n$.

We will begin to focus now on abelian difference sets, our main objects of study. Non-abelian difference sets are known [72] and are a valuable tool in the study of groups, but are not our area of interest here.

Theorem 3.7. Let p be an odd prime, and define D to be the set of nonzero squares in $\mathbb{Z}_p$. If D is a difference set in the group $G = (\mathbb{Z}_p, +)$, then $p \equiv 3 \pmod 4$.

Proof. Suppose D is a difference set in G. Note that $H = (\mathbb{Z}_p^*, \times)$ is also a group, where $\mathbb{Z}_p^*$ denotes $\mathbb{Z}_p$ without its additive identity. Define $\phi : H \to H$ so that $\phi(x) = x^2$ for all $x \in H$. Then for all x and y in H, we observe that because H is abelian, we have $\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\phi(y)$, so ϕ is a homomorphism. Since H has characteristic p, we know $-1 \neq 1$, and so from $x^2 = 1$ we have $x = \pm 1$. Hence, $|\ker \phi| = 2$, and thus we have $|D| = |H|/|\ker \phi| = (p-1)/2$. So, $k = (p-1)/2$ and by Lemma 3.5 and some algebra, we have $\lambda = (p-3)/4$. But since $\lambda \in \mathbb{N}$, it must be the case that $4|(p-3)$. In other words, $p \equiv 3 \pmod 4$. □

From now on, we will denote the automorphism group of an object G by $\mathrm{Aut}(G)$. A natural theorem involving the automorphism group of a group follows.

Theorem 3.8. Let D be a (v, k, λ)-difference set in an abelian group G. Then the following hold:

(i) For all $g \in G$, Dg is a (v, k, λ)-difference set.

(ii) If $\alpha \in \mathrm{Aut}(G)$, then $\alpha(D) = \{\alpha(d) : d \in D\}$ is a (v, k, λ)-difference set.

Proof. To prove (i), we note that upon multiplication by g, we know $h \in G$ maps to $hg \in G$ and there are now exactly λ ways to write $hg = (hd_1)(hd_2)^{-1}$, but since G is abelian, $(hd_1)(hd_2)^{-1} = d_1 d_2^{-1}$, and we are done. The proof of (ii) is more or less identical. □

The objects in result (i) in Theorem 3.8 invite some new terminology.

Definition 3.9. The difference sets Dg (with $g \in G$) described in Theorem 3.8 are called the *translates* of D with *offset* g. When the group operation is addition, these are written as $D + g$, which is the source of the term. Because we are considering only abelian cases, we shall be rather cavalier about writing translates of a set D by an element g as both Dg and gD, depending on context.

We now demonstrate the existence of an infinite class of difference sets.

Theorem 3.10. The existence of the Paley Difference Sets: Let q be a prime power such that $q \equiv 3 \pmod 4$ and let $G = (GF(q), +)$. Let D be the set of nonzero squares in $GF(q)$. Then D is a $\left(q, \frac{q-1}{2}, \frac{q-3}{4}\right)$-difference set. (This is the converse of Theorem 3.7.)

Proof. Let $GF(q)^*$ be the multiplicative group of nonzero elements of $GF(q)$. It is obvious that $D \leq GF(q)^*$ and that the map $\phi : GF(q)^* \to D$ such that $a \mapsto a^2$ is a homomorphism. Similarly, it is easy to see that $\ker(\phi) = \{-1, 1\}$. Since $GF(q)$ has odd characteristic, $-1 \neq 1$, so $|D| = \frac{q-1}{2}$, and $-1 \notin D$. Hence $a \in D$ if and only if $-a \notin D$.

To see that D is in fact a difference set, define Δ as in the proof of Lemma 3.5 and choose a nonzero element $a \in GF(q)$. If a is a square, then for $s, d_1, d_2 \in D$, we have $a = d_1 - d_2$ if and only if $sa = sd_1 - sd_2$, so all squares appear in the multiset

Δ the same number of times. If a is a non-square, then $-a$ is a square, and we have $a = d_1 - d_2$ if and only if $-a = d_2 - d_1$, so each non-square appears in Δ the same number of times as each square. To find λ, we may use Lemma 3.5, completing the proof. $\square$.

We have hinted many times at an intimate connection between difference sets and symmetric designs. We now make that connection explicit.

Definition 3.11. Given a difference set D in a group G, the *development* of D, denoted dev$D$, is an incidence structure whose points are the elements of G and whose blocks are the translates of D. In other words, the blocks are the set $\mathcal{B} = \{Dg : g \in G\}$.

Assmuss and Key [8] report that "translate design" is a term synonymous with "development". We will show that developments are designs.

Theorem 3.12. Let D be a (v, k, λ)-difference set in a group G. Then dev$D$ is a symmetric (v, k, λ)-design.

Proof. The fact that dev$D$ is a structure on v points and that there are k points in each translate (i.e., in each block) is obvious. Choose $g, h \in G$ such that $g \neq h$. Suppose $a \in (Dg \cap Dh)$. Then, there exist $d_1, d_2 \in D$ such that $a = gd_1 = hd_2$ if and only if $gh^{-1} = d_2 d_1^{-1}$. Since gh^{-1} is not the identity and D is a difference set, there are λ choices of pairs $(d_1, d_2) \in D \times D$ such that $gh^{-1} = d_2 d_1^{-1}$. It follows that if $g \neq h$, then Dg and Dh are different blocks. Hence, there are v blocks, establishing symmetry of the (alleged) design and that any two blocks have λ common points.

To see that $r = k$, note that a fixed $g \in G$ is in the translate Dh if and only if $g = dh$ for some $d \in D$. There are k ways to choose d, so g is in k blocks, and hence $r = k$. It follows that the elements of each pair $(g, h) \in G \times G$ appear together in exactly λ blocks, and we are done. $\square$

We now see the connection between difference sets and symmetric designs, but we can establish even stronger relationships. If D is a difference set in a multiplicative group G, we can define $\pi_g : x \mapsto gx$ for all $g \in G$, so in addition to being the source of the points of dev$D$, the group G is also an automorphism group of dev$D$. We can say more still. Our next theorem is due to Singer [83] and is one of the seminal results in

the study of difference sets. Our proof is that of Moore and Pollatsek [72].

Theorem 3.13. Singer's Theorem: Let G be a finite group of size v. Then G acts regularly on both the points and blocks of a symmetric (v, k, λ)-design if and only if G contains a (v, k, λ)-difference set.

Proof. First, assume G contains a (v, k, λ)-difference set D. By Theorem 3.12, it is immediate that dev$D$ is a symmetric (v, k, λ)-design. We write G multiplicatively, defining $\pi_g(x) = gx$. We have already established that G is an automorphism group of dev$D$. The group G must act regularly on the points of dev$D$, since otherwise there exists $g \in \text{stab}_G(x)\backslash\{1\}$, which means gD is not a translate unless it fixes all of D. But then there exists $h \in G$ such that $h \neq g$ but $hD = gD$, a contradiction. Because G acts regularly on the points of dev$D$, we have by Corollary 2.10 that G acts regularly on the blocks as well.

For the reverse assertion, suppose G acts regularly on a symmetric (v, k, λ)-design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$. Choose a point $p_o \in \mathcal{P}$. Since G acts regularly on $\mathcal{D}$, it acts regularly on $\mathcal{P}$. Hence, for each $p \in \mathcal{P}$, there exists a unique $g \in G$ such that $g(p_o) = p$. We identify g with p, and the identity element in G is identified with p_o. Now choose a block $B_o \in \mathcal{B}$. By identical reasoning, for each $B \in \mathcal{B}$, there exists a unique $g \in G$ such that $g(B_o) = B$. Define $D = \{g \in G : g(p_o) \in B_o\}$. This is the set of elements of G identified with points of B_o. We introduce notation to keep track of things. Let $D = \{d_1, ..., d_k\}$ and let $B_o = \{p_1, ..., p_k\}$. Then for each $i \in [k]$ there exists a unique $j \in [m]$ such that $p_i = d_j(p_o)$. As a result, for a block B there exists a unique $g \in G$ such that $B = g(B_o) = \{g(p_1), ..., g(p_k)\} = \{gd_1(p_o), ..., gd_k(p_o)\}$, so B is identified with the elements of gD. It remains to show that D is, in fact, a (v, k, λ)-difference set in G. Choose $x \in G$ such that x is not the identity. Fixing $g \in G$, we can write $x = h^{-1}g$ for $h \in G$, $h \neq g$. Then, we note that $g(B_o)$ and $h(B_o)$, being different blocks, have λ common points, and there exist $i, j \in [k]$ such that $gd_i(p_o) = hd_j(p_o)$. Since the action of G is regular, we have $gd_i = hd_j$, and so $h^{-1}g = d_j d_i^{-1}$. Hence there are λ ways to write x. This completes the proof. □

We note that some authors, such as Jungnickel [52], express Theorem 3.13 in

slightly less deliberate language by saying that a symmetric (v, k, λ)-design with a regular automorphism group G is *equivalent* to a (v, k, λ)-difference set in G.

While Jungnickel's use of the term 'equivalent' is literal, we should define *equivalence*, as the term applies to difference sets in a slightly non-obvious way.

Definition 3.14. Let D_1 and D_2 be difference sets in a group G. Then D_1 and D_2 are said to be *equivalent* if there exists $g \in G$ and $\sigma \in \mathrm{Aut}(G)$ such that $D_2 = g\sigma(D_1)$.

It is worth noting that g and σ above could be the identity elements of their respective groups. Indeed, any difference set is obviously equivalent to itself. We now provide a more useful example.

Example 3.15. Let $G = \langle a, b : a^4 = b^4 = 1, ab = ba \rangle$. Then G is clearly abelian and has size 16. It is a simple exercise to check that $D_1 = \{1, a, a^2, b, b^3, a^3b^2\}$ is a $(16, 6, 2)$-difference set in G. It is equivalent to the $(16, 6, 2)$-difference set $D_2 = \{ab, ab^2, ab^3, a^2b^2, 1, a^3b^2\}$, since $ab\sigma(D_1) = D_2$ if we define $\sigma \in \mathrm{Aut}(G)$ such that $\sigma(a) = b$ and $\sigma(b) = ab$.

It should be clear that if two difference sets in a group are equivalent, they have the same parameters (v, k, λ). A natural question follows: Does the converse hold? Unfortunately, it does not, as the proof of the next claim will demonstrate. This particularly concise counterexample comes from the work of Kibler [55].

Claim 3.16. Consider the multiplicative abelian group G of size 16 defined by $G = \langle a^8 = b^2 = 1, ab = ba \rangle$. Let $D_1 = \{1, a, a^2, a^4, ab, a^6b\}$ and let $D_2 = \{1, a, a^2, a^5, b, a^6b\}$. We claim that D_1 and D_2 are inequivalent $(16, 6, 2)$-difference sets in G.

Proof. Towards a contradiction, suppose that D_1 and D_2 are in fact equivalent difference sets in G. Then there exist $g \in G$ and $\sigma \in \mathrm{Aut}(G)$ such that $g\sigma(D_1) = D_2$, which implies $\sigma(D_1) = g^{-1}D_2$. Since $1 \in D_1$ and automorphisms map the identity to itself, $1 \in \sigma(D_1)$, so $1 \in g^{-1}D_2$. In other words, $g \in D_2$. To find candidates for $\sigma(D_1)$,

we list the translates of D_2 by the inverses of its elements:

$$\begin{aligned}
1D_2 &= \{1, a, a^2, a^5, b, a^6b\} \\
a^{-1}D_2 &= \{a^7, 1, a, a^4, a^7b, a^5b\} \\
a^{-2}D_2 &= \{a^6, a^7, a, ab, a^6b, a^4b\} \\
a^{-5}D_2 &= \{a^3, a^4, a^5, a, a^3b, ab\} \\
b^{-1}D_2 &= \{b, ab, a^2b, a^5b, a, a^6\} \\
(a^6b)^{-1}D_2 &= \{a^2b, a^3b, a^4b, a^7b, a^2, 1\}
\end{aligned}$$

Now, note that the respective orders of the elements of D_1 are $1, 8, 4, 2, 8, 4$. Since σ must preserve the orders of the elements of D_1, we can immediately eliminate a and a^5 as possible values of g, since the translates of D_2 by their inverses, which must equal $\sigma(D_1)$, each have four elements of order 8 instead of the necessary two. We now have $g \in \{1, a^2, b, a^6b\}$. Consider $a^4 \in D_1$. It has order 2, and so must map to an element of G of order 2 under σ. The only elements of order 2 in G are a^4, b, and a^4b. Let $\sigma(a) = a^ib^j$. But then $\sigma(a^4) = a^{4i}b^{4j} = a^{4i}$ since b has order 2. Therefore, $\sigma(a^4) = a^4$, yet a^4 is an element of $g^{-1}D_2$ only for $g \in \{a, a^5\}$, which we have already established is false. Hence, we have a contradiction, and our claim is proved. □

An immediate corollary follows.

Corollary 3.17. Suppose D_1 and D_2 are equivalent difference sets in a group G. Then devD_1 is isomorphic to devD_2.

We end this chapter with some examples of the many generalizations and modifications to the definition of a difference set that have been studied.

Definition 3.18. Let G be a group of size v and let $H \leq G$ have size m. A k-subset D in G is a (v, k, m, λ)-*relative difference set* with index λ and *forbidden subgroup* H if the following conditions hold:

(i) The multiset $[ab^{-1} : a, b \in D]$ contains each element of $G\backslash H$ exactly λ times

(ii) The multiset $[ab^{-1} : a, b \in D]$ contains each element of $H\backslash\{1\}$ exactly 0 times.

Flannery and de Launey [27] note that a difference set is a relative difference set with $H = \{1\}$ (i.e., with trivial forbidden subgroup), and give several results dealing with relative difference sets. Ionin and Shrikhande [48] give the following characterization of relative difference sets, as well as several examples.

Theorem 3.19. A subset R of a group G is a (v, k, m, λ)-relative difference set in G with forbidden normal subgroup N of size m if and only if $RR^{(-1)} = k - \lambda N + \lambda G$ in the integral group ring $\mathbb{Z}G$ (see Definition 6.1).

There is a useful extension of this concept.

Definition 3.20. Let G and N be groups. A relative difference set in the group $G \times N$ relative to the subgroup $\{1\} \times N$ is called a *splitting relative difference set*.

Often (e.g., in [48]), a (v, k, m, λ)-relative difference set having parameters given by:

$$\left(q^{d+1} - 1, q^d, \frac{q^{d+1} - 1}{q - 1}, q^{d-1}\right)$$

is said to be a *relative difference set with classical parameters*.

Chapter 4

EXISTENCE AND THE BRUCK-RYSER-CHOWLA THEOREM

We have seen that a (v, k, λ)-difference set can be developed into a symmetric (v, k, λ)-design. Hence, many existence proofs for symmetric designs function just as well as existence proofs for difference sets. One of the most important such tools is the Bruck-Ryser-Chowla (BRC) Theorem (see [12], [19]).

Theorem 4.1. The Bruck-Ryser-Chowla Theorem: Suppose $\mathcal{D}$ is a symmetric (v, k, λ)-design.

(i) If v is even, then $n = k - \lambda$ is a square.

(ii) If v is odd, then the equation $x^2 = ny^2 + (-1)^{(v-1)/2}\lambda z^2$ has a non-trivial solution in integers x, y, z.

Proof. The proof of (ii) is somewhat tedious and would be rather distracting to include here. It is included as Appendix A. We prove (i) here. If $\mathcal{D}$ is a symmetric (v, k, λ)-design with v even, then its incidence matrix M is a $v \times v$ matrix obeying $MM^\top = nI + \lambda J$. Since $\det M = \det M^\top$, we then have $\det M = \sqrt{\det(nI + \lambda J)}$. In Appendix B as Proof A, we prove that $\det(nI + \lambda J) = (n + \lambda v)n^{v-1}$. Because M is a $(0, 1)$-matrix, $\det M \in \mathbb{Z}$, so $(n + \lambda v)n^{v-1}$ must be a square. Recall from Lemma 3.5 and Definition 3.6 that $n + \lambda v = k^2$, so n^{v-1} must be a square. But v is even, so $v - 1$ is odd, and hence n must be a square. □

We give two examples of the application of the BRC theorem. Many more can be found in Moore and Pollatsek [72], Chapter 5.

Example 4.2. Let $(v, k, \lambda) = (22, 7, 2)$. These parameters obey the necessary condition that $k(k - 1) = \lambda(v - 1)$ (as will all parameters in future examples of this sort). Since v is even, we know that if a symmetric design, and hence a difference set,

with parameters $(22, 7, 2)$ exists, then $n = k - \lambda = 5$ must be a square. Since it is not, neither a symmetric $(22, 7, 2)$-design nor a $(22, 7, 2)$-difference set exists.

Example 4.3. Consider the parameters $(49, 16, 5)$. For a difference set or symmetric design with these parameters to exist, since 49 is odd, the equation $x^2 = 11y^2 + 5z^2$ must have a non-trivial integer solution. Note that such a solution is given by $(x, y, z) = (4, 1, 1)$, and we can not say whether or not such a design or difference set exists based on the BRC Theorem.

A natural concern, in light of the previous example, is whether or not the converse of the BRC theorem is true. That would be very convenient indeed, but sadly it is not the case, as our next example shows.

Example 4.4. Consider the parameters $(111, 11, 1)$. This would be a projective plane of order 10, which does not exist, as was proved by Lam in 1989 (see [57], [58]). However, the equation $x^2 = 10y^2 - z^2$ has $(x, y, z) = (1, 1, 3)$ as a solution. So the BRC theorem does not rule out the existence of a projective plane of order 10. This example shows that the converse of the BRC theorem does not hold.

Chapter 5

MULTIPLIERS

In addition to the BRC theorem, another important tool for demonstrating existence and nonexistence of difference sets is the concept of a multiplier.

Definition 5.1. Let D be a difference set in a group G. Then an automorphism σ of G is called a *multiplier* for D if σ maps D to aDb for some $a, b \in G$. If $b = 1$ we call σ a *left* multiplier.

For our purposes, G will always be an abelian group, so we have $aDb = abD$, and all multipliers are in fact left multipliers (as well as right multipliers). We will simply use the term 'multipliers' from now on. According to Assmus and Key [8], the term comes from the classical case of a difference set in the cyclic additive group $\mathbb{Z}_p$, where p is a prime. The automorphism group in this case is $\mathbb{Z}_p^\star$, and it acts on $\mathbb{Z}_p$ by multiplication. A specific kind of multiplier will be of particular use to us.

Definition 5.2. Let G be an abelian group of order v, and suppose $t \in \mathbb{Z}$ such that v and t are mutually prime. Define $\phi_t : g \mapsto g^t$. Suppose D is a difference set in G. We call ϕ_t (and, by abuse of terminology, t) a *numerical multiplier* if there is an $h \in G$ such that $\phi_t(D) = hD$.

We should alert the reader that a cursory glance at the literature will show that numerical multipliers are considered specifically so often that the word 'numerical' is sometimes neglected. It is often clear from the context whether authors are speaking about general multipliers or numerical ones specifically, and it is usually the latter. Note that if D is a difference set in a cyclic group G, then any automorphism of G is clearly a numerical multiplier for D, which is the source of this confusion. Additionally, the reader can easily convince themselves that the numerical multipliers for a difference set form a group of their own.

Example 5.3. In the cyclic multiplicative group $G = \langle a \rangle$ of order 13, the set $D = \{a^2, a^3, a^5, a^{11}\}$ is a difference set. The mapping ϕ_3 is a numerical multiplier for D since $D^3 = \{a^6, a^9, a^2, a^7\} = a^4 D$. Note that we denote the set of cubes of elements of D by D^3, although this notation will take on a different meaning when we discuss the integral group ring in Chapter 6.

Example 5.4. Let $G = \langle a, b, c, d : a^2 = b^2 = c^2 = d^2 = 1 \rangle$ be abelian and let $D = \{1, a, b, c, d, abcd\}$. Then D is a difference set in G and $\alpha = (abcd)$ is a multiplier since $\alpha D = D$. But α is not of the form ϕ_t described in Definition 5.2, so α is *not* a numerical multiplier for D.

We need two lemmas to prove our first result dealing with multipliers.

Lemma 5.5. Let S be a k-subset of a symmetric (v, k, λ)-design $\mathcal{D}$. Suppose S meets each block of $\mathcal{D}$ in at least λ points. Then S is itself a block of $\mathcal{D}$.

Proof. Our proof is a greatly expanded version of the somewhat terse proof given by Beth and co-authors [9]. Let the block set of $\mathcal{D}$ be labeled $B_1, ..., B_v$ and define $a_i = |S \cap B_i|$. Counting pairs (x, B_i) with $x \in S$ and $x \in B_i$ obviously gives $\sum_{i=1}^{v} a_i$ on the one hand, and on the other must give k^2, since there are k choices each for x, and each point has k replications. So we have $\sum_{i=1}^{v} a_i = k^2$.

We can count triples (x, y, B_i) as well, with $x \neq y$, $x, y \in S$. On the one hand, our choices for x, y give us $\sum_{i=1}^{v} a_i(a_i - 1)$. On the other hand, since each pair is in λ blocks and each block contains k points, we have $\lambda k(k-1)$. Therefore $\sum_{i=1}^{v} a_i(a_i - 1) = \lambda k(k-1)$.

Now, we use these results to obtain the following two equations, where we note that Lemma 3.5 gives $k - \lambda = k^2 - \lambda v$:

$$\sum_{i=1}^{v} (a_i - \lambda) = k^2 - \lambda v = k - \lambda = n,$$

and

$$\sum_{i=1}^{v}(a_i-\lambda)^2=\sum_{i=1}^{v}a_i(a_i-1)-\sum_{i=1}^{v}(2\lambda-1)a_i+\sum_{i=1}^{v}\lambda^2=k^2-k\lambda-\lambda k^2+\lambda^2 v$$
$$=k^2-k\lambda-\lambda(k-\lambda)=(k-\lambda)^2=n^2.$$

Now, since $a_i-\lambda\geq 0$ for each $i\in[v]$ by hypothesis, the only way for both of the above equations to hold is if there exists $j\in[v]$ such that $a_j-\lambda=n$, with $a_i-\lambda=0$ for all $i\neq j$. In other words, S meets each block in *exactly* λ points except for one, with which it has all points in common. This is the same as saying that S is a block. □

Lemma 5.6. Let M denote the $\mathbb{Z}$-module generated by the columns $e_1,...,e_v$ of the incidence matrix N of a symmetric (v,k,λ)-design $\mathcal{D}$. If $\langle\cdot,\cdot\rangle$ denotes the usual inner product on $\mathbb{Z}^v$, then for each vector $a\in M$, where $a=(a_1,...,a_v)$, we have:

$$\langle a,e_j\rangle\equiv\sum_{i=1}^{v}a_i\ (\text{mod } n)\ \forall j\in[v].$$

Proof. Any two different blocks of $\mathcal{D}$ share λ points, and $n=k-\lambda$, so we have $\lambda\equiv k\ (\text{mod } n)$. Therefore, for $i\neq j$, we have $\langle e_i,e_j\rangle\equiv k\ (\text{mod } n)$. We know that for some constants $c_i, i\in[v]$, we can write $a=\sum_{i=1}^{v}c_ie_i$. Then for all $j\in[v]$, we have:

$$\langle a,e_j\rangle=\langle\sum_{i=1}^{v}c_ie_i,e_j\rangle=\sum_{i=1}^{v}c_i\langle e_i,e_j\rangle\equiv k\sum_{i=1}^{v}c_i=\sum_{i=1}^{v}a_i\ (\text{mod } n).\qquad\square$$

We can now prove some key results about multipliers.

Theorem 5.7. The First Multiplier Theorem: Let D be an abelian (v,k,λ)-difference set in a group G. Suppose p is a prime such that $p\mid n$ but $p\nmid v$. If $p>\lambda$ then p is a multiplier (and clearly, furthermore, a numerical multiplier) for D.

Proof. Our proof is due to Jungnickel [52]. Let p be a prime greater than λ such that $p\mid n$. If G is written multiplicatively, we see that the columns of the incidence matrix N of dev$D$ are just the translates gD, where $g\in G$. Since $p\nmid v$, we see that

$\langle D \rangle$ is a $\mathbb{Z}_p$-module of the columns of N. We denote this module by M. Clearly, $D^p \in M$. By Lemma 5.6, we have $|D^p \cap gD| \equiv \lambda \pmod{p}$. Since $p > \lambda$, we can say $|D^{(p)} \cap gD| \geq \lambda$ for each $g \in G$. Hence, it follows from Lemma 5.5 that D^p is a block, and therefore that p is a (numerical) multiplier for D. $\square$

Multiple sources (e.g. [52], [72]) report that all known difference sets have as multipliers *every* prime divisor of their orders, including those which are less than or equal to λ. It is natural to ask, then, if the hypothesis of Theorem 5.7 can be weakened. That is, can we remove the requirement that $p > \lambda$? Indeed, it has been an open problem for quite some time.

Conjecture 5.8. It is not necessary to assume $p > \lambda$ in the First Multiplier Theorem (Theorem 5.7).

Recall that projective planes with regular automorphism groups are equivalent to the developments of planar ($\lambda = 1$) difference sets. It has been reported (e.g., by van Lint and Wilson [86]) that the conjecture that all projective planes with a regular automorphism group have prime power order has been settled for orders less than 3600 using, in part, the First Multiplier Theorem.

Most remaining results dealing with multipliers are an attempt to make progress towards a proof of Conjecture 5.8. A fairly comprehensive overview of its implications is given by Arasu and Stewart [3], and van Lint and Wilson [86]. We mention the concept of so-called "extraneous" multipliers below.

Definition 5.9. Suppose t is a multiplier of a difference set D having order n. If $t \nmid n$, t is said to be an *extraneous multiplier*.

Jungnickel [52] reports that "small primes are not (usually) extraneous multipliers", and gives the following theorem of Xiang and co-authors [94]. We do not prove it, as the proof requires the use of tools we will discuss in Chapter 6.

Theorem 5.10. Let D be an abelian (v, k, λ)-difference set. Then the following hold:

(i) No extraneous multiplier for D is equal to 2.

(ii) If 3 is an extraneous multiplier for D, then -1 is a multiplier for D.

(iii) If 5 is an extraneous multiplier for D, then $\lambda \neq 1$.

It serves us now to define a new term.

Definition 5.11. The least common multiple of the orders of all elements of an abelian group G is called the *exponent* of G, and is denoted $\exp(G)$.

It is obvious that groups of exponent 2 are abelian, but the converse is not true. There of course exist abelian groups of exponent greater than 2. Hence, the following theorem makes sense. It is due to Menon [69].

Theorem 5.12. The Second Multiplier Theorem: Let D be an abelian (v, k, λ)-difference set in a group G. Let $m > \lambda$ be a divisor of n co-prime to v. Let $\exp(G)$ denote the exponent of G. Let t be a co-prime integer to v satisfying the following: for every prime divisor p of m, there exists a nonnegative integer f that satisfies $t \equiv p^f \pmod{\exp(G)}$. Then t is a (numerical) multiplier for D.

We present the theorem without proof, to avoid a lengthy diversion into number theory. However, several different proofs are available [9], [52], [69], [77]. There is a natural corollary, with a proof due to Jungnickel [52].

Corollay 5.13. Let D be an abelian (v, k, λ)-difference set such that n is a prime power for some prime p. If p is coprime to v, then p is a numerical multiplier for D.

Proof. In the context of Theorem 5.12, suppose $n = m$. It is clear that a difference set D and its complimentary difference set D' have the same multipliers. As such, it must be true that $k \leq v/2$. From Theorem 1.13, we have:

$$\lambda = k(k-1)/(v-1) \leq k((v/2)-1)/(v-1) = (k/2)((v-2)/(v-1)) < k/2,$$

so Theorem 5.12 applies. □

It is worth noting that though it sounds extremely similar, a careful reading will convince the reader that Corollary 5.13 cannot be obtained from Theorem 5.7.

Example 5.14. Recall Example 3.3, and take $q = 5$. Then there exists a $(35, 17, 8)$-difference set in $G = (\mathbb{Z}_5, +) \oplus (\mathbb{Z}_7, +) \simeq (\mathbb{Z}_{35}, +)$. We have $n = 3^2$, so by

Corollary 5.13, 3 should be a numerical multiplier for D, as $\gcd(35, 3) = 1$. It is easy to check that this is indeed the case.

We now give some of the less-obvious properties of multipliers.

Theorem 5.15. Let D be a difference set in a group G, and let α be a multiplier for D. Then α is an automorphism of dev$D$.

Proof. To be an automorphism of dev$D$, α must be a permutation of both the point and block sets of dev$D$. The first is true by definition, since the elements of G are the point set of dev$D$. We will prove the second. Since α is a multiplier, $\alpha(D) = hD$ for some $h \in G$. That is, α gives a translate of D. For all $g \in G$, $\alpha(gD) = \alpha(g)\alpha(D) = \alpha(g)(hD)$, which is clearly a translate of D, and hence is a block in dev$D$. It is now clear that α permutes the block set of dev$D$, and we are done. □

We can use this result to prove an even more striking one.

Theorem 5.16. Let D be a difference set in a group G having left multiplier α. Then α fixes at least one block in dev$D$.

Proof. By Theorem 5.15, α is an automorphism of dev$D$. Therefore, it must map the identity in G to itself. Hence, α fixes at least one point. By Theorem 2.7, it must also fix at least one block. □

We are primarily concerned with *abelian* difference sets, and so the following theorem of McFarland and Mann [64] is of interest, and indeed is much stronger than Theorem 5.16.

Theorem 5.17. Let D be an abelian (v, k, λ)-difference set in a group G. If $\gcd(v, k) = 1$, then there is a $b \in G$ such that bD is fixed by every multiplier for D.

Proof. Of course, $|D| = k$. Define $\phi_k : g \mapsto g^k$. Because $\gcd(v, k) = 1$, it follows that $\phi_k \in \mathrm{Aut}(G)$. Hence, there is a unique element $b \in G$ such that $b^k \prod_{d \in D} d = 1$, where '1' is the identity element in G. Let α be a multiplier for D. Then there exists $c \in G$ such that $\alpha(bD) = cD$. It is sufficient to prove that $b = c$. Consider:

$$1 = \alpha(1) = \alpha\left(b^k \prod_{d \in D} d\right) = \alpha\left(\prod_{g \in bD} g\right) = \prod_{h \in cD} h = \prod_{d \in D} cd = c^k \prod_{d \in D} d,$$

so we can conclude that $c^k = b^k$, and hence that $c = b$. $\square$

It is worth noting that our assumption that G is abelian is absolutely vital in our proof above. Without it, not a single one of our manipulations is valid. The requirement that $\gcd(v, k) = 1$ is also necessary, since otherwise ϕ_k is not necessarily an automorphism. However, without it, we can essentially prove the same theorem, but only for the *numerical* multipliers of a difference set. The theorem and proof are due to McFarland and Rice [67].

Theorem 5.18. If D is a difference set in an abelian group G, then there is a translate of D fixed by all of its numerical multipliers.

Proof. The lengthy proof requires some character theory (Chapter 8), and is therefore included (partially) as Proof B in Appendix B. $\square$

We now show various ways to use the multipliers we have said so much about. We begin with several simple examples, taken from Moore and Pollatsek [72]. First, we note that for a difference set D in a group G with multiplier α such that $\alpha(D) = D$, D must clearly be some union of orbits for α acting on G.

Example 5.19. Let $G = \mathbb{Z}_{15}$. We need to find all the parameters k and λ such that $1 < k < v/2$ and $k(k-1) = \lambda(v-1)$. A little experimentation shows that this is only achieved for $k = 7$ and $\lambda = 3$. So, if a difference set in G exists, it has parameters $(15, 7, 3)$. Given that $n = 2^2$ and 2 is coprime to $v = 15$, Corollary 5.13 assures us that 2 must be a numerical multiplier for such a D. The orbits in G under ϕ_2 are: $(0), (5, 10), (1, 2, 4, 8), (3, 6, 12, 9)$, and $(7, 14, 13, 11)$. Since D must have seven elements, it is clear that D must contain $0, 5, 10$ and one of the other orbits. A little further experimentation shows that $D = \{0, 1, 2, 4, 5, 8, 10\}$ is indeed a $(15, 7, 3)$-difference set in G. In fact, this is the twin-prime power difference set with $q = 3$ from Example 3.3.

Example 5.20. We claim that no $(79, 13, 2)$-difference set exists. First, as 79 is prime, $G = \mathbb{Z}_{79}$. Upon looking for the easiest proofs of our claim, we note that the parameters solve the necessary conditional equation ($k(k-1) = \lambda(v-1)$). Furthermore, upon appealing to the Bruck-Ryser-Chowla Theorem, we note that the

equation $x^2 = 11y^2 - 2z^2$ does indeed have a solution, given by $(x, y, z) = (3, 1, 1)$. Our only hope rests with multipliers. Thankfully, they prove our claim efficiently. Since $11|n$ but $11 \nmid v$ and $11 > \lambda$, The First Multiplier Theorem (Theorem 5.7) says 11 is a numerical multiplier for any $(79, 13, 2)$-difference set. Upon writing the orbits for ϕ_{11} on G, however, we find that there are only three: one of size 1 and two of size 39. We cannot form a set of elements of G of size 13 consisting of a union of orbits, so this difference set does not exist.

Other examples, such as a proof that no difference sets having parameters $(253, 28, 3)$ or $(352, 27, 2)$ can exist, can be found in Beth [9]. The latter is especially interesting, as it quotes a result of Arasu [2] which eliminates all seven possible cases of abelian groups having size 352 simultaneously.

The following extremely strong result gives a bound on the possible number of multipliers of a difference set in a cyclic group, and is due to Xiang and Chen [95]. Their proof is short, but subtle, and requires in-depth knowledge of many other results, so we do not repeat it here.

Theorem 5.21. Let D be a (v, k, λ)-difference set in a cyclic group G, and let M be its multiplier group. Then $|M| \leq k$, unless D is the $(21, 5, 1)$-difference set in $\mathbb{Z}_{21}$, in which case $|M| = 6$.

Other sophisticated results may be obtained when information about the multipliers of a given difference set are known in advance. A good example is Wilbrink's Theorem [91]. A particularly simple proof is given by Jungnickel [52], and we expand upon that proof here.

Theorem 5.22. Wilbrink's Theorem: Let D be an abelian (v, k, λ)-difference set in a group G, and let p be a prime such that $p \nmid v$. Assume that $p \mid n$ but that $p^2 \nmid n$, and further that p is a multiplier of D. Then, in the context of $\mathbb{Z}_p G$ (see Definition 6.1), we have:

$$D^{p-1} + (D^{(-1)})^{p-1} = 1 \pm v^{p-2} G,$$

where the positive case occurs when $p \nmid \lambda$ and the negative case when $p \mid \lambda$.

Proof. Because the proof requires us to work in the integral group ring, covered in the next chapter, we will relegate the proof to Appendix B as Proof C. □

Wilbrink's Theorem can be used to obtain powerful restrictions of the parameters of difference sets. We give an example of Jungnickel [52] below. The proof is almost elementary by considering elements with coefficient 1 in $\mathbb{Z}_2 G$ once the integral group ring is understood.

Theorem 5.23. Let D be a planar abelian difference set of order n, and suppose that n is even. Then either $n = 2$ or n is a multiple of 4.

Two theorems of Mann [63] are discussed at some length in Jungnickel [52], where the first is referred to as "probably the most important nonexistence result for difference sets". We include both here, and refer the reader to Jungnickel for the substantial list of alternate proof sources and the proofs themselves, which can also be found in Beth [9], since they require material we will discuss later. The first of these two theorems is sometimes known as the Mann Test.

Theorem 5.24. The Mann Test: Let D be a (v, k, λ)-difference set in a group G of order v. Let $u \neq 1$ be a natural number such that $u \mid v$, and denote by U a normal subgroup of G having order s and index u. Define $H = G/U$, and suppose H is abelian with exponent $\exp(H)$. Let p be a prime such that $p \nmid \exp(H)$, and suppose there exists a nonnegative integer f and numerical multipler t for G/U such that $tp^f \equiv -1 \pmod{\exp(H)}$. Then the following are true:

(i) p does not divide the square-free part of n. That is, for some $j \in \mathbb{N}$, it is the case that $p^{2j} \mid n$ but $p^{2j+1} \nmid n$.

(ii) $p^j \leq s$.

(iii) If $u > k$, then $p^j \mid k$.

(iv) All of the intersection numbers (see Definition 6.3) of D relative to U are congruent modulo p^j. Let y denote their value modulo p^j for (v) below.

(v) $yu \equiv k \pmod{p^j}$, and the smallest nonnegative y such that this holds satisfies $yu \leq k$.

Example 5.25 Neither the group $\mathbb{Z}_2 \times \mathbb{Z}_{20}$ nor the group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$ contains a $(40, 13, 4)$-difference set. The same arguments apply to both groups, which we will refer to generically as G. Select $U \leq G$ such that U is of order 2 and G/U has exponent 10. Note that for $p = 3$, we have $p \nmid 10$ and $p^2 \equiv -1 \pmod{10}$, but $p^2 > s = 2$, a contradiction with statement (ii) of The Mann Test.

Including Example 5.25, Beth [9] gives no less than 10 distinct examples of uses of The Mann Test, and also gives the following generalization.

Theorem 5.26. Let D be an abelian (v, k, λ)-difference set in a group G, and let w be a natural number such that $w \mid v$. If there exists $h \in \mathbb{N}$ and a multiplier m of D such that $m^h \equiv -1 \pmod{w}$, then either n is a square or has the form a^2b^3 for some $a, b \in \mathbb{N}$, where w is a power of b and b is a prime. In the second case, let $r \neq q$ be a prime such that $r \mid v$. Then every multiplier of D has odd order modulo r, $q \equiv 1 \pmod{4}$, v is odd, and m is a quadratic residue in $\mathbb{F}_q$.

We close this chapter by mentioning that we are not through dealing with multipliers. Difference sets having multiplier -1 are especially important. Because we need a few more tools to discuss them, we will save their study for the end of Chapter 6.

Chapter 6

GROUP CONDITIONS

We have discussed many properties of difference sets that help us to show their existence or nonexistence in various scenarios, but so far we have said little about the groups themselves. To correct that, we begin with what at first appears to be a digression.

Definition 6.1. Let G be a finite group written multiplicatively. Then $\mathbb{Z}G$ denotes the *integral group ring*, which consists of formal sums of the form:

$$\sum_{g \in G} a_g g, \qquad a_g \in \mathbb{Z},\ \forall g \in G.$$

Note that the sums are truly formal, since G is not additive, and even if it was, the addition operation in G would need to be clearly distinguished from that in $\mathbb{Z}G$, since they are operations on different types of objects. We define addition in the integral group ring in the following predictable manner:

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g.$$

We define multiplication similarly:

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} a_h h \right) = \sum_{g \in G} \sum_{h \in G} a_g a_h gh.$$

It should be obvious that $0 = \sum_{g \in G} 0g$, and that $0 = \sum_{g \in G} a_g g$ if and only if $a_g = 0$ for every $g \in G$. Furthermore, it is easy to see that the integral group ring $\mathbb{Z}G$ is commutative if and only if G is abelian. We have followed the development for the

integral group ring used by Moore and Pollatsek [72]. An alternative, yet equivalent, development of the concept of an integral group ring is given by Assmus and Key [8].

We now specify some notation. For $A = \sum_{g \in G} a_g g$, we define $A^{(t)} := \sum_{g \in G} a_g g^t$. Note that any $S \subset G$ can be written in the form $\sum_{g \in G} a_g g$ by letting $a_g = \mathbb{1}_S(g)$, which is the indicator function for S. More often, we will just write $S = \sum_{g \in S} g$, and (by abuse of terminology) consider this to be an element of the corresponding integral group ring.

Theorem 6.2. Let $D \subsetneq G$ be non-empty such that $|D| = k$, and let $|G| = v$. Then D is a (v, k, λ)-difference set in G if and only if $DD^{(-1)} = n + \lambda G$ in $\mathbb{Z}G$.

Proof. This is merely a restatement of Definition 3.1. □

We should note that as Jungnickel and Pott [53] point out, Theorem 6.2 is technically false. If D is a (v, k, λ)-difference set, then indeed $DD^{(-1)} = n + \lambda G$, but the converse actually only holds when $\mathbb{Z}G$ has characteristic zero. This is no problem, though, for this will almost always be the case, and for this treatise, is indeed always true. We will use the above results to prove an important result relating to *intersection numbers*, which we will define momentarily.

Let D be a difference set in a group G. If N is a normal subgroup in G, then the cosets of G modulo N form a partition of G.

Definition 6.3. Let G be a group with a normal subgroup N such that N satisfies $[G : N] = r$, and let $\{g_1, ..., g_r\}$ be a complete set of coset representatives of N in G. Suppose D is a difference set in G. The numbers $|D \cap g_i N|$, denoted n_i, are called the *intersection numbers* for D with respect to N. Sometimes we instead say the intersection numbers are 'for D mod N'.

Example 6.4. By now we are familiar with the twin-prime power difference sets, and they make a nice subject here. Letting $q = 5$, we have $G = \mathbb{Z}_5 \oplus \mathbb{Z}_7$. Then the twin-prime power difference set D in G is a $(35, 17, 8)$-difference set. If $N_1 = \{(a, 0) \mid a \in \mathbb{Z}_5\}$ and $N_2 = \{(0, b) \mid b \in \mathbb{Z}_7\}$, then N_1 and N_2 are both obviously normal subgroups in G. Writing out D and the cosets of N_1 and N_2 shows that for N_1, we have intersection numbers of 5 (once) and 2 (six times). For N_2, we have

intersection numbers of 1 (once) and 4 (four times).

It will not have escaped the observant reader that in both cases in the above example, the intersection numbers sum to k. This fact should now be obvious, but more can be said.

Theorem 6.5. Let D be a (v, k, λ)-difference set in a group G. Let N be a normal subgroup of G with index r and size s. Suppose $\{g_1, ..., g_r\}$ is a complete set of coset representatives for N in G. Then the following are true:

$$\sum_{i=1}^{r} n_i = k \quad \text{and} \quad \sum_{i=1}^{r} (n_i)^2 = n + \lambda s.$$

Proof. The first equation is obviously true. To prove the second, recall Theorem 6.2: in the integeral group ring $\mathbb{Z}G$, we have $DD^{(-1)} = n + \lambda G$. We may also write the right-hand side of this result as $n + \lambda N + \lambda(G/N)$, so that it is clear that the sum of coefficients of the elements of N is $n+\lambda s$. Now, let D_i denote $D \cap g_i N$, and write the left-hand side as $(D_1 + \cdots + D_r)(D_1 + \cdots + D_r)^{-1} = \sum_{i \neq j} D_i D_j^{-1} + \sum_{i=1}^{r} D_i D_i^{(-1)}$. Observe that $D_i D_j^{(-1)}$ has nonzero coefficients only for elements of $g_i g_j^{-1} N$. Such elements are in N if and only if $i = j$, so the sum of all coefficients in N is the same as in $\sum_{i=1}^{r} D_i D_i^{(-1)}$, which is precisely the sum of the squares of the intersection numbers. □

The concept of the integral group ring has many other uses, and it suits us to now prove a useful result relating two such rings.

Theorem 6.6 Let G and H be groups and $\phi : G \to H$ be a homomorphism. Define $\hat{\phi} : \mathbb{Z}G \to \mathbb{Z}H$ by:

$$\hat{\phi}\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \phi(g).$$

Then $\hat{\phi}$ is a ring homomorphism.

Proof. The proof is a straightforward one in which the identity element is preserved since ϕ is a homomorphism, and the nature of the map makes it clear that both addition and multiplication in the group ring sense are respected. □

In light of this result and Theorem 6.2, the following should be not at all surprising, and the proof is intuitive.

Theorem 6.7. Let D be a (v, k, λ)-difference set in a group G and let H be a group as well. We retain the notation of Theorem 6.6. Suppose $\phi : G \to H$ is a surjective homomorphism. If $\hat{D} = \hat{\phi}(D)$ and $s = |\ker \phi|$, then $\hat{D}$ satisfies the following in the integral group ring $\mathbb{Z}H$:

$$\hat{D}\hat{D}^{(-1)} = n + s\lambda H.$$

The integral group ring concept invites a somewhat natural generalization of a difference set, called a difference *list*, first described by Arasu and Ray-Chauduri [1].

Definition 6.8. An element $E \in \mathbb{Z}G$ written as $E = \sum_{g \in G} a_g g$ is a (r, k, s, λ)-*difference list* over G if the following conditions hold:

(i) $s, k \in \mathbb{N}$

(ii) $\lambda \in \mathbb{N} \cup \{0\}$

(iii) $a_g \in \mathbb{N} \cup \{0\},\ \forall g \in G$

(iv) $|H| = r$

(v) $\sum_{h \in H} a_h = k$

(vi) $EE^{(-1)} = k - \lambda + s\lambda H.$

Some observations regarding Definition 6.8 should be made plain. E is usually thought of strictly as a multiset of elements of H. That is, it contains each $h \in H$ exactly a_h times. If $s = 1$ and $a_h \in \{0, 1\}$ for each $h \in H$, then E thought of as a subset of H is an (r, k, λ)-difference set in H.

Difference lists can be obtained in the following manner, though Beth and co-authors assert that it is not exhaustive [9]. A difference list obtained in the way described below is a *homomorphic image* of a difference set. If D is a difference set in a group G and $\phi : G \to H$ is a homomorphism such that $H \simeq G/N$ for some $N \triangleleft G$, then $D \mapsto E$ under $\hat{\phi} : \mathbb{Z}G \to \mathbb{Z}H$ and E is a difference list, which can be seen simply by

writing out the result of applying $\hat{\phi}$ to D written as an element of $\mathbb{Z}G$. Furthermore, suppose that $E = \sum_{h \in H} a_h h$. Then $a_h = |D \cap hN|$.

The BRC Theorem (Theorem 4.1) has an analogue in difference lists, though Beth and co-authors [9] assert that it is actually a stronger statement. Our proof is based on their outline, though their statement of the theorem seems to leave out a necessary condition: namely that it only works on difference lists which are homomorphic images of difference sets. We have included that detail here. The theorem itself is due to Bruck [13] as well as Hall and Ryser [41].

Theorem 6.9. If $E = \sum_{h \in H} a_h h$ is the homomorphic image of a difference set D with $|D| = v$, and is an (r, k, s, λ)-difference list over a group H with r odd, then the equation given by:

$$x^2 = ny^2 + (-1)^{(r-1)/2} r z^2$$

has a non-trivial solution (x, y, z) in integers.

Proof. Suppose $E = \sum_{h \in H} a_h h$ is a homomorphic image of such a difference set, and furthermore that it is an (r, k, s, λ)-difference list over a group H. Let $h_1, ..., h_r$ be a list of the elements of H. Let $M = (m_{ij})$ be the $r \times r$ matrix with entries defined by $m_{ij} = a_{h_i h_j}$, where the coefficients are taken from E. That is, the entry m_{ij} is the coefficient on the element $h_i h_j$ in the difference list E.

By the definition of a difference list, and by Theorem 6.7, we have:

$$\sum_{h \in H} a_{ih} a_{jh} = \begin{cases} n + \lambda s, & \text{if } i = j, \\ \lambda s, & \text{if } i \neq j. \end{cases}$$

Hence, $MM^\top = nI + \lambda s J$, and therefore, by the BRC Theorem, the equation $a^2 = nb^2 + (-1)^{(r-1)/2} s \lambda c^2$ has a non-trivial solution in integers (a, b, c). Recall that $v = rs$ since $|H| = |G/N|$ for some group G such that $N \triangleleft G$ and so we have $k^2 - n =$

$\lambda v = \lambda rs$. Hence, the following holds:

$$(k^2 - n)a^2 = n(k^2 - n)b^2 + (-1)^{(r-1)/2} r(\lambda sc)^2.$$

From the above, we obtain, after some minor arithmetic:

$$(ak - nb)^2 = n(bk + a)^2 + (-1)^{(r-1)/2} r(\lambda sc)^2,$$

and $(x, y, z) = (ak - nb, bk + a, \lambda sc)$ is our solution. $\square$

There is a notion of a numerical multiplier for difference lists as well, and it is a natural extension of that for difference sets.

Definition 6.10. Let S be (r, k, s, λ)-difference list over a group H. Any integer t coprime to r such that $S^{(t)} = hS$ holds in $\mathbb{Z}$ for some $h \in H$ is said to be a *numerical multiplier* for S.

Beth [9] gives two relevant multiplier theorems for difference lists that are natural generalizations of The Second Multiplier Theorem (Theorem 5.12).

Two of the more important results dealing with the existence of difference sets and the properties of their containing groups are Turyn's Exponent Bound (discussed and proved in Chapter 9) and Dillon's so-called 'dihedral trick', which we discuss now. We first introduce a new concept.

Definition 6.11. Let G and $H \subset G$ be abelian groups and suppose there exists $g \in G \backslash H$ with $g^2 = 1$ and $ghg^{-1} = h^{-1}$ for each $h \in H$ such that $G = H + gH$ in the integral group ring $\mathbb{Z}G$. Then G is called a *generalized dihedral extension* of H, and g is referred to as the *extension element*.

Some authors (e.g., see [72]) state that $g \notin H$ instead of that $g \in G \backslash H$ in the above definition, but notice that $g \in G$ is clear, since $G = H + gH$ in $\mathbb{Z}G$ means the elements of G are precisely those of H and those of gH. Since H is a group, it has an

identity, which we denote 1, and gH contains $g1 = g$ so $g \in G$, and we make this plain by writing $g \in G \backslash H$.

Example 6.12. If $H = \langle a, b | a^6 = b^2 = 1, ab = ba \rangle$, then $G = \langle a, b, c | a^6 = b^2 = c^2 = 1, ab = ba, ac = ca^{-1}, bc = cb \rangle$ is a generalized dihedral extension of H with extension element c.

Theorem 6.13. Dillon's Dihedral Trick: Let H be an abelian group and let G be a generalized dihedral extension of H. If G contains a difference set, then any abelian group K such that $[K : H] = 2$ also contains a difference set.

Proof. Suppose $G = H + gH$ in $\mathbb{Z}G$ is a generalized dihedral extension of H and let D be a (v, k, λ)-difference set in G. Then we have subsets X and Y of H such that $D = X + gY$. We know from our proof of Theorem 6.5 that we have $(X + gY)(X + gY)^{(-1)} = n + \lambda G$. Observe that $g = g^{-1}$ from the definition of a generalized dihedral extension and $XY = YX$ since H is abelian. Then, we have $Xg = gX^{(-1)}$ and $(gY)^{(-1)} = Y^{(-1)}g = gY$. Therefore, in $\mathbb{Z}G$, we have:

$$\begin{aligned} n + \lambda G =& (X + gY)(X^{(-1)} + Y^{(-1)}g) = (X + gY)(X^{(-1)} + gY) \\ =& XX^{(-1)} + XgY + gYX^{(-1)} + gYgY \\ =& XX^{(-1)} + XgY + gYX^{(-1)} + Y^{(-1)}g^{-1}gY \\ =& XX^{(-1)} + XgY + gYX^{(-1)} + YY^{(-1)} = XX^{(-1)} + YY^{(-1)} + 2gYX^{(-1)}. \end{aligned}$$

Equating elements of H and gH, we obtain:

$$XX^{(-1)} + YY^{(-1)} = n + \lambda H \quad \text{and} \quad 2YX^{(-1)} = \lambda H = 2XY^{(-1)},$$

where the last equality follows from $H = H^{(-1)}$ since H is abelian.

Now, let K be an abelian group such that $[K : H] = 2$. We have $K = H + kH$

for some $k \in K \backslash H$. Since $k^2 \in H$, we have $k^2 H = H$. Let $C = X + kY$. Then:

$$\begin{aligned} CC^{(-1)} =& (X + kY)(X + kY)^{(-1)} = XX^{(-1)} + YY^{(-1)} + kYX^{(-1)} + k^{-1}XY^{(-1)} \\ =& XX^{(-1)} + YY^{(-1)} + k\left(YX^{(-1)} + k^{-2}XY^{(-1)}\right) = n + \lambda(H + kH) = n + \lambda K, \end{aligned}$$

and we are done. □

As promised at the end of the previous chapter, we now return to multipliers, and specifically discuss difference sets having multiplier -1.

If -1 is a multiplier of a difference set D, then by Theorem 5.17 we can assume it fixes D. In such a case, D is called *reversible* or, more archaically, *symmetric*. Jungnickel [52] notes that all known reversible difference sets obey the condition $v = 4n$ and are referred to as Menon difference sets, with the exception of one. The exception is a $(4000, 775, 250)$-difference set which can be constructed using a method of McFarland described in Chapter 7. It occurs in the group $G = E_{125} \times E_{32}$, where E_n is the elementary abelian group of size n (in this group, take $q = 5$ and $d = 2$ in the context of McFarland's construction, Chapter 7).

Whether further non-Menon reversible difference sets exist is an open problem. Several authors conjecture that the one mentioned above is the only such example, and results due to McFarland and Ma [68] have been further generalized by Ma [62] to show that no other non-Menon reversible difference sets exist for $n \leq 10^8$.

Most results dealing with Menon difference sets are summed up in the following large theorem, collected by Jungnickel [52] from several sources. We will prove only part of it, following a proof of McFarland and Ma [68].

Theorem 6.14. Let D be a reversible (v, k, λ)-difference set in a group G. Then the following hold:

(i) 2 divides both v and λ, and n is a square.

(ii) v and n share all odd prime divisors.

(iii) If p is a prime such that $p \mid n$, then $D^{(p)} \equiv 0 \pmod{p}$.

(iv) It $t \in \mathbb{N}$ is coprime to v, then t is a multiplier for D.

(v) The Sylow subgroups of G are non-cyclic.

(vi) Suppose for some $i \in \mathbb{N}$ that $p^{2i} \mid n$ for a prime p. Then $p^{i+1} | v$, $p^i \mid k$, and $p^i \mid \lambda$. Furthermore, if t is the greatest integer such that $p^t \mid v$, then $k(p^i - 1) \leq \lambda(p^t - 1)$.

Proof. We prove the first three results, and refer the reader to the many sources given by Jungnickel [52] for the others.

Since D is a difference set, its complement in G must also be one, so we can assume $k < v/2$. By Theorem 5.17, we may also assume that $D^{(-1)} = D$, so that in $\mathbb{Z}G$, $D^2 = n + \lambda G$. Towards a contradiction, suppose v is odd. Then the squares of the elements of G are all distinct. Hence there must exist $g, h \in G \backslash \{1\}$ such that the coefficients a_h and a_g equal 0 and 1 respectively in $D^{(2)} = \sum_{d \in D} a_d d^2$. But since $D^2 \equiv D^{(2)} \pmod{2}$, a_g and a_h must be either both even or both odd, a contradiction. Hence, v is even, and by Lemma 3.5, so is λ. By Theorem 4.1, this means n is a square, and we are done with result (i).

Now, we prove (iii). Let p be an odd prime. We have:

$$D^p = D(D^2)^{(p-1)/2} = D(n + \lambda G)^{(p-1)/2},$$

so there exists some u such that $k \mid u$ and the above becomes $uG + (\sqrt{n})^{p-1} D$. Suppose $p \mid n$. Then we have $D^{(p)} \equiv uG \pmod{p}$. We know $p \mid v$, since otherwise all p-th powers of elements of G are distinct, meaning $D^{(p)} \not\equiv uG \pmod{p}$. Since $\lambda k = k^2 - n$, then $p \mid k$ as well, and hence $p \mid \lambda$. Therefore $D^{(p)} \equiv 0 \pmod{p}$. If $p = 2$, then n and k are even, and we immediately have $D^{(2)} \equiv 0 \pmod{2}$. This proves part (iii).

Now, suppose $p \nmid n$ for some odd prime p. We have $(\sqrt{n})^{p-1} \equiv 1 \pmod{p}$ by

Fermat's Little Theorem, so we can write $D^{(p)} - D \equiv uG \pmod{p}$. Then $k < v/2$ implies that $D^{(p)}$ and D both have a coefficient of zero on at least one mutual element of G, so that $u \equiv 0 \pmod{p}$, and hence $D^{(p)} \equiv D \pmod{p}$. Then it must be true that $D^{(p)} = D$. Hence:

$$n + \lambda G = D^2 = \left(D^{(p)}\right)^2 = (D^2)^{(p)} = (n + \lambda G)^{(p)} = n + \lambda G^{(p)}.$$

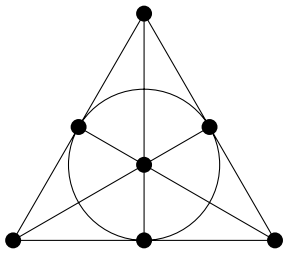
Therefore, $G = G^{(p)}$, and hence $p \nmid v$. As such, all odd prime divisors of v are divisors of n, and we have already shown the reverse. $\square$

Chapter 7

CONSTRUCTIONS AND FAMILIES

In this chapter, we will present several explicit constructions for some of the most well-studied difference sets. We will then give some general families of difference sets as well, and occasionally mention some more narrow constructions. Many more are given, for example, in [48]. We begin with the construction of Singer [83].

Consider $PG(2, q)$, the projective plane of order q constructed from the 3-dimensional vector space $GF(q)^3$ (in other words, the Desarguesian plane of order q), where q is a prime power. An example for $q = 2$, known as the Fano Plane, is given below.



The projective plane denoted by $PG(2, q)$ contains $q^2 + q + 1$ points, with $q + 1$ points on a given line, and any pair of points occurring together on exactly 1 line. Hence, $PG(2, q)$ gives a symmetric $(q^2 + q + 1, q + 1, 1)$-design. Notice that any line of $PG(2, 2)$ gives a $(7, 3, 1)$-difference set. It is important to remember that difference sets are always defined in a group, not a set. We naturally ask, then: What *is* the group in which a line in $PG(2, 2)$ is a difference set? To answer this question thoroughly, we generalize our considerations.

We will work in projective geometries in higher dimensions, such as projective volumes $PG(3, q)$, or even more generally, $PG(m, q)$ for any integer $m \geq 2$. Then we have v points, k points on each hyperplane, and each pair of points will occur together on λ hyperplanes, where:

$$v = \frac{q^{m+1} - 1}{q - 1}, \quad k = \frac{q^m - 1}{q - 1}, \quad \lambda = \frac{q^{m-1} - 1}{q - 1}.$$

There is a natural model of $PG(m, q)$ using the field $GF(q^{m+1})$. Equipped with multiplication, $GF^*(q^{m+1})/GF^*(q)$ is a group of size v, which represents the points of $PG(m, q)$ and hence any hyperplane in $PG(m, q)$ gives a (v, k, λ)-difference set in $GF^*(q^{m+1})/GF^*(q)$. We will prove this explicitly.

Theorem 7.1. Let q be a prime power and let $m \geq 1$ be an integer. Then the symmetric design defined by the points and hyperplanes of $PG(m, q)$ has an automorphism φ of order $(q^{m+1} - 1)/(q - 1)$, and $G = \langle \varphi \rangle$ is a cyclic group acting regularly on points of $PG(m, q)$.

Proof. The group $GF^*(q^{m+1})$ is cyclic and $GF(q^{m+1})$ is an $(m+1)$-dimensional vector space over $GF(q)$. Let $V = GF^*(q^{m+1})/GF^*(q)$. Suppose ω is a generator for $GF(q^{m+1})$. Then $\langle \omega \rangle$ is a cyclic group under multiplication, and $GF^*(q) \leq \langle \omega \rangle$. Furthermore, $|GF^*(q)| = q - 1$. In other words, if we let $v = (q^{m+1} - 1)/(q - 1)$, then $\langle \omega^v \rangle = \{1, \omega^v, \omega^{2v}, ..., \omega^{(q-2)v}\}$, and as such, $GF(q) = \{0, 1, \omega^v, \omega^{2v}, ..., \omega^{(q-2)v}\}$. Treat $GF(q^{m+1})$ as a vector space over $GF(q)$. The elements ω^i and ω^j such that $i, j \in \mathbb{N}$ span the same 1-dimensional subspace of $GF^*(q^{m+1})$ if and only if there exists $\alpha \in GF^*(q)$ such that $\omega^i = \alpha\omega^j$. In this way, we establish a bijection between the 1-dimensional subspaces of $GF(q^{m+1})$ and the cosets $x_i = \omega^i GF^\star(q)$, where we let $x_i = \{\omega^i, \omega^{v+i}, \omega^{2v+i}, ..., \omega^{(q-2)v+i}\}$.

Suppose φ is a map such that $x_i \mapsto x_{i+1}$, where the subscripts are modulo v

(i.e., $x_{v-1} \mapsto x_0$). Then φ is an automorphism of V and $\langle\varphi\rangle$ is obviously regular on V. To show that φ is an automorphism of the symmetric design defined by the points and hyperplanes of $PG(m,q)$, consider the obvious fact that $\varphi(x_i) = \omega x_i$. This clearly maps blocks to blocks (that is, hyperplanes to hyperplanes) and preserves incidence of the points and hyperplanes, and is hence an automorphism of the design. $\square$

By Singer's Theorem (Theorem 3.13), Theorem 7.1 tells us that $G = \langle\varphi\rangle$ as defined in the proof above contains a difference set with parameters:

$$\left(\frac{q^{m+1}-1}{q-1}, \frac{q^m-1}{q-1}, \frac{q^{m-1}-1}{q-1}\right).$$

We can find these difference sets by letting H be an m-dimensional subspace of $GF(q^{m+1})$. Then the set $\{i \in \mathbb{Z}_v : x_i \in H\}$, where we retain the definitions and symbols in the proof of Theorem 7.1, is a Singer difference set.

Put more plainly, Singer's construction gives difference sets in the group of automorphisms generated by φ of the projective geometry $PG(m,q)$.

We now discuss McFarland's construction [65], which allows us to create an enormous variety of diverse difference sets in a straightforward way. A rather different treatment of McFarland's construction is given by Ionin and Shrikhande [48].

Let V be an $(s+1)$-dimensional vector space over $GF(q)$, and further, let $r = (q^{s+1}-1)/(q-1)$. There are r 1-dimensional subspaces and therefore r hyperplanes in V, which we denote $H_1, ..., H_r$. Define $E = (V, +)$ to be the additive group of V and let K be any group of order $r+1$.

Define $G = E \times K$. Furthermore, let $\{k_1, ..., k_r\}$ be a set of elements in K and $\{e_1, ..., e_r\}$ be a multiset in E. That is, the k_i are distinct, but the e_i are not necessarily distinct. Then $H_i + e_i$ is a coset in E with coset representative e_i for all $i \in [r]$, and

hence $(H_i + e_i, k_i)$ is a coset in G with coset representative (e_i, k_i). Define D as follows:

$$D = \bigcup_{i=1}^{r} \{(h + e_i, k_i) : h \in H_i\}.$$

Theorem 7.2. Using the notation established above, D is a (v, k, λ)-difference set in $G = E \times K$ with:

$$v = q^{s+1}\left(\frac{q^{s+1}-1}{q-1} + 1\right), \quad k = q^s\left(\frac{q^{s+1}-1}{q-1}\right), \quad \lambda = q^s\left(\frac{q^s-1}{q-1}\right).$$

Proof. By Theorem 6.2, it is enough to show that $DD^{(-1)} = n + \lambda G$ in $\mathbb{Z}G$. Observe that as a multiset, $\bigcup_{i=1}^{r} H_i$ contains the identity in E exactly r times and contains any other element of E exactly $(q^s - 1)/(q - 1)$ times. Similarly, viewed as a multiset, $H_i + H_i = \{h_1 + h_2 : h_1, h_2 \in H_i\}$ contains any $h \in H_i$ exactly q^s times for any $i \in [r]$. For $x \in E$, we know $H_i + H_j$ contains x exactly q^{s-1} times for any $(i, j) \in [r] \times [r]$ such that $i \neq j$.

To avoid confusing addition in G with addition in $\mathbb{Z}G$, we will write G multiplicatively from here until the completion of the proof. Then $D = \sum_{i=1}^{r} H_i e_i k_i$ and from our observations, we obtain:

$$\sum_{i=1}^{r} H_i = r + \left(\frac{q^s - 1}{q - 1}\right)(E - 1) \quad \text{and} \quad H_i H_j = \begin{cases} q^s H_i, & i = j, \\ q^{s-1} E, & i \neq j. \end{cases}$$

Then, we have the following for $DD^{(-1)}$:

$$\begin{aligned}
DD^{(-1)} =& \left(\sum_{i=1}^{r} H_i e_i k_i\right)\left(\sum_{j=1}^{r} H_j e_j^{-1} k_j^{-1}\right) = \sum_{i=1}^{r} H_i H_i + \sum_{i\neq j} H_i H_j e_i e_j^{-1} k_i k_j^{-1} \\
=& q^s \sum_{i=1}^{r} H_i + q^{s-1} \sum_{i\neq j} (E e_j^{-1} e_i)(k_j^{-1} k_i) \\
=& q^s \left(q^s + \left(\frac{q^s-1}{q-1}\right) E\right) + q^s \left(\frac{q^s-1}{q-1}\right) E(K-1) \\
=& q^{2s} + q^s \left(\frac{q^s-1}{q-1}\right)(E \times K) = n + \lambda G. \qquad \square
\end{aligned}$$

It is worth noting that G inherits nearly all of its properties from the choice of K. As an interesting example, if K is non-abelian, then G will be non-abelian. Also of note is that McFarland difference sets are not cyclic, in general. The already very general construction was further generalized to arbitrary products of groups by Dillon [30]. In his work, Dillon gave the following conjecture, which he proved for some types of groups, and which Davis [23] expanded upon just six years later. The rest of the proof was given by Kraemer [56] shortly after this.

Conjecture 7.3. Dillon's Conjecture: Let $d \in \mathbb{N}$. Then any group of order 2^{2d+2} contains a difference set if it has a normal subgroup isomorphic to $\mathbb{Z}_2^{d+1}$.

A special kind of matrix also gives efficient ways to construct difference sets.

Definition 7.4. An $m \times m$ *Hadamard matrix* H is a square matrix in which all entries are either 1 or -1 such that $HH^\top = mI_m$, where I_m is the $m \times m$ identity matrix. We say that H *is of order* m in this case.

It should be immediately clear from the definition that we have $H^\top H = mI$ as well, where we drop the m designation on the identity matrix, since the size is clear from the context. Indeed, $H^\top$ is a Hadamard matrix if and only if H is.

Example 7.5. A Hadamard matrix H of order 4 is given below, and it can be easily verified that $HH^\top = 4I$.

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Theorem 7.6. Multiplying any row or column of a Hadamard matrix by -1 gives another Hadamard matrix, as does permuting columns and rows.

Proof. We first prove the statement about multiplication by -1. It is clear that for any two rows u and v of an m-order Hadamard matrix, $\langle u, v\rangle = m\delta_{uv}$, where $\langle \cdot, \cdot \rangle$ is the usual dot product and δ_{uv} is 1 when $u = v$ and 0 otherwise. Therefore, multiplication by -1 in the case $u \neq v$ still gives zero, and in the case $u = v$ gives a scaling by $(-1)^2 = 1$ and leaves the result $HH^\top = mI$ unchanged. When columns are permuted, it is obvious that $\langle u, v\rangle = m\delta_{uv}$ still holds. $\square$

Definition 7.7. Two Hadamard matrices are said to be *equivalent* if we can obtain one from the other via only the operations described in Theorem 7.6.

Theorem 7.6 also allows us to assume that any Hadamard matrix has all 1's on both the first row and column. Such a matrix is said to be *normalized*.

Upon attempting to construct a Hadamard matrix of order 3, one would quickly become frustrated and perhaps even conjecture that it is impossible. This is true, and much more can be said.

Theorem 7.8. If H is a Hadamard matrix of order m, then either $m = 1$, $m = 2$, or $m \equiv 0 \pmod 4$.

Proof. Hadamard matrices of orders 1 and 2 are trivial to construct, so suppose H is of order $m > 2$. By Theorem 7.6, we may assume H is normalized. Further, we can arrange the columns of H so that the entries of the second row have some number w of 1's followed by some number x of -1's, followed by some number y of 1's, followed by some number z of negative 1's. The third row, then, by the obvious orthogonality rules for the rows of a Hadamard matrix, must be sortable so that we have w 1's,

followed by x -1's, followed by y -1's, followed by z 1's and such that our statement about the second row still holds. In other words, the first three rows of H are as so for some integers w, x, y, z:

$$\begin{pmatrix} \overbrace{1 \cdots 1}^{w \text{ columns}} & \overbrace{1 \cdots 1}^{x \text{ columns}} & \overbrace{1 \cdots 1}^{y \text{ columns}} & \overbrace{1 \cdots 1}^{z \text{ columns}} \\ 1 \cdots 1 & 1 \cdots 1 & 1 \cdots 1 & 1 \cdots 1 \\ 1 \cdots 1 & 1 \cdots 1 & -1 \cdots -1 & -1 \cdots -1 \\ 1 \cdots 1 & -1 \cdots -1 & -1 \cdots -1 & 1 \cdots 1 \end{pmatrix}$$

Then since $HH^\top = mI$, we derive the following from considering the dot products of rows 1 and 2, 1 and 3, and 2 and 3 respectively:

$$w + x - y - z = 0$$

$$w - x + y - z = 0$$

$$w - x - y + z = 0.$$

We also have, of course, that $w + x + y + z = m$. Solving this system of four equations gives $w = x = y = z = m/4$, and we are done. $\square$

The converse of Theorem 7.8 is still an open problem and an active area of research. With the discovery in 2004 of a Hadamard matrix of order 428 by Kharaghani and Tayfeh-Rezaie [54], the smallest order for which the existence of a Hadamard matrix is open is 668. These gaps are mainly due to constructions such as the following one, which prove the existence of infinite families of Hadamard matrices within the constraint $m \equiv 0 \pmod 4$.

Definition 7.9. Let A and B be Hadamard matrices of respective dimensions $m \times n$ and $k \times l$. The *Kronecker product* $A \otimes B$ of A and B is the $mk \times ln$ matrix consisting of mn blocks, and has the following form, where a_{ij} denotes the ij-th entry as usual of A:

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}.$$

The following theorem is easy to prove by considering the form of a Kronecker product's transpose.

Theorem 7.10. If A and B are Hadamard matrices, then $A \otimes B$ is a Hadamard matrix.

Definition 7.11. A Hadamard matrix is said to be *regular* if it has all row and column sums equal.

Note that, obviously, no normalized Hadamard matrix can be regular, and that regularity is not preserved as part of the operations which give equivalent Hadamard matrices. To see this, consider a regular Hadamard matrix H with not all row and column sums equal to zero and multiply the first row by -1 to get a new Hadamard matrix H'. Then H and H' are equivalent, despite the fact that H is regular and H' is clearly not.

One family of difference sets related to Hadamard matrices is called, perhaps unsurprisingly, the Paley-Hadamard family. An explicit connection between symmetric designs and Hadamard matrices exists.

Theorem 7.12. A Hadamard matrix of order $4n$ exists if and only if a symmetric $(4n-1, 2n-1, n-1)$-design exists.

Proof. Suppose first that H is a Hadamard matrix of order $4n$. We may assume that H is normalized. Delete the first row and column of H to form a new matrix H', and further, replace by 0 all instances of -1 in H' to obtain a matrix H''. Then H'' gives an incidence matrix for some design. Since the rows of H are orthogonal and H is normalized, each row and each column in H'' must have exactly $2n-1$ entries equal to 1, and so the design associated with H'' has equal replication number and block

size.

With appropriate column permutations, we may consider the first two rows of H' to consist of 1's and -1's as such for some natural numbers w, x, y, z: the first row has w 1's, then x 1's, then y -1's, then z -1's. The second row has w 1's, then x -1's, then y 1's, then z -1's. Hence, it follows that:

$$\begin{aligned} w + x + y + z &= 4n - 1 \\ w + x &= 2n - 1 \\ w + y &= 2n - 1, \end{aligned}$$

and since H was a Hadamard matrix, the dot product of the first two rows of H' must give $w - x - y + z = -1$. From this system, we obtain $w = n - 1$ and $x = y = z = n$, so any two different blocks in the design given by H'' must share $n-1$ common points. Therefore, H'' is the incidence matrix of a symmetric $(4n - 1, 2n - 1, n - 1)$-design.

For the reverse assertion, suppose there exists a symmetric $(4n-1, 2n-1, n-1)$-design $\mathcal{D}$ with incidence matrix A. Denote by A' the matrix obtained by replacing all 0 entries of A with -1. Denote by A'' the matrix obtained by attaching a leading row and column of 1's to A'. Let w, x, y, z play the same roles as in the forward proof, and consider any two rows of A'. Since A is the incidence matrix of $\mathcal{D}$, we have the following:

$$\begin{aligned} w + x + y + z &= 4n - 1 \\ w &= n - 1 \\ w + x &= 2n - 1 \\ w + y &= 2n - 1, \end{aligned}$$

from which we obtain (as before) $x = y = z = n$ and $w = n - 1$. Hence, taking the dot product of the two corresponding rows in A'' to those in question above, we have $1 + w - x - y + z = 0$. Taking the dot product of either of these rows with the leading row (which consists entirely of 1's) gives 0. Furthermore, it is obvious that any row of A'' dotted with itself gives $4n$, and so we have $A''(A'')^\top = 4nI$, completing the proof. $\square$

From Theorem 3.7, we know that for $q \equiv 3 \pmod 4$ a prime power, the set of nonzero squares D in $GF(q)$ is a difference set in $(GF(q), +)$. This family of difference sets is called the Paley family, and are related to the Hadamard matrices, since setting $n = (q+1)/4$, D is a $(4n-1, 2n-1, n-1)$-difference set.

A particularly specialized family known as the Hall family is worth noting. Hall details two proofs for his construction, though the prerequisite information and proof that the construction indeed gives a family of difference sets are highly technical and lengthy, and are not repeated here. His first proof can be found in [42] and a slight generalization can be found in [43].

It is worth mentioning that a slightly less-structured type of set can be obtained when $q \equiv 1 \pmod 4$. We must first define the new terms.

Definition 7.13. A subset D of elements of a group G is called a (v, k, λ, μ)-*partial difference set* in G if $|G| = v$, $|D| = k$, and for all $g \in G \backslash \{1\}$, g appears exactly λ times in Δ (as defined in the proof of Lemma 3.5) if $g \in D$ and g appears μ times in Δ if $g \in G \backslash D$.

Note that for $\lambda = \mu$, D is a (v, k, λ)-difference set. When $q \equiv 1 \pmod 4$ is a prime power, and D is the set of all nonzero squares in $GF(q)$, then D is a $(q, (q-1)/2, (q-5)/4, (q-1)/4)$-partial difference set in $(GF(q), +)$.

The sets in the Hadamard family of difference sets satisfy $v = 4n$, where we are using v as usual and still have $n = k - \lambda$. By the Bruck-Ryser-Chowla Theorem, there

exists $m \in \mathbb{N}$ such that $v = 4m^2$. We note here that as Beth and co-authors [9] point out, we are using the contemporary definition of Hadamard difference sets. An older use of this term referred to what are now known as the Paley-Hadamard difference sets, as discussed above. The Hadamard family makes more explicit use of Hadamard matrices, and there is a theorem that connects them directly. We first require a simple lemma.

Lemma 7.14. If a symmetric (v, k, λ)-design exists and $v = 4n$, then there exists $m \in \mathbb{N}$ such that $(v, k, \lambda) = (4m^2, 2m^2 - m, m^2 - m)$.

Proof. We know that $\lambda = k - m^2$ and by Theorem 1.7 and Definition 1.11, we have $k(k-1) = \lambda(v-1)$, which we may rewrite as $k^2 - 4\lambda m^2 = m^2$. Substituting the first equation into the second gives $k^2 - 4m^2k + 4m^4 - m^2 = 0$, so that $k = 2m^2 \pm m$. However, $k = 2m^2 + m$ does not satisfy the necessary condition $k(k-1) = \lambda(v-1)$, so we have $k = 2m^2 - m$ and hence $\lambda = m^2 - m$. $\square$

Theorem 7.12 is similar to our next theorem, but since in the following theorem we assume H is regular, we have a bit more flexibility in the parameters of our design.

Theorem 7.15. A symmetric (v, k, λ)-design with $v = 4n$ exists if and only if a regular Hadamard matrix of order $4n$ exists.

Proof. Suppose H is a regular Hadamard matrix, and let k denote the number of 1's in each row and column (this value is indeed the same for each row and column by regularity of H). Let H' be the matrix found by replacing all -1's in H by 0's. Then H' is an incidence matrix. For any two rows of H, denote by x the number of columns having a 1 in both rows, and denote by y the number of columns having a -1 in both rows. Since each row must have exactly k 1's, we know that there are $k - x$ columns such that the first row has a 1 and the second a -1. Similarly, there must be $4n - k - y$ with the reverse true. Hence, $x + 4n - y - k = k$ and by dotting the two rows, we obtain $x - (k - x) - (4n - k - y) + y = 0$. Therefore, $x = k - n$ and

$y = 3n - k$. We thus have $\lambda = k - n$ and there exists a symmetric (v, k, λ)-design.

Now, assume a symmetric (v, k, λ)-design exists with $v = 4n$. Let A be its incidence matrix and let A' be the matrix obtained by replacing all 0's in A with -1's. Choose two rows of A' and let w be the number of columns sharing a 1, x the number of columns having a 1 in the first row and a -1 in the second, y the number of columns with the reverse, and z the number of columns having a -1 in both columns. We know that:

$$\begin{aligned} w + x + y + z &= v \\ w + x &= k \\ w + y &= k \\ w &= \lambda, \end{aligned}$$

and from Lemma 7.14, there exists $m \in \mathbb{N}$ such that $(v, k, \lambda) = (4m^2, 2m^2 - m, m^2 - m)$. Then it is clear that any two different rows of A' have dot product $w + z - x - y = v - 4k + 4\lambda = 0$. The dot product of any row with itself is $w + z + y - x = w + z - y + x = 4m^2$, so $A'(A')^\top = 4m^2 I$. Finally, it is now obvious that the rows and columns of A' each sum to $w + x - y - z = w - x + y - z = -2m$, and we are done. $\square$

The small Hadamard family described below was constructed by Dillon in his 1974 doctoral thesis [29]. The proof involves manipulations in the relevant integral group ring.

Theorem 7.16. Let G be a group of order $4u^2$ for some even prime power u. Assume G contains u subgroups $H_1, ..., H_u$ such that $|H_i| = 2u$ for each $i \in [u]$ and that $H_i \cap H_j = \{1\}$ for each $i \neq j$, where 1 is the identity element. Then $D = \left(\bigcup_{i=1}^{u} H_i \right) \setminus \{1\}$ is a difference set in G.

Menon [70] has demonstrated extensive connections directly between difference

sets and Hadamard families. Note that his theorem (given below) is immediately generalizable to arbitrary products of groups.

Theorem 7.17. Let j represent either 1 or 2. Suppose D_j is (v_j, k_j, λ_j)-difference set in a group G_j. Let $\overline{D}_j$ represent the $(v_j, v_j - k_j, \overline{\lambda}_j)$ complementary difference set in G_j to D_j. Define $G = G_1 \times G_2$ and $D = (D_1 \times D_2) \cup (\overline{D}_1 \times \overline{D}_2)$. Then D is a difference set in G if and only if $v_j = 4n_j$ for $j \in \{1, 2\}$. Furthermore, we have $|G| = 4n_1n_2$.

Proof. We first need to establish some formalism in the integral group ring $\mathbb{Z}G$. We write all groups multiplicatively, so that the identity element in G is $(1, 1)$. For some $S \in \mathbb{Z}G$, when $S = (X, Y)$ with $X \subseteq G_1$ and $Y \subseteq G_2$, we write:

$$S = (X, Y) = \sum_{x \in X, y \in Y} (x, y) = \left(\sum_{x \in X} x, \sum_{y \in Y} y \right).$$

Suppose $X, Z \subseteq G_1$ and $Y, W \subseteq G_2$. It is easy to check the following in $\mathbb{Z}G$:

$$(X, Y)(Z, W) = (XZ, YW)$$

$$(X + Z, Y) = (X, Y) + (Z, Y)$$

$$(X, Y + W) = (X, Y) + (X, W).$$

Furthermore, for $m \in \mathbb{N}$, we have $(mX, Y) = m(X, Y) = (X, mY)$. Since for $j \in [2]$ we know that D_j is a difference set in G_j, we may write the following:

$$\begin{aligned} D_j D_j^{(-1)} &= n_j + \lambda_j G_j \\ \overline{D}_j \overline{D}_j^{(-1)} &= n_j + \overline{\lambda}_j G_j \\ D_j \overline{D}_j^{(-1)} = \overline{D}_j D_j^{(1)} &= n_j (G_j - 1). \end{aligned}$$

In $\mathbb{Z}G$, we have:

$$D = (D_1, D_2) + (\overline{D}_1, \overline{D}_2)$$

$$D^{(-1)} = (D_1^{(-1)}, D_2^{(-1)}) + (\overline{D}_1^{(-1)}, \overline{D}_2^{(-1)}),$$

so that

$$DD^{(-1)} = \left[(D_1, D_2) + (\overline{D}_1, \overline{D}_2)\right] \left[(D_1^{(-1)}, D_2^{(-1)}) + (\overline{D}_1^{(-1)}, \overline{D}_2^{(-1)})\right]$$

$$= (n_1 + \lambda_1 G_1, n_2 + \lambda_2 G_2) + 2(n_1(G_1 - 1), n_2(G_2 - 1)) + (n_1 + \overline{\lambda}_1 G_1, n_2 + \overline{\lambda}_2 G_2).$$

Note that $(G_1 - 1, G_2 - 1) = (G_1, G_2) - (G_1, 1) - (1, G_2) - (1, 1)$, and using the equations above, we can obtain:

$$DD^{(-1)} = 4n_1 n_2 (1,1) + n_1(\lambda_2 + \overline{\lambda}_2 - 2n_2)(1, G_2) + n_2(\lambda_1 + \overline{\lambda}_1 - 2n_1)(G_1, 1)$$

$$+(2n_1 n_2 + \lambda_1\lambda_2 + \overline{\lambda}_1\overline{\lambda}_2)(G_1, G_2).$$

Now, our proof can truly begin. It is quite short compared to the setup! First, we assume that D_1 and D_2 are Hadamard difference sets in G_1 and G_2, respectively. Then $v_1 = 4n_1$ and $v_2 = 4n_2$, and by Lemma (7.14), for $j \in [2]$ there exists $m_j \in \mathbb{N}$ such that $n_j = m_j^2$, $k_j = 2m_j^2 - m_j$, and $\lambda_j = m_j^2 - m_j$. Additionally, $\overline{\lambda}_j = m_j^2 + m_j$, so that $\overline{\lambda}_j + \lambda_j = 2m_j^2$. Define $m = 2m_1 m_2$ so that $v = 4m^2$ and $k = 2m^2 + m$. Then we have $DD^{(-1)} = n(1,1) + \lambda(G_1, G_2)$, and we are done.

The reverse assertion is even quicker. If D is a difference set in G, then the coefficients for $(G_1, 1)$ and $(1, G_2)$ in our final expression for $DD^{(-1)}$ must be zero. Hence, for $j = 1$ and for $j = 2$, we see that $2n_j = \lambda_j + \overline{\lambda}_j$, from which it follows that $v_j = 4n_j$, and that D_1 and D_2 are Hadamard difference sets. $\square$

The following is readily apparent from Theorem 7.17.

Corollary 7.18. A (v, k, λ)-difference set with $v = 4n$ such that n is a square implies the existence of a (v', k', λ')-difference set such that $v' = 16n$. In other words, $n' = 4n$.

Further relationships among the Hadamard families have been studied by Turyn [85] and McFarland [66], as well as by Davis and Jedwab [24]. McFarland's result is intriguing enough that we state it here, but we defer to McFarland's paper for the lengthy proof.

Theorem 7.19. Let G be an abelian group of order $4p^2$ such that p is an odd prime. If G contains a difference set, then $p = 3$.

Two further families we have not mentioned are the Chen [17] and Spence [84] families. We refer the reader to the sources, but include the parameters below out of interest.

The Chen family of difference sets, for q a prime power and d a nonnegative integer, has parameters (v, k, λ) given by:

$$\left(4q^{2d+2}\left(\frac{q^{2d+2}-1}{q^2-1}\right), q^{2d+1}\left(\frac{2(q^{2d+2}-1)}{q+1}+1\right), q^{2d+1}(q-1)\left(\frac{q^{2d+1}+1}{q+1}\right)\right).$$

The Spence family of difference sets, for d a nonnegative integer, has parameters (v, k, λ) given by:

$$\left(3^{d+1}\left(\frac{3^{d+1}-1}{2}\right), 3^d\left(\frac{3^{d+1}+1}{2}\right), 3^d\left(\frac{3^d+1}{2}\right)\right)$$

Davis and Jedwab [25] give some relationships between base cases of various families of difference sets, including those above.

The last family of difference sets we discuss will be based on hyperovals in $PG(2, q)$. Xiang [97] gives a fairly nice introduction to the necessary preliminaries (for the reasonably experienced reader), which we follow here.

Recall that $PG(2,q)$ denotes the Desarguesian projective plane of order q, where we will assume here that q is an even prime power.

Definition 7.20. A *hyperoval* in $PG(2,q)$ is a set of $q+2$ points, no three of which are colinear.

Definition 7.21. A *quadrangle* in $PG(2,q)$ is a set of four distinct points. The set $\{(1,0,0),(0,1,0),(0,0,1),(1,1,1)\}$ is known as the *fundamental quadrangle*.

Definition 7.22. Two hyperovals are said to be *projectively equivalent* if one can be mapped to the other by some projective linear transformation on $PG(2,q)$.

Projective linear transformations on $PG(2,q)$ are transitive on quadrangles (see Xiang [97]), so we will focus on hyperovals which contain the fundamental quadrangle. We begin with a theorem of Segre. The proof requires some technical knowledge of projective geometry and would amount to a digression from our main goal, but can be found in Hirschfeld [45].

Theorem 7.23. Let $q > 2$ be an even prime power. Then any hyperoval in $PG(2,q)$ containing the fundamental quadrangle can be written as:

$$D(f) = \{(1,t,f(t) : t \in \mathbb{F}_q)\} \cup \{(0,1,0),(0,0,1)\},$$

where f is a permutation polynimial over $\mathbb{F}_q$ of degree at most $q-2$. Furthermore, f is such that $f(0)=0$, $f(1)=1$, and forall $s \in \mathbb{F}_q$, we have:

$$f_s(x) = \begin{cases} \dfrac{f(x+s)+f(s)}{x} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

Definition 7.24. A hyperoval which is projectively equivalent to $D(t^h)$, where $h > 2$ is a natural number is said to be a *monomial hyperoval*.

Xiang and co-authors [98] demonstrated a very direct connection between hyperovals and difference sets, which we sketch below, via a theorem of Maschietti. We give their first lemma without proof for the same reason that we neglected to give the proof of Theorem 7.23, but we give the proof of the main result, which they simplified.

Lemma 7.25. Let q be a power of 2 and let $D(x^h)$ be a $(q+2)$-set in $PG(2,q)$. Then $D(x^h)$ is a hyperoval if and only if both h and $q-1$ are coprime and the map $\tau : x \to x^h$ is precisely a two-to-one map $\mathbb{F}_q \to \mathbb{F}_q$.

Theorem 7.26. Let q be a power of 2, and define τ as in Lemma 7.25. If $D(x^h)$ is a hyperoval in $PG(2,q)$, then the image of τ with $\{0\}$ removed is a difference set in $\mathbb{F}_q^*$ with parameters $(q-1,(q/2)-1,(q/4)-1)$.

Proof. The proofs requires the use of character theory, which we cover in Chapter 8. As such, this proof will be given in Appendix B as Proof D. □

Xiang and co-authors [98] also show that projectively equivalent monomial hyperovals in $PG(2,q)$, with $q > 2$ an even prime power, give rise to equivalent difference sets according to the construction of Theorem 7.26. Their paper contains many more results on difference sets, especially as they relate to number theory, a subject we will discuss in Chapter 9.

Chapter 8

CHARACTERS OF GROUPS

Almost every major tool in abstract algebra is useful in the study, discovery, and construction of difference sets. Character Theory is no different.

Definition 8.1. Let G be a finite abelian group and let $\chi : G \to \mathbb{C}^*$ be a group homomorphism. Then χ is a *character* of G. The *trivial character* is the character such that $g \mapsto 1$ for every $g \in G$. Some authors (e.g., [33]) use the term *principal character* instead of *trivial character*.

There are other definitions of characters (see [72], for example), but ours is highly efficient for our purposes.

Theorem 8.2 Let G be a finite multiplicative group of order n, and let χ be a character of G. Then for all $g \in G$, $\chi(g)$ is an n-th root of unity.

Proof. Since χ is a homomorphism and G has order n, $\chi(g)^n = \chi(g^n) = \chi(1)$, and $\chi(1) = 1$ for every $g \in G$. $\square$

It follows that $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$ for $g \in G$, where $\overline{z}$ denotes the conjugate of z.

Theorem 8.3. Let G be a finite abelian group and let χ_o denote the trivial character. Then:

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{if} \chi = \chi_o, \\ 0, & \text{if} \chi \neq \chi_o. \end{cases}$$

Proof. If χ is the trivial character, then $\chi(g) = 1$ for all $g \in G$ and we are done. Otherwise, there must exist some $g' \in G$ such that $\chi(g') \neq 1$, and we have:

$$\sum_{g \in G} \chi(g) = \sum_{g'g \in G} \chi(g'g) = \sum_{g'g \in G} \chi(g')\chi(g) = \chi(g') \sum_{g'g \in G} \chi(g),$$

and since g' is fixed, our index includes all elements of G, and we can write:

$$\sum_{g \in G} \chi(g) = \chi(g') \sum_{g \in G} \chi(g),$$

and since $\chi(g') \neq 1$, we must have $\sum_{g \in G} \chi(g) = 0$. $\square$

Corollary 8.4. Let χ_1 an χ_2 be complex characters of a finite group G. Then

$$\sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} = \begin{cases} n & \text{if } \chi_1 = \chi_2, \\ 0 & \text{if } \chi_1 \neq \chi_2. \end{cases}$$

Proof. If $\chi_1 = \chi_2$, then for all $g \in G$, $\chi_1(g)\overline{\chi_2(g)} = \chi_1(gg^{-1}) = 1$. Otherwise, $\chi_1\overline{\chi_2}$ is not a principal character, and the sum is zero by Theorem 8.3. $\square$

Theorem 8.5. Let G be a finite abelian group, and let $G^\star$ be the set of all complex characters of G. Let 1 denote the identity in G. Then:

$$\sum_{\chi \in G^\star} \chi(g) = \begin{cases} |G|, & \text{if } g = 1, \\ 0, & \text{if } g \neq 1. \end{cases}$$

Proof. If $g = 1$, the result is obvious. If $g \neq 1$, let $\chi' \in G^\star$ be such that $\chi'(g) \neq 1$. Then:

$$\chi'(g) \sum_{\chi \in G^\star} \chi(g) = \sum_{\chi \in G^\star} \chi'(g)\chi(g).$$

It is easy to check that $G^\star$ is a group under multiplication. Therefore, by a

reindexing argument similar to that in the proof of Theorem 8.3, we can say:

$$\sum_{\chi \in G^\star} \chi'(g)\chi(g) = \sum_{\chi \in G^\star} \chi(g),$$

and since $\chi'(g) \neq 1$, we are done. $\square$

Definition 8.6. Let G be a finite abelian group and let χ be a character of G. Suppose $\sum_{g \in G} a_g g$ is an element of $\mathbb{C}G$. We define $\chi^\star$ to be the map from $\mathbb{C}G$ to $\mathbb{C}$ such that:

$$\chi^\star \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g \chi(g).$$

We note that some texts (e.g., [52]) abuse the notation slightly and make little or no distinction between the maps we formally refer to as χ and $\chi^\star$, though their meaning when discussion characters is typically quite clear from the context. The above definition makes it easy to verify the inversion formula for the coefficients a_g. If G is a finite abelian group, and if $A = \sum_{g \in G} a_g g$ in $\mathbb{C}G$, then:

$$a_h = \frac{1}{|G|} \sum_{\chi \in G^\star} \chi^\star(A)\chi(h^{-1}),\ \forall h \in G,$$

where $G^\star$ is the set of all characters of G. Indeed, we simply write:

$$\sum_{\chi \in G^\star} \chi^\star(A)\chi(h^{-1}) = \sum_{\chi \in G^\star} \sum_{g \in G} a_g \chi(g)\chi(h^{-1}) = \sum_{g \in G} \sum_{\chi \in G^\star} a_g \chi(gh^{-1}) = |G| a_h.$$

To prove our next Theorem, we require a Lemma of Ionin and Shrikhande [48].

Lemma 8.7. Denote by $\mathbb{Z}G^\star$ the set of characters on $\mathbb{Z}G$. Let G be a finite abelian group, and let $\alpha, \beta \in \mathbb{Z}G$. If $\chi^\star(\alpha) = \chi^\star(\beta)$ for every $\chi^\star \in \mathbb{Z}G^\star$, then $\alpha = \beta$.

Proof. Let $\alpha = \sum_{g \in G} a_g g$ and $\beta = \sum_{g \in G} b_g g$. Suppose $\chi^\star(\alpha) = \chi^\star(\beta)$ for every

$\chi^\star \in \mathbb{Z}G^\star$. By Theorem 8.5, we have the following for all $h \in G$:

$$\sum_{\chi^\star \in \mathbb{Z}G^\star} \chi^\star(\alpha h^{-1}) = |G|a_h \quad \text{and} \quad \sum_{\chi^\star \in \mathbb{Z}G^\star} \chi^\star(\beta h^{-1}) = |G|b_h.$$

Now, $\chi^\star(\alpha h^{-1} - \beta h^{-1}) = 0$ for every $\chi^\star \in \mathbb{Z}G^\star$, so we have $a_h = b_h$ for all $h \in G$, and hence $\alpha = \beta$. $\square$

Theorem 8.8. Let G be an abelian group of size v. Let $G^\star$ be the set of all characters of G, and let χ_0 denote the trivial character. Let $D \subseteq G$ have size k, and suppose $\lambda \in \mathbb{N}$, where $\lambda = \frac{k(k-1)}{v-1}$. Then D is (v, k, λ)-difference set in G if and only if:

$$\chi^\star(D)\overline{\chi^\star(D)} = \begin{cases} n, & \text{if } \chi = \chi_0, \\ k^2, & \text{if } \chi = \chi_0, \end{cases}$$

for all $\chi \in G^\star$.

Proof. If D is a (v, k, λ)-difference set in G, the claim is obvious from Theorem 6.2 and the fact that $\chi_0^\star(D) = k$. For the converse, suppose $D \subseteq G$ is a set such that:

$$\chi^\star(D)\overline{\chi^\star(D)} = \begin{cases} n, & \text{if } \chi = \chi_0, \\ k^2, & \text{if } \chi = \chi_0, \end{cases}$$

holds. Then, for non-trivial χ, we can write $\chi^\star(D)\overline{\chi^\star(D)} = \chi^\star(n + \lambda(G))$ by Theorem 8.3. Additionally, $|D| = k$ by the fact that $\chi_0^\star(D) = k$. Let $D = \{d_1, ..., d_k\}$. Then $DD^{(-1)} = (d_1 + \cdots + d_k)(d_1^{-1} + \cdots + d_k^{-1}) = k + \sum_{g \in G \setminus \{1\}} a_g g$, where $a_g \in \mathbb{Z}$ for all $g \in G$. Therefore, by Theorem 8.5, we have:

$$\sum_{\chi^\star \in \mathbb{Z}G^\star} \chi^\star(D)\overline{\chi^\star(D)} = \sum_{\chi^\star \in \mathbb{Z}G^\star} \chi^\star(DD^{(-1)}) = |G|k.$$

However, it is also true that:

$$\sum_{\chi^\star \in \mathbb{Z}G^\star} (k - \lambda + \lambda G) = \sum_{\chi^\star \in \mathbb{Z}G^\star} (k - \lambda(G-1)) = |G|k.$$

From the above, it is clear that $\chi^\star(DD^{(-1)}) = \chi^\star(n + \lambda G)$ for all non-trivial $\chi^\star \in \mathbb{Z}G^\star$. Therefore, it follows that we must have $\chi_0^\star(DD^{(-1)}) = \chi_0^\star(n + \lambda G)$ as well. By Lemma 8.7, then, we have $DD^{(-1)} = n + \lambda G$. By Theorem 6.2, if we let $|G| = v$, then D is a (v, k, λ)-difference set in G, and we are done. $\square$

Chapter 9

NUMBER THEORY AND TURYN'S EXPONENT BOUND

When we discussed multipliers and the First and Second Multiplier Theorems (Theorems 5.7 and 5.12), it was clear that we could make little progress for situations involving difference sets for which $n \mid v$. In Chapter 7, we met the Hadamard family of difference sets, for which such a hurdle is present. Thankfully, Turyn's Exponent Bound, which we mentioned briefly in Chapter 7, will provide us with a (partial) way around the hurdle. Some preliminary material is required.

We work in $\mathbb{C}$, and say that η is a *primitive m-th root of unity* when $\eta = e^{2\pi li/m}$ for m and l coprime.

Definition 9.1. Let η be a primitive m-th root of unity. Let $\mathbb{Q}(\eta)$ denote the subfield of $\mathbb{C}$ obtained by adjoining η to $\mathbb{Q}$. We call $\mathbb{Q}(\eta)$ the *m-th cyclotomic field*.

Note that if we define:

$$\mathbb{Z}[\eta] := \left\{ \sum_{j=0}^{\phi(m)-1} a_j \eta^j : a_j \in \mathbb{Z} \right\},$$

where ϕ is the totient function, then $\mathbb{Z}[\eta]$ is a subring of $\mathbb{Q}(\eta)$. We refer to it as the set of *cyclotomic integers* in $\mathbb{Q}(\eta)$.

Theorem 9.2. Let η be a primitive p^q-th root of unity, where p is a prime. Suppose $\sum_{j=0}^{p^q-1} a_j \eta^j = 0$, where $a_j \in \mathbb{Q}$ for each $j \in [p^q - 1]$. If $j \equiv l \pmod{p^{q-1}}$ for some $j, l \in [p^q - 1]$, then $a_j = a_l$.

Since this result will only be a tool in our study of difference sets, we forgo the proof here, and instead refer the reader to Iiams' proof [47]. We will do this with most of the proofs relating strictly to number theory in this chapter.

Theorem 9.3. Let η be a primitive m-th root of unity. If $r \in \mathbb{Z}[\eta]$ and $r\overline{r} = 1$, then r is a root of unity.

Theorem 9.3 is given as Corollary 15.9 in [9], where a proof sketch is also given.

Definition 9.4. An ideal A in a commutative ring R is said to be a *prime ideal* if $a, b \in R$ and $ab \in A$ together imply that either $a \in A$ or $b \in A$. We define the product of ideals A and B as:

$$AB = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in A, b_i \in B, n \in \mathbb{N} \right\}.$$

Theorem 9.5. Let η be a primitive m-th root of unity and let $R = \mathbb{Z}[\eta]$. Then every ideal in R can be written as a product of prime ideals.

The proof of Theorem 9.5 is given by Ireland and Rosen on page 180 of [49].

Theorem 9.6. Let η be a primitive m-th root of unity and let $R = \mathbb{Z}[\eta]$. Suppose p is a prime. Then the following hold:

(i) Suppose $p \nmid m$. If f is the smallest integer such that $p^f \equiv 1 \pmod{m}$, then there exist distinct prime ideals $P_i, i \in [g]$, for $g = \phi(m)/f$, such that $pR = P_1 \cdots P_g$.

(ii) If $m = p$, then $(1 - \eta)R$ is a prime ideal in R and $pR = ((1 - \eta)R)^{p-1}$.

(iii) Suppose P is a factor of pR. Then for odd p, P has multiplicity greater than 1 if and only if $p \mid m$. For $p = 2$, P has multiplicity greater than 1 if and only if $4 \mid m$.

The proof of Theorem 9.6 is given on page 196 of [49].

Definition 9.7. Let p be a prime. For $m \in \mathbb{N}$, let $m = p^a m'$, where a is the highest power of p dividing m, and as such $p \nmid m'$. If there exists an integer $j > 0$ such

that $p^j \equiv -1 \pmod{m'}$, then we say p is *self-conjugate modulo* m.

Theorem 9.8. Let η be a primitive m-th root of unity and let $R = \mathbb{Z}[\eta]$. Let p be a prime that is self-conjugate modulo m, and let P be a prime ideal factor of pR. Then $P = \overline{P}$.

The proof of Theorem 9.8 is given by Beth and co-authors on page 438 of [9].

Existence results using algebraic number theory are typically somewhat intricate.

It is almost time to prove Turyn's exponent bound. We note that some authors (e.g. [72]) distinguish two versions of Turyn's exponent bound. The first is really a special case of the second, and we will treat the second, and more general, version here. Before that, we require two lemmas. Our first is traditionally attributed to Ma [61], though Moore and Pollatsek [72] note that a similar result was obtained by Lander [59] prior to Ma's result, using different methods. We defer to Ma for the highly technical proof, and state his result here.

Recall that for a prime p, a Sylow p-subgroup P of a group G is a subgroup of the largest size possible in G such that all elements of P have order p. Recall also that any Sylow p-subgroup of an abelian group is unique. We refer the reader to Isaacs [50] for a review of Sylow's Theorems and their consequences.

Lemma 9.9. Ma's Lemma: Let G be a finite abelian group with a cyclic Sylow p-subgroup P, and let Q be the unique subgroup of P having order p. Suppose $Y \in \mathbb{Z}G$ such that $\chi^\star(Y) \equiv 0 \pmod{p^a}$ for all non-trivial characters χ of G, where a is some natural number. Then there exist $X_1, X_2 \in \mathbb{Z}G$ such that $Y = p^a X_1 + Q X_2$. Additionally, if the coefficients of Y in $\mathbb{Z}G$ are nonnegative, then X_1 and X_2 can be chosen to have nonnegative coefficients in $\mathbb{Z}G$ as well.

Lemma 9.10. Let η be a primitive m-th root of unity and let $R = \mathbb{Z}[\eta]$. Let $p \in \mathbb{Z}$ be a self-conjugate prime modulo m, and suppose there exists $z \in R$ such that

$z\overline{z} = n$ for some $n \in \mathbb{N}$. Suppose further that there exists $a \in \mathbb{N}$ such that $p^{2a} \mid n$. Then $z \equiv 0 \pmod{p^a}$.

Proof. Let $Z_1, ..., Z_s$ represent the factorization of zR into prime ideals, which we assume there to be s of, without loss of generality. Let $P_1, ..., P_t$ be similarly defined for pR. Because p is self-conjugate modulo m, $P_i = \overline{P}_i$ for each $i \in [t]$. Since $p^{2a} \mid n$, there must exist $q \in \mathbb{Z}$ such that $p^{2a}q = n$. As such, we can write $(zR)(\overline{z}R) = (pR)^{2a}(qR)$, and hence:

$$\begin{aligned}(Z_1 \cdots Z_s)(\overline{Z}_1 \cdots \overline{Z}_s) =& (P_1 \cdots P_t)^a(\overline{P}_1 \cdots \overline{P}_t)^a(qR) \\ =& (P_1 \cdots P_t)^{2a}(qR).\end{aligned}$$

Since each P_j is self-conjugate, it occurs equally often among the prime ideals of zR and among their conjugates. Therefore, each P_i^a occurs among the Z_j, for $i \in [t]$ and $j \in [s]$. Hence, there exists some ideal A such that $zR = (p^aR)A$, and thus that there exists $r \in R$ such that $z = p^ar$, completing the proof. □

In our next proof, we will use the Structure Theorem for finitely-generated abelian groups: specifically that any finite abelian group is isomorphic to a direct sum of cyclic groups having prime power order. With these basic facts in hand, we will prove Turyn's exponent bound. We will use the proof of Moore and Pollatsek [72], with additional details and expansions.

Theorem 9.11. Turyn's Exponent Bound: Let G be an abelian group which contains a (v, k, λ)-difference set D. Let p be a prime such that $p \mid v$ and let P denote the Sylow p-subgroup of G. Suppose there exists $a \in \mathbb{N}$ such that $p^{2a} \mid n$, and let $U \leq G$ such that $U \cap P = \{1\}$, where 1 is the identity in G. If p is self-conjugate

modulo the exponent of G/U, then:

$$\exp(P) \leq \frac{|U||P|}{p^a},$$

where $\exp(P)$ is the exponent of P.

Proof. By the Structure Theorem, P can be decomposed into a sum of cyclic subgroups, of which there is some natural number t. Thus, we can write:

$$P \simeq \bigoplus_{i=1}^{t} C_i,$$

where for each $i \in [t]$, C_i is a cyclic group of order p and size p^{a_i} for some $a_i \in \mathbb{N}$. Reordering the C_i if necessary, we can assume without loss of generality that if $i \geq j$, then $a_i \geq a_j$. There must exist $W \leq P$ such that:

$$W \simeq \bigoplus_{i=2}^{t} C_i.$$

Then $P/W \simeq C_1$ and P/W has order p^{a_1}. Additionally, P/W must be cyclic, so $|W| = |P|/exp(P)$, since $exp(P)$ is also the exponent of C_1 by construction. Chose $U \leq G$ such that $U \cap G = \{1\}$. We are assured that such a U exists since we could select U to be the group containing just the identity element. Let $K = \langle U, W \rangle$. That is, K is the group generated by the generators of U and of W. Then $|K| = |U||W|$. Let $H = G/K$. As such, H has a cyclic Sylow p-subgroup of order p^{a_1}.

Define $\phi : G \to H$ naturally (that is, ϕ sends elements to their relevant cosets), and consider $\mathbb{Z}H$. Let $E = \hat{\phi}(D)$. By Theorem 6.2, we have $EE^{(-1)} = n + \lambda|K|H$ (recall that D is a difference set in G, not in H). Now, let χ be a non-trivial character of H. Define $z := \chi^\star(E)$ and let $\exp(H)$ denote the exponent of H. Let η be the primitive $\exp(H)$-th root of unity. It must be true that $z \in \mathbb{Z}[\eta]$, and we can write

$z\overline{z} = n$ by Theorem 9.3.

The exponent of G/U can be written wp^b for some positive integer $b < a$ and w coprime to p. By hypothesis, p is self-conjugate modulo the exponent of G/U. Now, consider the exponent of G/W. Since $K = \langle U, W \rangle$, we note that $U \cap P = \{1\}$, and also that $W \subset P$, so elements of G/K have the same orders as those of G/U. As such, we must be able to write the exponent of $G/$ as wp^c, where $b + c = a$. Therefore, p is also self-conjugate modulo the exponent of G/K. Therefore, by Lemma 9.10, we have $z \equiv 0 \pmod{p^a}$.

For every non-trivial character χ of H, have $\chi^\star(E) \equiv 0 \pmod{p^a}$. By Lemma 9.9, we can therefore find X_1 and X_2 in $\mathbb{Z}H$ such that $E = p^a X_1 + QX_2$, where Q is the subgroup of order p in the Sylow p-subgroup of H. Because E has nonnegative coefficients, we can assume X_1 and X_2 do as well.

Towards a contradiction, suppose that $X_1 = 0$. Then $E = QX_2$. Let χ' be a character of H and let $\chi'|_Q$ be the restriction of χ' to Q. We may assume $\chi'|_Q$ is non-trivial, and therefore that $\chi'^\star(Q) = \chi'^\star|_Q(Q) = 0$. Then $z = \chi'^\star(E) = 0$, a contradiction since we have $z\overline{z} = n$. As such, $X_1 \neq 0$. Therefore there must exist at least one coefficient in $E = p^a X_1 + QX_2$ which is greater than or equal to p^a. However, since the coefficients of E are precisely the intersection numbers for D with respect to K, no coefficient of E can be greater than $|K|$. As $|K| = |U||W|$, we obtain:

$$p^a \leq |U||W| = \frac{|U||P|}{\exp(P)},$$

which is easily rearranged to give the desired result. □

A slightly different, though equivalent, treatment of Turyn's Exponent Bound is given by Beth [9].

A much more general exponent bound was given by Schmidt [80]. Its proof

is extremely technical and we do not attempt to replicate it here. It uses a function $F(m, n)$, the domain of which is $\mathbb{N} \times \mathbb{N}$, which deals with the relationship of the square-free part of m and the prime divisors of n. We refer the reader to Beth [9] and Schmidt [80] for a comprehensive treatment, and simply state the highly advanced result here.

Theorem 9.12. Schmidt's Exponent Bound: Let D be a (v, k, λ)-difference set in a group G. Suppose $U \triangleleft G$ such that G/U is cyclic of order k. Then:

$$k \leq \left(\frac{2^{s-1} F(k, n)}{n} \right)^{1/2} v,$$

where s is the number of distinct odd prime divisors of k.

Chapter 10

RECENT DEVELOPMENTS AND ACTIVE RESEARCH

As a reference, we note that useful tables of difference sets are given by Jungnickel [52], Kibler [55], and Lander [59]. Literal hundreds of results relating to various combinations of parameters of difference sets and groups can be found in Beth [9], as a fairly comprehensive reference for the subject until the year 1999.

The comprehensive work of Beth and co-authors [9] is one of the last major overviews or surveys of the subject of difference sets, and was published in 1999. That same year, Pott and co-editors issued a volume (see [25], [53], [97]) collecting several surveys of more specific areas of difference sets by such major researchers as Davis, Jedwab, Xiang, Jungnickel, Arasu, Dillon, Pott, and others. Since then, other major works have been published, such as the volume of Moore and Pollatsek [72] used throughout this work, which serves as one of the first textbook-style introductions to the study of difference sets and is meant to be accessible to non-experts. Occasional smaller reviews of the subject are found in the literature. The 2005 review by Xiang [100] is a notable one. Additionally, conference proceedings relating to difference sets continue to be released as collected works (two such examples are [21] and [44]).

As comprehensive monographs constituting broad surveys of major results have not been published in over fifteen years, we will close with a brief review of some developments in the study of difference sets in that time frame. The reader is cautioned that a comprehensive survey could occupy several volumes, and we make no claim to such comprehensiveness here. Rather, we simply offer a cursory glance, with a non-rigid

focus on authors cited elsewhere in this work. We will prove one of the new results, but cannot possibly make even a small dent in this manner. Indeed, a cursory search on just one popular aggregation service reveals no less than 600 articles containing the phrase 'difference sets' in the last fifteen years - an astonishing amount of activity - published in just a small handful of journals.

Constructions of difference sets and families of difference sets continue to arguably dominate the field. The rich structure of difference sets invites many methods and contexts for construction. In 2001, for example, Arasu and Chen settled the question (affirmatively) of the existence of a $(320, 80, 24)$-difference set in $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_5$ using the methods of building sets and building blocks, which we have not covered in this work. The reader is directed to the paper of Arasu and Chen [5] as well as the work of Davis and Jedwab [25] and Beth [9] for a general overview of the methods of building blocks and sets. Constructive methods for difference sets continue to appear each year, whether for specific contexts (see [6], [18], [102]), or for new families (see [31], [76], [81]).

Constructive methods for partial differences (and using them to construct other difference sets) have also seen rich work. Briefly, Davis and Xiang have constructed a family of partial difference sets in abelian 2-groups [26], and in other contexts as well [99], as have Hou and co-authors [46]. Many papers have been published more recently on using partial difference sets to construct Hadamard difference sets and strongly regular graphs. For a very small sample, see the papers of Feng and Xiang ([37] and [38]), as well as by Ott [73] and Michel [71].

In 2008, Feng and Xiang [36] constructed a class of relative difference sets having notably large forbidden subgroups, and in 2016, Ott [75] unified several known families of partial difference sets as special cases of a more general construction.

The astute reader will have noted while reading Chapter 7 that Hadamard

matrices of all orders divisible by 4 up to 100 are very easy to construct, with the exception or order 96, using the theorems presented. As such, Hadamard matrices of order 96 (and therefore difference sets in groups of size 96) have attracted attention for quite some time, and still do. As recently as 2010, new investigations into Hadamard difference sets of order 96 have been undertaken [11].

Similarly, despite their classical nature and the great attention they have attracted for several decades, difference sets with multiplier -1 are still a rich area of research, either on their own merits [34], or as elements of a generalization of their properties (see, for example, [88] and [89]).

Some other noteworthy work includes new nonexistence results by Arasu and Ma [4] in 2001, which settled several previously open cases and may be thought of as progress in the affirmative towards a resolution of Conjecture 5.8. Chandler and Xiang showed in 2003 that two families, known as the HKM and Lin difference sets, were in fact inequivalent, with non-isomorphic developments [16]. Weng and co-authors showed an example of the power of difference sets as tools with the presentation of several new results related to the Paley family of graphs in a 2007 paper [90], Cao proposed a new generalization of difference sets in 2008 [15], and Coulter and Gutekunst introduced the new concept of 'special subsets' for studying difference sets in 2009 [22]. In 2016, Ott made several advances in the use of cyclotomy to study difference sets [74].

Among the many exciting constructive results in the last 15 years, a theorem of Arasu and co-authors [7] is not only significant, but highly accessible. We present it here, but first we require a lemma.

Lemma 10.1 Let $a_1, ..., a_m \in \mathbb{Z}$ such that:

$$\sum_{i=1}^{m} a_i = n.$$

If $n = qm + r$, where q and r are integers satisfying $0 \leq r < m$, then:

$$\sum_{i=1}^{m} a_i^2 \geq (m-r)q^2 + r(q-1)^2,$$

with equality if and only if exactly $m - r$ elements of $\{a_1, ..., a_m\}$ are equal to q and exactly r are equal to $q + 1$.

Proof. Suppose our proposed conditions for equality above are not satisfied. Then there exists at least one pair $i, j \in [m]$ such that $a_i - a_j > 1$. Let the set $\{a'_k\}_{k=1}^m$ be defined as follows: if $k \notin \{i, j\}$, then $a'_k = a_k$. If $k = i$, then $a'_i = a_i - 1$ and if $k = j$, then $a'_j = a_j + 1$. Then it is clear that we still have:

$$\sum_{k=1}^{m} a'_k = n.$$

However:

$$\sum_{k=1}^{m} (a'_k)^2 = \sum_{k=1}^{m} a_k^2 + 2(1 + a_j - a_i) < \sum_{k=1}^{m} a_k^2,$$

completing the proof. □

We are now ready to present and prove the theorem of Arasu and co-authors [7].

Theorem 10.2. Let G be an abelian group of size v and let $D_1, ..., D_{2l+1}$ be (v, k, λ)-difference sets in G with the property that $n \mid \lambda$. Suppose that:

$$n^l \mid \prod_{i=1}^{2l+1} D_i$$

in $\mathbb{Z}G$. Then there exists a (v, k, λ)-difference set D in G such that:

$$\prod_{i=1}^{2l+1} D_i = n^l \left(\frac{k\left((1 + (\lambda v/n))^l - 1\right)}{v} G + D \right) = (n + \lambda G)^l D$$

in $\mathbb{Z}G$.

Proof. For each $g \in G$, define a_g so that in $\mathbb{Z}G$, we have:

$$\prod_{i=1}^{2l+1} D_i = \sum_{g \in G} a_g g.$$

We know that we have:

$$\left(\prod_{i=1}^{2l+1} D_i\right)\left(\prod_{i=1}^{2l+1} D_i\right)^{(-1)} = (n + \lambda G)^{2l+1}.$$

Furthermore, since $k^2 = n + \lambda v$ (see Lemma 3.5), we can write:

$$\sum_{g \in G} a_g = k^{2l+1} = k(n + \lambda v)^l = kn^l(1 + (\lambda v/n))^l$$

and

$$\sum_{g \in G} a_g^2 = n^{2l+1} + \frac{(n + \lambda v)^{2l+1} - n^{2l+1}}{v} = n^{2l+1}\left(1 + \frac{(1 + (\lambda v/n))^{2l+1} - 1}{v}\right).$$

We know that n^l divides $\prod_{i=1}^{2l+1} D_i$ in $\mathbb{Z}G$ by hypothesis, so we have $a_g/n^l \in \mathbb{Z}$ for every $g \in G$. Additionally, we have:

$$\sum_{g \in G} \frac{a_g}{n^l} = k(1 + (\lambda v/n))^l = k((1 + (\lambda v/n))^l - 1) + k,$$

and

$$\sum_{g \in G} \frac{a_g^2}{n^{2l}} = n\left(1 + \frac{(1 + (\lambda v/n))^{2l+1} - 1}{v}\right).$$

Now, we can easily verify that:

$$n\left(1+\frac{(1+(\lambda v/n))^{2l+1}-1}{v}\right)=\left(\frac{k((1+(\lambda v/n))^{l}-1)}{v}\right)^{2}(v-k)$$
$$+\left(\frac{k((1+(\lambda v/n))^{l}-1)}{v}+1\right)^{2}k.$$

By Lemma 10.1, there must exist a k-subset of D such that:

$$\prod_{i=1}^{2l+1}D_i=n^l\left(\frac{k((1+(\lambda v/n))^{l}-1)}{v}G+D\right)=(n+\lambda G)^l D,$$

and we are done. □

Most excitingly, several conjectures relevant to difference sets have recently seen progress towards a conclusion, or been settled altogether, and we close with those encouraging results.

In 1983, Lander [58] made the following conjecture.

Conjecture 10.3. Let G be an abelian group of size v, and let D be a difference set of order n in G. If p is a prime such that $p \mid v$ and $p \mid n$, then the Sylow p-subgroup of G is not cyclic.

Progress has been made in the affirmative by Feng and co-authors [39]. In a 2014 paper, they proved that Lander's conjecture holds when n is a power of a prime $p > 3$, though they note that the conjecture is unlikely to hold in total generality.

In Jungnickel [52], the following conjecture is given special attention.

Conjecture 10.4. Suppose there exists a (v, k, λ)-difference set with $v = 4u^2$, $k = 2u^2 \pm u$, and $\lambda = u^2 \pm u$ for some integer u. Then u is of the form $2^r 3^s$ for nonnegative integers r and s.

In a 1992 paper (published almost concurrently with the volume in which Jungnickel stated the conjecture), Xia [92] gave a construction refuting it. A simplified

proof of Xia's method was then given by Xiang and Chen in 1996 [96].

In fact, Jungnickel gives many open problems at the end of his work, and almost all remain at least partially open. For example, he mentions the problem of finding non-Menon reversible difference sets other than the case of the $(4000, 775, 150)$-difference set already known, and mentions the following closely related conjecture.

Conjecture 10.5. Let p be an odd prime, let $a \geq 0$ and let $b, t, r \geq 1$. Then:

(i) $Y = 2^{2a+2}p^{2t} - 2^{2a+2}p^{t+r} + 1$ is a square if and only if $Y = 1$, or, equivalently, if $t = r$.

(ii) $Z = 2^{2b+2}p^{2t} - 2^{b+2}p^{t+r} + 1$ is a square if and only if $Z = 2401$, or, equivalenly, if $(p, b, t, r) = (5, 3, 1, 2)$.

The second statement is still open, but Le and Xiang [59] proved the first in a 1996 paper.

Beth's work [9] lists many open problems. Progress has been made on several, most notably the following.

Conjecture 10.6. There exist no non-trivial dihedral difference sets.

While other specific cases of this conjecture were solved as early as 1985 [35] and 1996 [82], Deng [28] was able to confirm this in 2004 for the case of groups having order $4p^t$ for a prime p and positive integer t.

REFERENCES

[1] Arasu, KT and DK Ray-Chauduri. *Multiplier theorem for a difference list*. Ars Combinatoria, 1986. 22, Pgs. 119-137.

[2] Arasu, KT. *Singer groups of biplanes of order 25*. Archiv der Mathematik, 1988. 51, Pgs. 188-192.

[3] Arasu, KT and DL Stewart. *Certain implications of the multiplier conjecture*. Journal of Combinatorial Mathematics and Combinatorial Computing, 1988. 3, Pgs 207-211.

[4] Arasu, KT and SL Ma. *A nonexistence result on difference sets, partial difference sets and divisible difference sets*. Journal of Statistical Planning and Inference, 2001. 95, Pgs. 67-73.

[5] Arasu, KT and YQ Chen. *A difference set in* $(\mathbb{Z}/4\mathbb{Z})^3 \times \mathbb{Z}/5\mathbb{Z}$. Designs, Codes, and Cryptography, 2001. 23, Pgs. 317-323.

[6] Arasu, KT and KJ Player. *A New Family of Cyclic Difference Sets with Singer Parameters in Characteristic Three*. Designs, Codes, and Cryptography, 2003. 28, Pgs. 75-91.

[7] Arasu, KT et. al. *Abelian difference sets of order n dividing* λ. Designs, Codes, and Cryptography, 2007. 44, Pgs. 307-319.

[8] Assmus, EF and JD Key. *Designs and Their Codes*. Cambridge University Press, 1993 (corrected version).

[9] Beth, T et al. *Design Theory*, vol. 1. Cambridge University Press, 1999. 2nd ed.

[10] Bose, RC. *On the Construction of Balanced Incomplete Block Designs*. Annals of Eugenics, 1939. 9, Pgs. 353-399.

[11] Braić, S et. al. *Graphs and Symmetric Designs Corresponding to Difference Sets in Groups of order* 96. Glasnik Matematicki, 2010. 45, Pgs. 1-14.

[12] Bruck, RH and HJ Ryser. *The nonexistence of certain finite projective planes.* Canadian Journal of Mathematics, 1949. 1, Pgs. 88-93.

[13] Bruck, RH. *Difference Sets in a Finite Group.* Transactions of the American Mathematical Society, 1955. 78, 464-481.

[14] Camion, P. *Difference Sets in Elementary Abelian Groups.* Les Presses De L'Université De Montréal, 1979.

[15] Cao, X. *Some results on generalized difference sets.* Journal of Systems Science & Complexity, 2008. 21, Pgs. 76-84.

[16] Chandler, DB and Q Xiang. *The invariant factors of some cyclic difference sets.* Journal of Combinatorial Theory A, 2003. 101, Pgs. 131-146.

[17] Chen, YQ. *A construction of difference sets.* Design, Codes, and Cryptography, 1998. 13, Pgs. 247-250.

[18] Chen, YQ and T Feng. *Paley type sets from cyclotomic classes and Arasu–Dillon–Player difference sets.* Designs, Codes, and Cryptography, 2015. 74, Pgs. 581-600.

[19] Chowla, S and HJ Ryser. *Combinatorial problems.* Canadian Journal of Mathematics, 1950. 2, Pgs. 93-99.

[20] Colbourn, CJ and PC van Oorschot. *Applications of combinatorial designs in computer science.* ACM Computing Surveys, 1989. 21, Pgs. 223-250.

[21] Colbourn, CJ, editor. *Algebraic Design Theory and Hadamard Matrices.* Springer International, 2015.

[22] Coulter, RS and T Gutekunst. *Special subsets of difference sets with particular emphasis on skew Hadamard difference sets.* Designs, Codes, and Cryptography, 2009. 53, Pgs. 1-12.

[23] Davis, JA. *A Result on Dillon's Conjecture in Difference Sets.* Journal of Combinatorial Theory A, 1991. 57, Pgs. 238-242.

[24] Davis, JA and J Jedwab. *A unifying construction for difference sets.* Journal of Combinatorial Theory A, 1997. 80, Pgs. 13-78.

[25] Davis, JA and J Jedwab. *A Unified Approach to Difference Sets with* $\gcd(V, N) > 1$ in *Difference Sets, Sequences, and Their Correlation Properties*. A Pott et al., editors. Kluwer Academic Publishers, 1999.

[26] Davis, JA and Q Xiang. *A Family of Partial Difference Sets with Denniston Parameters in Nonelementary Abelian* 2*-Groups*. European Journal of Combinatorics, 2000. 21, 981-988.

[27] de Launey, W and D Flannery. *Algebraic Design Theory*. American Mathematical Society, 2011.

[28] Deng, Y. *A note on difference sets in dihedral groups*. Archiv Mathematik., 2004. 82, Pgs 4-7.

[29] Dillon, JF. *Elementary Hadamard Difference Sets*. Doctoral thesis, 1974. University of Maryland.

[30] Dillon, JF. *Variations on a scheme of McFarland for noncyclic difference sets*. Journal of Combinatorial Theory A, 1985. 40, Pgs. 9-21.

[31] Ding, C et. al. *Skew Hadamard difference sets from the ReeTits slice symplectic spreads in* $PG(3, 3^2h + 1)$. Journal of Combinatorial Theory A, 2007. 114, Pgs. 867-887.

[32] Ding, C. *Codes From Difference Sets*. World Scientific, 2014.

[33] Dummit, DS and RM Foote. *Abstract Algebra*. Wiley, 2004. 3rd ed.

[34] Elvira, DT. *On Hadamard difference sets with weak multiplier minus one*. Hokkaido Mathematical Journal, 2001. 32, Pgs. 31-39.

[35] Fan, CT et. al. *Difference Sets in Dihedral Groups and Interlocking Difference Sets*. Ars Combinatoria, 1985. 20, Pgs. 99-107.

[36] Feng, T and Q Xiang. *Semi-regular relative difference sets with large forbidden subgroups*. Journal of Combinatorial Theory A, 2008. 115, Pgs. 1456-1473.

[37] Feng, T et. al. *Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes*. Combinatorica, 2011. 35, Pgs. 413-434.

[38] Feng, T and Q Xiang. *Cyclotomic constructions of skew Hadamard difference sets*. Journal of Combinatorial Theory A, 2012. 119, Pgs. 245-256.

[39] Feng, T et. al. *Hadamard difference sets related to Lander's Conjecture*. Journal of Algebra, 2014. 403, Pgs. 29-47.

[40] Hall, M. *Cyclic Projective Planes*. Duke Mathematical Journal, 1947. 14, Pgs. 1079-1090.

[41] Hall, M and HJ Ryser. *Cyclic incidence matrices*. Canadian Journal of Mathematics, 1951. 3, Pgs. 495-502.

[42] Hall, M. *A survey of difference sets*. Proceedings of the American Mathematical Society, 1956. 7, Pgs. 975-986.

[43] Hall, M. *Combinatorial Theory*. Wiley, 1986.

[44] Helleseth, T and J Jedwab, editors. *Sequences and Their Applications - SETA 2012, 7th International Conference Proceedings*. Springer, 2012.

[45] Hirschfeld, JWP. *Projective Geometries over Finite Fields*. Oxford University Press, 1979.

[46] Hou, X et. al. *New Partial Difference Sets in $\mathbb{Z}_{p^2}^t$ and a Related Problem about Galois Rings*. Finite Fields and Their Applications, 2001. 7, Pgs 165-188.

[47] Iiams, JE. *On difference sets in groups of order $4p^2$*. Journal of Combinatorial Theory A, 1995. 72, Pgs. 256-276.

[48] Ionin, YJ and MS Shrikhande. *Combinatorics of Symmetric Designs*. Cambridge University Press, 2006.

[49] Ireland, K and M Rosen. *A Classical Introduction to Modern Number Theory*. Springer, 1998. 2nd ed (corrected).

[50] Isaacs, IM. *Algebra: A Graduate Course*. American Mathematical Society, 2009.

[51] Jones, BW. *The Arithmetic Theory of Quadratic Forms*. MAA, 1950.

[52] Jungnickel, D. *Difference Sets* in *Contemporary Design Theory: A Collection of Surveys*. JH Dinitz and DR Stinson, editors. Wiley Interscience, 1992.

[53] Jungnickel, D and A Pott. *Difference Sets: An Introduction* in *Difference Sets, Sequences, and Their Correlation Properties*. A Pott et al., editors. Kluwer Academic Publishers, 1999.

[54] Kharaghani, H and B Tayfeh-Rezaie.*A Hadamard Matrix of Order 428*. Preprint, 2004. http://math.ipm.ac.ir/tayfeh-r/papersandpreprints/h428.pdf

[55] Kibler, RE. *A summary of non-cyclic difference sets, $k < 20$*. Journal of Combinatorial Theory A, 1978. 25, Pgs. 62-67.

[56] Kraemer, RG. *Proof of a conjecture on Hadamard 2-groups*. Journal of Combinatorial Theory A, 1993. 63, Pgs. 1-10.

[57] Lam, CWH et al. *The non-existence of finite projective planes of order 10*. Canadian Journal of Mathematics, 1989 Pgs. 1117-1123.

[58] Lam, CWH. *The search for a finite projective plane of order 10*. The American Mathematical Monthly, 1991. 98, Pgs. 305-315.

[59] Lander, ES. *Symmetric Designs: An Algebraic Approach*. Cambridge University Press, 1983.

[60] Le, M and Q Xiang. *A result on Ma's conjecture*. Journal of Combinatorial Theory A, 1996. 73, Pgs. 181-184.

[61] Ma, SL. *Polynomial addition sets*. Doctoral thesis. University of Hong Kong, 1985.

[62] Ma, SL. *On McFarland's conjecture on abelian difference sets with multiplier minus one*. Designs, Codes, and Cryptography, 1992. 1, Pgs. 321-332.

[63] Mann, HB. *Balanced incomplete block designs and abelian difference sets*. Illinois Journal of Mathematics, 1964. 8, Pgs. 252-261.

[64] McFarland, RL and HB Mann. *On multipliers of difference sets*. Canadian Journal of Mathematics, 1965. 17, Pgs. 541-542.

[65] McFarland, RL. *A family of difference sets in non-cyclic groups*. Journal of Combinatorial Theory A, 1973. 15, Pgs. 1-10.

[66] McFarland, RL. *Difference sets in abelian groups of order $4p^2$*. Journal of Combinatorial Theory A, 1973. 15, Pgs. 1-10.

[67] McFarland, RL and BF Rice. *Translates and multipliers of abelian difference sets*. Proceedings of the American Mathematical Society, 1978. 68, Pgs. 375-379.

[68] McFarland, RL and SL Ma. *Abelian difference sets with multiplier minus one*. Archiv Mathematik, 1990. 54, Pgs. 610-623.

[69] Menon, PK. *Difference Sets in Abelian Groups*. Proceedings of the American Mathematical Society, 1960. 11, Pgs. 368-375.

[70] Menon, PK. *On difference sets whose parameters satisfy a certain relation*. Proceedings of the American Mathematical Society, 1962. 13, Pgs. 739-745.

[71] Michel, J. *New Partial Geometric Difference Sets and Partial Geometric Difference Families*. Acta Mathematica Sinica, English Series, 2016. 33, Pgs. 591-606.

[72] Moore, EH and HS Pollatsek. *Difference Sets*. American Mathematical Society, 2013.

[73] Ott, U. *Some new families of partial difference sets in finite fields*. Journal of Geometry, 2016. 107, Pgs. 267-278.

[74] Ott, U. *On Jacobi sums, difference sets and partial difference sets in Galois domains*. Designs, Codes, and Cryptography, 2016. Pgs. 80, Pgs. 241-281.

[75] Ott, U. *A generalization of a cyclotomic family of partial difference sets given by Fernández-Alcober, Kwashira and Martínez*. Discrete Mathematics, 2016. 339, Pgs. 2153-2156.

[76] Polhill, J et al. *A new product construction for partial difference sets*. Designs, Codes, and Cryptography, 2013. 68, Pgs. 155-161.

[77] Pott, Alexander. *Finite Geometry and Character Theory*. Springer, 1995.

[78] Roetteler, M. *Quantum algorithms for abelian difference sets and applications to dihedral hidden subgroups*, 2016. arXiv: `608.02005v1`.

[79] Ryser, HJ. *The existence of symmetric block designs*. Journal of Combinatorial Theory A, 1982. 32, Pgs. 103-105.

[80] Schmidt, B. *Cyclotomic integers and finite geometry*. Journal of the American Mathematical Society, 1999. 12, Pgs. 929-952.

[81] Schmidt, B and MM Tan. *Construction of relative difference sets and Hadamard groups*. Designs, Codes, and Cryptography, 2014. 73, Pgs. 105-119.

[82] Shiu, WC. *Difference Sets in Groups Containing Subgroups of Index 2*. Ars Combinatoria, 1996. 42, Pgs. 199-205.

[83] Singer, J. *A theorem in finite projective geometry and some applications to number theory*. Transactions of the American Mathematical Society, 1938. 43, 377-385.

[84] Spence, E. *A family of difference sets*. Journal of Combinatorial Theory A, 1977. 22, Pgs. 103-106.

[85] Turyn, RJ. *Character sums and difference sets*. Pacific Journal of Mathematics, 1965. 15, Pgs. 319-346.

[86] van Lint, JH and RM Wilson. *A Course in Combinatorics*. Cambridge University Press, 2006. 2nd. ed. (corrected version).

[87] Wallis, WD. *Combinatorial Designs*. Marcel Dekker, Inc., 1988.

[88] Webster, JD. *Reversible and DRAD difference sets in* $(C_{2^{2r}})^3$. Journal of Combinatorial Designs, 2010. DOI 10.1002/jcd

[89] Webster, JD. *Reversible difference sets with rational idempotents*. Arabian Journal of Mathematics, 2013. 2, Pgs. 103-114.

[90] Weng, G et. al. *Pseudo-Paley graphs and skew Hadamard difference sets from presemifields*. Designs, Codes, and Cryptography, 2007. 44, Pgs. 49-62.

[91] Wilbrink, HA. *A note on planar difference sets*. Journal of Combinatorial Theory AA, 1985. 38, Pgs. 94-95.

[92] Xia, MY. *Some infinite classes of special Williamson matrices and difference sets*. Journal of Combinatorial Theory A, 1992. 61, Pgs. 230-242.

[93] Xia, P et al. *Achieving the Welch Bound with Difference Sets*. IEEE Transactions on Information Theory, 2005. 51, Pgs. 1900-1907.

[94] Xiang, Q et al. *Extraneous Multipliers of Abelian Difference Sets* in *Combinatorial Designs and Applications*. WD Wallis et al., editors. Marcel Dekker, Inc., 1990.

[95] Xiang, Q and YQ Chen. *On the size of the Multiplier Groups of Cyclic Difference Sets*. Journal of Combinatorial Theory A, 1995. 69, Pgs. 168-169.

[96] Xiang, Q and Chen, YQ. *On Xia's Construction of Hadamard Difference Sets*. Finite Fields and Their Applications, 1996. 2, Pgs. 87-95.

[97] Xiang, Q. *Recent Results of Difference Sets With Classical Parameters* in *Difference Sets, Sequences, and Their Correlation Properties*. A Pott et al., editors. Kluwer Academic Publishers, 1999.

[98] Xiang, Q et al. *Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets*. Journal of Combinatorial Theory A, 1999. 87, Pgs. 74-119.

[99] Xiang, Q and JA Davis. *Constructions of Low Rank Relative Difference Sets in 2-Groups Using Galois Rings*. Finite Fields and Their Applications, 2000. 6, 130-145.

[100] Xiang, Q. *Recent progress in algebraic design theory*. Finite Fields and Their Applications, 2005. 11, Pgs. 622-653.

[101] Xie, Y. et al. *Quantum stabilizer codes from difference sets*. Proc. IEEE Information Theory Symposium, Istanbul, Turkey, 2013.

[102] Yamada, M. *Difference sets over Galois rings with odd extension degrees and characteristic an even power of 2*. Designs, Codes, and Cryptography, 2011. 67, Pgs. 37-57.

[103] Zhang, L. et al. *Pattern Design and Imaging Methods in 3-D Coded Aperture Techniques*. Proc. IEEE Nuclear Science Symposium, Toronto, Canada, 1998.

Appendix A

PROOF OF THE BRUCK-RYSER-CHOWLA THEOREM

We proved the case of v even in the text. We now give a proof of the case v odd. Our proof draws from Moore [72] and the simplified proof given by Ryser [79]. We begin with a simple lemma.

Lemma A.1. Let p be an odd prime. Then for $x, y \in \left[0, \frac{p-1}{2}\right] \cap \mathbb{Z}$, $x^2 \equiv y^2 \pmod{p}$ implies that $x = y$.

Proof. Since $x^2 \equiv y^2 \pmod{p}$, we can say that $p \mid (x^2 - y^2)$, from which we obtain $p \mid [(x+y)(x-y)]$, but it is clear that $0 \leq x + y \leq (p-1)$ so $p \nmid (x+y)$, so it must be true that $p|(x-y)$ and $x - y \leq x + y$, so we have $x - y = 0$, and $x = y$. $\square$

Lemma A.2. If p is an odd prime, then there exist $n, x, y \in \mathbb{N}$ such that $np = x^2 + y^2 + 1$ and $1 \leq n < p$.

Proof. By Lemma A.1, the set $\left|\{x^2 \mod p : x \in \left[0, \frac{p-1}{2}\right] \cap \mathbb{Z}\}\right|$ and the set $\left|\{-y^2 - 1 \mod p : y \in \left[0, \frac{p-1}{2}\right] \cap \mathbb{Z}\}\right|$ both have cardinality $\frac{p+1}{2}$. But there are only p residues modulo p, so there must exist $x, y \in \left[0, \frac{p-1}{2}\right] \cap \mathbb{Z}$ such that $x^2 \equiv -y^2 - 1 \pmod{p}$, and hence $x^2 + y^2 + 1 \equiv 0 \pmod{p}$, from which we know there must exist $n \in \mathbb{N}$ such that $x^2 + y^2 + 1 = np$. Further, we have $np = x^2 + y^2 + 1 \leq 2\left(\frac{p-1}{2}\right)^2 + 1 < p^2$, so $n < p$, and since $n \in \mathbb{N}$, we have $1 \leq n < p$. $\square$

Theorem A.3. Lagrange's Theorem: Every integer can be written as the sum of four (not necessarily distinct) squares.

Proof. If a and b can be written as the sum of four squares, then we can write $a = w^2 + x^2 + y^2 + z^2$ and $b = q^2 + r^2 + s^2 + t^2$. Then it is easy to check that $ab = (qw +$

$rx+sy+tz)^2+(wr-rx+yt-sz)^2+(ws-tx-qy+rz)^2+(tw+sy-sx-qz)^2$. Therefore, it is enough to prove Lagrange's Theorem for primes. Note that $2 = 1^2+1^2+0^2+0^2$, so suppose p is an odd prime. By Lemma A.2, there exist $n, x, y \in \mathbb{N}$ such that $1 \leq n < p$ and $np = x^2 + y^2 + 1$. Thus, $np = x^2 + y^2 + 1^2 + 0^2$, and np is the sum of four squares. If n is the smallest integer such that np is the sum of four squares $a^2 + b^2 + c^2 + d^2$, we claim that $n = 1$.

Towards a contradiction, suppose $n > 1$. Define $a \equiv A \pmod{n}$, $b \equiv B \pmod{n}$, $c \equiv C \pmod{n}$, and $d \equiv D \pmod{n}$. We can choose these such that each of A, B, C, D is in the set $(-n/2, n/2) \cap \mathbb{Z}$, so that $A^2 + B^2 + C^2 + D^2 \equiv 0 \pmod{n}$. Hence, there exists $m \in \mathbb{N}$ such that $mn = A^2 + B^2 + C^2 + D^2$. We also have $0 \leq A^2 + B^2 + C^2 + D^2 \leq 4\left(\frac{n}{2}\right)^2 = n^2$, so that $0 \leq m \leq n$.

If $m = 0$, then $A = B = C = D = 0$ and n divides each of a, b, c, and d. Then $n^2|(a^2 + b^2 + c^2 + d^2)$ implies that $n^2|np$, and thus $n|p$, a contradiction since p is prime and $1 < n < p$ (specifically, the contradiction occurs since $n \neq 1$).

If $m = n$, then $A = B = C = D = \frac{n}{2}$ and a, b, c, d are all odd multiples on $\frac{n}{2}$. Again, then, $n^2|(a^2 + b^2 + c^2 + d^2)$, giving a contradiction. Hence, $0 < m < n$.

Now, we can write:

$$\begin{aligned}(np)(mn) =&(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2)\\ =&(aA + bB + cC + dD)^2 + (aB - bA + cD - dC)^2\\ &+ (aC - bD - cA + dB)^2 + (aD + bC - cB - dA)^2,\end{aligned}$$

and note that each squared term is 0 modulo n, so each squared term has a natural number j such that that term is equal to $(jn)^2$. Dividing by n^2 gives mp as a sum of four squares with $0 < m < n$. But we chose n to be the smallest natural number such that np is a sum of four squares, so this is a contradiction. Hence $n = 1$ and we are

done. □

Definition A.4. Square matrices of the same size with entries in $\mathbb{Q}$ are said to be *equivalent* over $\mathbb{Q}$ if there exists an invertible matrix S with entries from $\mathbb{Q}$ such that $S^\top AS = B$. In this case, S is said to *transform* A into B. We denote this by writing $A \sim B$. This is easily seen to be an equivalence relation.

Theorem A.5. Let I_4 denote the 4×4 identity matrix. Then for all $n \in \mathbb{N}$, we have $nI_4 \sim I_4$.

Proof. By Theorem A.3, there exist integers a, b, c, d such that $n = a^2 + b^2 + c^2 + d^2$. Let S be defined as below:

$$S = \begin{pmatrix} a & b & c & d \\ b & -a & -d & c \\ c & d & -a & -b \\ d & -c & b & -a \end{pmatrix}.$$

Then it is easy to check that S is invertible with entries in $\mathbb{Z} \subset \mathbb{Q}$ and that $S^\top I_4 S = nI_4$. □

Theorem A.6. Witt's Cancellation Theorem: Let A and B be invertible $n \times n$ matrices with entries in $\mathbb{Q}$ and also let $c \in \mathbb{Q}$.

$$\text{If } \left(\begin{array}{c|c} c & 0 \\ \hline 0 & A \end{array}\right) \sim \left(\begin{array}{c|c} c & 0 \\ \hline 0 & B \end{array}\right),$$

then $A \sim B$.

Proof. Our proof is due to Jones [51]. We must find S such that $S^\top AS = B$. Since A and B are invertible, S must be as well. By hypothesis, there must exist a matrix of the form:

$$\left(\begin{array}{c|c} t & u^\top \\ \hline v & M \end{array}\right),$$

where u and v are elements of $\mathbb{Q}^n$, $t \in \mathbb{Q}$, and M is an $n \times n$ matrix, such that:

$$\left(\begin{array}{c|c} t & v^\top \\ \hline u & M^\top \end{array}\right)\left(\begin{array}{c|c} c & 0 \\ \hline 0 & A \end{array}\right)\left(\begin{array}{c|c} t & u^\top \\ \hline v & M \end{array}\right) = \left(\begin{array}{c|c} c & 0 \\ \hline 0 & B \end{array}\right).$$

Hence, the following must hold:

$$\begin{aligned} c &= t^2 c + v^\top A v \\ 0 &= tcu^\top + v^\top AM \\ 0 &= tcu + M^\top Av \\ B &= cuu^\top + M^\top AM. \end{aligned}$$

Let $d := \frac{1}{t+1}$ for $t \neq -1$ and $d := \frac{1}{t-1}$ otherwise, and let $S = M - dvu^\top$. Using the relations derived above, we have:

$$\begin{aligned} S^\top AS =& (M^\top - duv^\top)A(M - dvu^\top) \\ =& M^\top AM - dM^\top Avu^\top - duv^\top AM + d^2 uv^\top AVu^\top \\ =& M^\top AM + 2cdtuu^\top - d^2 cu(t^2-1)u^\top \\ =& M^\top AM + cd(2t - d(t^2-1))uu^\top \\ =& M^\top AM + cuu^\top = B, \end{aligned}$$

and we are done. □

We now prove the BRC theorem for v odd. We assume a symmetric design $\mathcal{D}$ with parameters (v, k, λ) exists. Let N be its $v \times v$ incidence matrix. Then $N^\top N = nI + \lambda J$. We can assume $\lambda > 0$ and hence define the following, all of which are to be understood as $(v+1) \times (v+1)$ matrices:

$$A = \left(\begin{array}{ccc|c} & N & & 1 \\ & & & \vdots \\ & & & 1 \\ \hline 1 & \cdots & 1 & k/\lambda \end{array}\right), D = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \vdots \\ \vdots & 0 & 1 & 0 \\ 0 & \cdots & 0 & -\lambda \end{pmatrix}, E = \begin{pmatrix} n & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \vdots \\ \vdots & 0 & n & 0 \\ 0 & \cdots & 0 & -n/\lambda \end{pmatrix}.$$

It is easy to check that D and E are invertible and that $A^\top DA = E$, so $D \sim E$. The proof now splits into two cases, since v is odd. We now use the notation $\text{di}[a, b, c, ...]$ to denote a matrix with diagonal entries respectively given in the array and 0 as every non-diagonal entry.

Case 1: Suppose $v \equiv 1 \pmod 4$. Then by Theorem A.5, $E \sim \text{di}[1, ..., 1, n, -n\lambda]$, and both are diagonal, and hence invertible. By $v - 1$ applications of Theorem A.6 with D, then, we have $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -\lambda \end{smallmatrix}\right) \cong \left(\begin{smallmatrix} n & 0 \\ 0 & -n/\lambda \end{smallmatrix}\right)$, so there must exist a matrix M such that $M^\top \left(\begin{smallmatrix} 1 & 0 \\ 0 & -\lambda \end{smallmatrix}\right) M = \left(\begin{smallmatrix} n & 0 \\ 0 & -n/\lambda \end{smallmatrix}\right)$. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Equating the top right matrix entry on both sides gives $a^2 - c^2\lambda = n$, or $a^2 = n + \lambda c^2$. In other words, $(x, y, z) = (a, 1, c)$ is a solution in $\mathbb{Q}$ to the equation $x^2 = ny^2 + \lambda z^2$, and multiplying by an appropriate constant gives our solution in $\mathbb{Z}$, completing the proof of Case 1.

Case 2. Suppose $v \equiv 3 \pmod 4$. We know $D \sim E$. It follows from Theorem A.6 and a few basic properties about matrices, then, that the following holds, where each is a $(v + 2) \times (v + 2)$ matrix:

$$\text{di}[1, ..., 1, n, -\lambda] \sim \text{di}[n, ..., n, n, -n/\lambda].$$

By Theorem A.5, we can then write $\text{di}[1, ..., 1, n, -\lambda] \sim \text{di}[1, ..., 1, n, -n/\lambda]$, and again by Theorem A.6 as in Case 1, we have $\left(\begin{smallmatrix} n & 0 \\ 0 & -\lambda \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} 1 & 0 \\ 0 & -n/\lambda \end{smallmatrix}\right)$. By the same rationale as in Case 1, then, there exist $a, c \in \mathbb{Q}$ such that $a^2n - c^2\lambda = 1$ so that $(x, y, z) = (1, a, c)$ is a solution in $\mathbb{Q}$ to $x^2 = ny^2 - \lambda z^2$, and we can again multiply by an appropriate constant to get a solution in $\mathbb{Z}$. Our proof of Case 2, and hence the Bruck-Ryser-Chowla

Theorem in its entirety, is now finished. □

Appendix B

ADDITIONAL PROOFS

Proof A (See Theorem 4.1). We want to show that $\det(nI + \lambda J) = (n + \lambda v)n^{v-1}$. We proceed by adding each row to the first, removing a constant, subtracting the first column from each entry, and exploiting the resulting convenient form:

$$\det(nI + \lambda J) = \begin{vmatrix} k & \lambda & \lambda & \cdots & \lambda \\ \lambda & k & \lambda & \cdots & \lambda \\ \lambda & \lambda & k & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & k \end{vmatrix}$$

$$= \begin{vmatrix} k+\lambda(v-1) & k+\lambda(v-1) & k+\lambda(v-1) & \cdots & k+\lambda(v-1) \\ \lambda & k & \lambda & \cdots & \lambda \\ \lambda & \lambda & k & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & k \end{vmatrix}$$

$$= (k+\lambda(v-1)) \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ \lambda & k & \lambda & \cdots & \lambda \\ \lambda & \lambda & k & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & k \end{vmatrix} = (k+\lambda(v-1)) \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ \lambda & k-\lambda & 0 & \cdots & 0 \\ \lambda & 0 & k-\lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & \cdots & k-\lambda \end{vmatrix}$$

$$= (k+\lambda(v-1))(k-\lambda)^{v-1} = (n+\lambda v)n^{v-1}. \qquad \square$$

Proof B (See Theorem 5.18). We will prove the theorem in a specific case, and refer to the reader to the proof of McFarland and Rice [67] for the lengthy second case. Let D be an abelian difference set in a group G. Then G is isomorphic to a

direct product of m groups G_i each having prime power order for some $m \in \mathbb{N}$. Using the same logic as in Theorem 6.6, for each $i \in [m]$ we define the ring homomorphism $\hat{\phi}_i : \mathbb{Z}G \to \mathbb{Z}G_i$. Let $D_i = \hat{\phi}_i$. Define T to be the group of numerical multipliers of D, and for each $i \in [m]$, let T_i be the group of numerical multipliers of D_i. There are two cases.

If T_i is cyclic, then let $t \in T$ be such that $\langle t \rangle = T_i$ and Dg is fixed by t for some fixed $g \in G$. Then $\phi : g \mapsto g_i$ and $D_i g_i$ is fixed by t. Hence, $D_i g_i$ is fixed by all elements of T_i, and hence of t.

We refer the reader to the detailed proof in [66] for the case in which T_i is not cyclic. $\square$

Proof C (See Theorem 5.22). Consider D in the context of $\mathbb{Z}G$. It is obvious that $D^p \equiv D^{(p)} \pmod{p}$, so since $D^{(p)} = D$ by hypothesis, we have $D(D^{p-1} - 1) = D^p - D = pA$ for some $A \in \mathbb{Z}G$. Therefore:

$$\begin{aligned} 0 \equiv &(pA)(pA^{(-1)}) = (D^p - D)\left[\left(D^{(-1)}\right)^p - D^{(-1)}\right] \\ = &D^p\left(D^{(-1)}\right)^p - D^p D^{(-1)} - D\left(D^{(-1)}\right)^p + DD^{(-1)} \\ = &\left(DD^{(-1)}\right)^p + DD^{(-1)}\left[1 - D^{p-1} - \left(D^{(-1)}\right)^{p-1}\right] \pmod{p^2}. \end{aligned}$$

Since it is clear that $DG = D^{(-1)}G = kG$, and also by using Theorem 6.2, we can write our last line above as:

$$\begin{aligned} (n + \lambda G)^p + (n + \lambda G)&\left[1 - D^{p-1} - \left(D^{(-1)}\right)^{p-1}\right] \\ &= (n + \lambda G)^p + (n + \lambda G) - nD^{p-1} - n\left(D^{(-1)}\right)^{p-1} - 2\lambda k^{p-1} G. \end{aligned}$$

Therefore, we have:

$$n\left[D^{p-1}+\left(D^{(-1)}\right)^{p-1}\right]\equiv(n+\lambda G)^p+(n+\lambda G)-2\lambda k^{p-1}G\ (\mathrm{mod}\ p^2),$$

which we will refer to for the rest of this proof as "$\star$". We now break the problem into cases.

Case (i): If $p \mid \lambda$, then $p \mid k$ since $p \mid n$. As such, we can write $(n+\lambda G)^p \equiv \lambda k^{p-1} \pmod{p^2}$. Since from Lemma 3.5 we have $\lambda v = k^2 - n$, we can write $\lambda v \equiv -n \pmod{p^2}$, so that $\lambda \equiv -nv^{-1} \equiv -nv^{p(p-1)-1} \pmod{p^2}$. From $\star$, we obtain the following by substitution:

$$n\left[D^{p-1}+\left(D^{(-1)}\right)^{p-1}\right]\equiv n+\lambda G\equiv n-nv^{p(p-1)-1}G\ (\mathrm{mod}\ p^2),$$

and since $p^2 \nmid n$ by hypothesis, we have $D^{p-1}-\left(D^{(-1)}\right)^{p-1} = 1+v^{p-2}G$ in $\mathbb{Z}_pG$, completing our first case.

Case (ii): If $p \nmid \lambda$, then $p \nmid k$, since $p \mid n$. By Lemma 3.5, $\lambda \equiv v \equiv k \pmod{p}$. As such, if we let D' be the complimentary difference set in G to D, and suppose it has parameters (v', k', λ'), then $p|\lambda'$, and as such $G - D$ obeys the hypothesis of Case (i). As such, it must be true that:

$$(G-D)^{p-1}+\left(G-D^{(-1)}\right)\equiv 1-v^{p-2}G\ (\mathrm{mod}\ p^2).$$

We will refer to the above as "$\dagger$". Since $(G-D)G = (v-k)G$, we can write:

$$(G-D)^{p-1}\equiv -D(G-D)^{p-2}\equiv\cdots\equiv(-D)^{p-2}(G-D)\equiv -k^{p-2}G+D^{p-1}\ (\mathrm{mod}\ p).$$

It is now also clear that $\left(G - \left(D^{(-1)}\right)\right)^{p-1} - k^{p-2}G + \left(D^{(-1)}\right)^{p-1} \pmod p$. Substituting into † and rearranging gives:

$$D^{p-1} + \left(D^{(-1)}\right)^{p-1} \equiv 1 + (2k^{p-2} - v^{p-2})G \equiv 1 + v^{p-2}G \pmod p,$$

where the last equivalence comes from the fact that $v \equiv k \pmod p$. Our proof of Wilbrink's Theorem is now complete. □

Proof D (See Theorem 7.26). To reiterate, this is the proof given by Xiang and co-authors [98]. Let χ be a non-trivial character of $\mathbb{F}_q$, and let the image of τ with $\{0\}$ removed be denoted as D_k. Since D_k is a hyperoval, we know that τ is precisely two-to-one by Lemma 7.25. As such, working over $\mathbb{Z}\mathbb{F}_q$ we can write:

$$\chi^\star(D_k) = \frac{1}{2}\sum_{x\in\mathbb{F}_q} \chi^\star(x + x^h) = \frac{1}{2}\sum_{x\in\mathbb{F}_q} \chi^\star(x)\chi^\star(1 + x^{h-1}).$$

By Lemma 7.25, we also know that $q-1$ and $h-1$ are coprime. As such, there must exist a non-trivial character χ' of $\mathbb{F}_q$ such that $\chi = \chi'^{q-1}$. Then the above can be written as:

$$\frac{1}{2}\sum_{x\in\mathbb{F}_q} \chi'^\star(x^{h-1})\chi^\star(1 + x^{h-1}).$$

This last expression is precisely half of the Jacobi sum for χ and χ'. Since the Jacobi sum is always equal to q, which is a power of two by hypothesis, we have $\chi^\star(D_k)\overline{\chi^\star(D_k)} = \frac{q}{4}$, and by Theorem 8.8, we are done. □