Linking Systems of Difference Sets

by

Samuel Simon

B.Sc., Carnegie Mellon University, 2015

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Summer 2017

Approval

Name:	**Samuel Simon**
Degree:	**Master of Science (Mathematics)**
Title:	***Linking Systems of Difference Sets***
Examining Committee:	**Chair:** Tom Archibald Professor

Jonathan Jedwab
Senior Supervisor
Professor _____

Marni Mishna
Co-Supervisor
Associate Professor _____

Petr Lisoněk
Internal Examiner
Professor _____

Date Defended: August 11 2017

Abstract

A linking system of difference sets is a collection of mutually related group difference sets, whose advantageous properties have been used to extend classical constructions of systems of linked symmetric designs. The central problems are to determine which groups contain a linking system of difference sets, and how large such a system can be. All previous results are constructive, and are restricted to 2-groups. We use an elementary projection argument to show that neither the McFarland nor the Spence construction of difference sets can give rise to a linking system of difference sets in non-2-groups. We then give a new construction for linking systems of difference sets in 2-groups, taking advantage of a previously unrecognized connection with group difference matrices. This construction simplifies and extends prior results, producing larger systems than before in certain 2-groups and new linking systems in other 2-groups for which no system was previously known.

Keywords: Construction, Difference Set, Difference Matrix, Infinite Family, Linking System, Nonexistence

Acknowledgements

This research was partially funded through my committee members. I appreciate the funding I received through SFU, including the C.D. Nelson Memorial Graduate Entrance Scholarship and Provost Prize of Distinction.

I have received various forms of support from many people which ultimately led to the completion of my thesis.

I would like to thank Shuxing Li for being a principal (but nontrivial) character throughout the many sessions working on my thesis problems and his contributions to the results. I appreciate the help of Ken Smith in proving Proposition 1.7 and in formulating Corollary 4.6.

Thank you to Marni for her valuable contributions in the editing process and providing constant motivation (so that I can start my PhD with her).

Thank you to Petr Lisoněk for examining my thesis in remarkable detail.

Thank you to Tara for graduating a semester before me to show that finishing a Masters thesis with Jonathan *can* be done, and to Adam for suffering alongside me.

Thank you to my sister, who at a young age taught me math until it annoyed her. Thank you to my parents, who have encouraged and enabled my love of math.

Thanks to all my friends and family who provided various distractions throughout my studies (and therefore any errors here are your responsibility).

Lastly, thank you to my advisor Jonathan who has taught me things from background on difference sets to different writing styles to the difference in certain homophones (which I should have known already). I have been convinced that if he were granted immortality, he could spend an eternity creating an infinite sequence of thesis drafts, which would eventually simply permute the phrasing of various statements, each of which I never had a preference. Finally, thank you for compl-e-menting (and occasionally compl-i-menting) my work.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Difference Sets

The study of difference sets lies at the intersection of combinatorics, finite geometry, and coding theory. The structures are defined in the combinatorial sense of counting objects, although many examples are constructed from objects in geometry such as hyperplanes. Advantageous properties of difference sets enable the solution of problems in radar, optical image alignment, and other areas of digital communication. A comprehensive survey of difference sets is given by Jungnickel [Jun92], with updates in [JS97] and [JS98]. Difference sets occur within the larger context of the theory of experimental design, as pioneered in 1926 by Fisher [Fis26]. Indeed, difference sets are highly structured examples of combinatorial designs: a (v, k, λ, n)-difference set in a group G is equivalent to a symmetric (v, k, λ, n)-design with a regular automorphism group G [Che98].

Classical constructions of difference sets were given by Paley [Pal33] and Singer [Sin38]. Turyn [Tur65] introduced the systematic use of character theory to study constructions and nonexistence of difference sets in abelian groups. The study of difference sets in nonabelian groups often uses representation theory. Ryser [Rys63] and Hall [Hal67] situated difference sets in the broader context of combinatorial theory.

Definition 1.1. Let G be a group of order v, written multiplicatively, and let D be a subset of G with k elements. Then D is a (v, k, λ, n)-**difference set in** G if the multiset $\{d_1 d_2^{-1} : d_1, d_2 \in D \text{ and } d_1 \neq d_2\}$ contains every non-identity element of G exactly λ times. In this case, we define $n := k - \lambda$.

The central problems are to determine which groups contain a difference set, and to enumerate all inequivalent examples in such groups. Many of the known difference sets have been organized into families according to the form of their parameters (v, k, λ, n) [Jun92]. The parameter n is often considered to be the most fundamental of the four parameters [Ass89].

Jungnickel and Schmidt [JS97] proposed a classification of the known families of difference sets into three classes: those with Singer parameters; cyclotomic difference sets; and difference sets with $\gcd(v, n) > 1$. The construction methods for the three classes are notably different. The Singer difference sets [Sin38] can be obtained from the action of a cyclic group of linear transformations on the one-dimensional subspaces of a finite field. The cyclotomic difference sets are unions of cosets of multiplicative subgroups of finite fields. Lastly, the five known families of difference sets with $\gcd(v, n) > 1$ share common structure and construction methods, as shown in [DJ97] for the Hadamard [Men62], McFarland [McF73], Spence [Spe77], and Davis-Jedwab [DJ97] families, and as subsequently extended to the Chen family [Che97]. Table 1.1 describes these parameter families.

Family	v	k	λ	n
McFarland	$q^{d+1}\left(\frac{q^{d+1}-1}{q-1}+1\right)$	$q^d\left(\frac{q^{d+1}-1}{q-1}\right)$	$q^d\left(\frac{q^d-1}{q-1}\right)$	q^{2d}
Hadamard	$4N^2$	$N(2N-1)$	$N(N-1)$	N^2
Spence	$3^{d+1}\left(\frac{3^{d+1}-1}{2}\right)$	$3^d\left(\frac{3^{d+1}+1}{2}\right)$	$3^d\left(\frac{3^d+1}{2}\right)$	3^{2d}
Davis-Jedwab	$2^{2d+4}\left(\frac{2^{2d+2}-1}{3}\right)$	$2^{2d+1}\left(\frac{2^{2d+3}+1}{3}\right)$	$2^{2d+1}\left(\frac{2^{2d+1}+1}{3}\right)$	2^{4d+2}
Chen	$4q^{2d+2}\left(\frac{q^{2d+2}-1}{q^2-1}\right)$	$q^{2d+1}\left(\frac{2(q^{2d+2}-1)}{q+1}+1\right)$	$q^{2d+1}(q-1)\left(\frac{q^{2d+1}+1}{q+1}\right)$	q^{4d+2}

Table 1.1: Parameter families for difference sets where q is a prime power, N is a positive integer, and d is a nonnegative integer.

For each prime power q and nonnegative integer d, there exist difference sets in the McFarland, Spence, and Davis-Jedwab families. For the Hadamard family, existence is known when N is a product of powers of 2 or 3 or p^2, where p is a prime greater than 3. For the Chen family, existence is known for all d when q is a power of 2 or 3 or p^2, where p is a prime greater than 3.

The Hadamard and McFarland families intersect in the 2-groups (those groups whose order is a power of 2): the Hadamard parameters with $N = 2^d$ are the same as the McFarland parameters with $q = 2$. Furthermore, the parameters of a (nontrivial) difference set in a 2-group necessarily take this form, as shown in the following result.

Theorem 1.2 (Beth, Jungnickel, and Lenz [BJL99, Theorem II 3.17])**.** *Suppose a group G of order 2^r contains a (v, k, λ, n)-difference set where $2 \le k \le \frac{v}{2}$. Then $r = 2d+2$ for some $d \ge 0$ and*

$$(v, k, \lambda, n) = \left(2^{2d+2}, 2^d(2^{d+1}-1), 2^d(2^d-1), 2^{2d}\right).$$

The 2-groups give rise to many difference sets, and have been well studied. In particular, Theorem 1.3 gives necessary and sufficient conditions for the existence of a difference set in an abelian 2-group. This result, proved using character theory, was the culmination of

decades of research by many authors. Write $\exp(G)$ for the **exponent** of G, defined as the smallest positive integer α for which $g^\alpha = \mathbf{1}_G$ for all $g \in G$.

Theorem 1.3 (Kraemer [Kra93]). *A difference set exists in an abelian group G of order 2^{2d+2} if and only if $\exp(G) \leq 2^{d+2}$.*

Theorem 1.3 gives conditions for McFarland parameters with $q = 2$. For the McFarland parameters with $q = 4$, Davis-Jedwab [DJ97] and Ma-Schmidt [MS97] showed that a difference set exists in an abelian group G if and only if the Sylow 2-subgroup of G has exponent at most 4. This result, and Theorem 1.3 are the only two known results which determine both necessary and sufficient conditions for the existence of a difference set in a parameter family.

Example 1.4. Let $G = \mathbb{Z}_2^2 = \langle x, y \rangle$ and $D = \{x, y, xy\}$. The multiset of differences formed from D is

$$\left\{xy^{-1}, x(xy)^{-1}, yx^{-1}, y(xy)^{-1}, (xy)x^{-1}, (xy)y^{-1}\right\} = \{xy, y, xy, x, y, x\} = \{x, x, y, y, xy, xy\}.$$

We see that G is a group of order 4 containing a subset D of 3 elements, such that the multiset of differences contains every non-identity element of G exactly 2 times. Therefore, D is a $(4, 3, 2, 1)$-difference set in G.

Now we introduce group ring notation. By a common notation convention, we identify a multiset of elements of the group G with its corresponding element in the group ring $\mathbb{Z}[G]$. For example, if we represent the multiset $\{x, x, xy\}$ of elements of the group $G = \langle x, y \rangle$ as S, then we also represent the corresponding element $x + x + xy = 2x + xy$ of the group ring $\mathbb{Z}[G]$ as S. Thus, the group ring element G represents the sum of all elements of the group G. Given a multiset S of elements of the group G, we write $S^{(-1)}$ for the group ring element $\sum_{d \in S} d^{-1}$, where the sum is over the elements in the multiset S, and the inverse is taken in G.

Lemma 1.5 (Group Ring Relations). *Let G be a group and let $S, T \in \mathbb{Z}[G]$. Then*

$$\left(S^{(-1)}\right)^{(-1)} = S \tag{1.1}$$

$$S = T \iff S^{(-1)} = T^{(-1)} \tag{1.2}$$

$$ST^{(-1)} = \sum_{s \in S, t \in T} st^{-1} \tag{1.3}$$

$$(ST)^{(-1)} = T^{(-1)} S^{(-1)} \tag{1.4}$$

Proof. The first three relations follow immediately from the definition of $S^{(-1)}$. For the fourth relation we have

$$(ST)^{(-1)} = \sum_{s \in S, t \in T} (st)^{-1} = \sum_{s \in S, t \in T} t^{-1} s^{-1} = T^{(-1)} S^{(-1)}. \tag{1.5}$$

□

Lemma 1.6. *Let G be a group of order v and D a subset of G with k elements. Then D is a (v, k, λ, n)-difference set in G if and only if*

$$DD^{(-1)} = n\mathbf{1}_G + \lambda G \quad \text{in } \mathbb{Z}[G]. \tag{1.6}$$

Proof. Use the definition of a difference set with (1.3) and the relation $n = k - \lambda$. □

Note that the number of elements on both sides of (1.6) must be equal, giving the following relationship between the parameters (v, k, λ, n) of a difference set:

$$k^2 = n + \lambda v. \tag{1.7}$$

Using group ring notation, the verification given in Example 1.4 becomes

$$\begin{aligned} DD^{(-1)} &= (x + y + xy)(x^{-1} + y^{-1} + (xy)^{-1}) \\ &= 3 \cdot \mathbf{1}_G + 2(x + y + xy) \\ &= \mathbf{1}_G + 2G. \end{aligned}$$

It is straightforward to verify that the complement of a (v, k, λ, n)-difference set in a group G is a $(v, v - k, v - 2k + \lambda, n)$-difference set in G, and so we may assume $k \leq \frac{v}{2}$. We also consider the cases $k = 0$ and $k = 1$ to be trivial (and this accounts for the condition $2 \leq k \leq \frac{v}{2}$ in Theorem 1.2). We may interpret Example 1.4 as the complement of a trivial $(4, 1, 0, 1)$-difference set.

Proposition 1.7. *Suppose D is a (v, k, λ, n)-difference set in a (not necessarily abelian) group G. Then $D^{(-1)}$ is also a (v, k, λ, n)-difference set in G.*

Proof. Since D is a (v, k, λ, n) difference set in G, by Lemma 1.6 we have

$$DD^{(-1)} - \lambda G = n\mathbf{1}_G \quad \text{in } \mathbb{Z}[G].$$

For $g \in G$ we have $gG = G$ in $\mathbb{Z}[G]$, so for $S \subset G$ we have $SG = |S|G$ in $\mathbb{Z}[G]$. Therefore, $DG = kG$ and so

$$D\left(D^{(-1)} - \frac{\lambda}{k}G\right)\frac{1}{n} = \mathbf{1}_G.$$

Therefore D has a right inverse $A = \left(D^{(-1)} - \frac{\lambda}{k}G\right)\frac{1}{n}$ in $\mathbb{R}[G]$. Since G is a finite group, $\mathbb{R}[G]$ is a semisimple ring [Lam01, p. 118] and so A is also a left inverse of D in $\mathbb{R}[G]$ [Lam01, Ex. 3.10].

Since $\mathbf{1}_G$ and G are in the center of $\mathbb{R}[G]$,

$$\begin{aligned} D^{(-1)}D = (AD)D^{(-1)}D &= A(DD^{(-1)})D \\ &= A(n\mathbf{1}_G + \lambda G)D \\ &= AD(n\mathbf{1}_G + \lambda G) \\ &= n\mathbf{1}_G + \lambda G. \end{aligned}$$

Furthermore, $D^{(-1)}$ is a subset of G with k elements and so by Lemma 1.6 and (1.1), $D^{(-1)}$ is a (v, k, λ, n)-difference set in G. □

1.2 Character Theory

Character theory, and in particular Theorem 1.13 below, has become the standard tool for studying constructive and nonexistence results for difference sets in abelian groups. We now give an overview of this theory for completeness, although the contents of this section are not needed for the rest of the thesis.

Definition 1.8. A **character** of a finite abelian group G is a homomorphism χ from G to the complex numbers $\mathbb{C}$.

We multiply characters χ_1, χ_2 of G according to

$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g) \text{ for all } g \in G.$$

Under this multiplication, the characters of G form a group $\widehat{G}$, which is isomorphic to G. The **principal** character χ_0 of G, defined by $\chi_0(g) = 1$ for all $g \in G$, is the identity of $\widehat{G}$. We say that all other characters are nonprincipal. For a multiset S of elements of an abelian group G, we write $\chi(S)$ to mean $\sum_{s\in S}\chi(s)$.

Since a character χ is a homomorphism, the identity $\mathbf{1}_G$ must be mapped to 1. Similarly, if g is an element of G of order k, then $\chi(g)^k = 1$. Thus, χ maps elements of G onto the complex roots of unity.

The following orthogonality relations are fundamental in character theory.

Lemma 1.9 (Orthogonality Relations)**.** *For an abelian group G,*

$$\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = \mathbf{1}_G \\ 0 & \text{if } g \neq \mathbf{1}_G \end{cases} \tag{1.8}$$

$$\sum_{g\in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0. \end{cases} \tag{1.9}$$

Proof. We first prove (1.8). Since χ is a homomorphism, we have $\chi(\mathbf{1}_G) = 1$ for each $\chi \in \widehat{G}$, so

$$\sum_{\chi \in \widehat{G}} \chi(\mathbf{1}_G) = |\widehat{G}| = |G|.$$

Now take $g \neq \mathbf{1}_G$ and choose $\chi^* \in \widehat{G}$ so that $\chi^*(g) \neq 1$. Then

$$\chi^*(g) \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} (\chi^* \chi)(g),$$

by the definition of character multiplication. As χ runs through $\widehat{G}$, the character $\chi^*\chi$ also runs through $\widehat{G}$ because $\widehat{G}$ is a group under character multiplication. Hence,

$$\chi^*(g) \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \chi(g).$$

Thus, we have

$$(\chi^*(g) - 1) \sum_{\chi \in \widehat{G}} \chi(g) = 0.$$

Since $\chi^*(g) \neq 1$ by assumption, this implies that the complex number $\sum_{\chi \in \widehat{G}} \chi(g)$ is 0.

Now we prove (1.9). Since $\chi_0(g) = 1$ for all $g \in G$, we have $\sum_{g \in G} \chi_0(g) = |G|$. For $\chi \neq \chi_0$, choose $g^* \in G$ such that $\chi(g^*) \neq 1$ and then

$$\begin{aligned} \chi(g^*) \sum_{g \in G} \chi(g) &= \sum_{g \in G} \chi(g^* g) \\ &= \sum_{g \in G} \chi(g) \end{aligned}$$

and so $\sum_{g \in G} \chi(g)$ is 0. □

Lemma 1.10. *Let G be an abelian group and let $A \in \mathbb{Z}[G]$ and $\chi \in \widehat{G}$. Then*

$$\chi\left(AA^{(-1)}\right) = |\chi(A)|^2. \tag{1.10}$$

Proof. For all $g \in G$ we have

$$\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$$

because χ is a homomorphism and $\chi(g)$ is a complex root of unity. Therefore, we have

$$\chi(A^{(-1)}) = \overline{\chi(A)}$$

and so

$$\chi\left(AA^{(-1)}\right) = \chi(A)\chi(A^{(-1)}) = \chi(A)\overline{\chi(A)} = |\chi(A)|^2.$$

□

Theorem 1.11 (Fourier Inversion Formula)**.** *Let G be an abelian group and let*

$$A = \sum_{g \in G} a_g g \in \mathbb{Z}[G].$$

Then

$$a_g = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(A)\overline{\chi(g)} \text{ for all } g \in G.$$

Proof. Write $A = \sum_{h \in G} a_h h$ and fix $g \in G$ and let $\chi \in \widehat{G}$. Then

$$\begin{aligned} \chi(A)\overline{\chi(g)} &= \left(\sum_{h \in G} a_h \chi(h) \right) \overline{\chi(g)} \\ &= \sum_{h \in G} a_h \chi(hg^{-1}), \end{aligned}$$

using $\overline{\chi(g)} = \chi(g^{-1})$. Sum over $\chi \in \widehat{G}$ to get

$$\begin{aligned} \sum_{\chi \in \widehat{G}} \chi(A)\overline{\chi(g)} &= \sum_{h \in G} a_h \sum_{\chi \in \widehat{G}} \chi(hg^{-1}) \\ &= a_g |G| \end{aligned}$$

because by (1.8) we have $\sum_{\chi \in \widehat{G}} \chi(hg^{-1}) = 0$ unless $hg^{-1} = \mathbf{1}_G$. Dividing both sides by $|G|$ finishes the proof. □

Lemma 1.12. *Let G be an abelian group, and suppose $A \in \mathbb{Z}[G]$ satisfies $\chi(A) = 0$ for all $\chi \neq \chi_0$. Then $A = c\,G$ for some integer c.*

Proof. Let $A = \sum_{g \in G} a_g g$ where each $a_g \in \mathbb{Z}$. From the Fourier Inversion Formula we have for all $g \in G$,

$$\begin{aligned} a_g = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(A)\overline{\chi(g)} &= \frac{1}{|G|} \chi_0(A)\overline{\chi_0(g)} \\ &= \frac{1}{|G|} \chi_0(A) \cdot 1 \end{aligned}$$

which is independent of g. So for some integer c we have $a_g = c$ for all $g \in G$ and therefore

$$A = \sum_{g \in G} cg = c\,G.$$

□

Theorem 1.13. *Let G be an abelian group of order v, and D a subset of G of size k. Then D is a (v, k, λ, n)-difference set in G if and only if $|\chi(D)| = \sqrt{n}$ for all $\chi \neq \chi_0$.*

Proof. First we prove the forward direction. Apply $\chi \neq \chi_0$ to (1.6) to give

$$\chi\left(DD^{(-1)}\right) = n + \lambda\chi(G).$$

Use Lemma 1.10 and (1.9) to give $|\chi(D)|^2 = n$.

We now prove the reverse direction. For all $\chi \neq \chi_0$, by Lemma 1.10 we have

$$\chi\left(DD^{(-1)} - n\mathbf{1}_G\right) = |\chi(D)|^2 - n = 0.$$

So by Lemma 1.12,

$$DD^{(-1)} - n\mathbf{1}_G = c\,G$$

for some integer c. By counting terms on both sides we get $k^2 - n = cv$, which implies that $c = \lambda$ from (1.7). The result follows from Lemma 1.6. □

We now show how Theorem 1.13 can be used to verify that a subset of an abelian group is a difference set.

Example 1.14. Let $G = \mathbb{Z}_4^2 = \langle x, y\rangle$ and let $D = x + x^3y + y^3 + xy^2 + xy + x^2y$. By Theorem 1.13, D is a $(16, 6, 2, 4)$-difference set in G provided $|\chi(D)| = 2$ for each nonprincipal character χ of G. For $0 \leq a, b \leq 3$, define $\chi_{a,b} \in \widehat{G}$ to be the map

$$x \mapsto i^a \text{ and } y \mapsto i^b \quad \text{where } i^2 = -1.$$

The set $\{\chi_{a,b} : 0 \leq a, b \leq 3\}$, along with the operation of character multiplication, forms the group $\widehat{G}$. We now evaluate each $\chi_{a,b}(D)$. For example,

$$\begin{aligned}\chi_{1,2}(D) &= \chi_{1,2}(x + x^3y + y^3 + xy^2 + xy + x^2y)\\ &= i + i - 1 + i - i + 1\\ &= 2i.\end{aligned}$$

The entry indexed by (a, b) in the following table is $\chi_{a,b}(D)$.

		b			
		0	1	2	3
a	0	6	$2i$	-2	$-2i$
	1	$2i$	$-2i$	$2i$	$2i$
	2	-2	$-2i$	-2	$2i$
	3	$-2i$	$-2i$	$-2i$	$2i$

For each nonprincipal $\chi_{a,b}$, we have $|\chi_{a,b}(D)| = 2$, so D is a difference set.

1.3 Linking Systems of Difference Sets

A linking system of difference sets was introduced in [DMP14]. Such a system gives rise to a system of linked symmetric designs, which is equivalent to a particular kind of association scheme [vD99].

Definition 1.15. Let G be a group of order v, written multiplicatively, and let $\ell \geq 2$. Suppose $\mathcal{L} = \{D_{i,j} : 0 \leq i, j \leq \ell \text{ and } i \neq j\}$ is a collection of size $\ell(\ell+1)$ of (v, k, λ, n)-difference sets in G. Then $\mathcal{L}$ is a $(v, k, \lambda, n; \ell+1)$**-linking system of difference sets in** G if there are integers μ, ν such that for all distinct i, j, h, the following equations hold in $\mathbb{Z}[G]$:

$$D_{h,i}D_{i,j} = (\mu - \nu)D_{h,j} + \nu G \tag{1.11}$$

$$D_{i,j} = D_{j,i}^{(-1)}. \tag{1.12}$$

The central problems are to determine which groups contain a linking system of difference sets, and how large such a system can be. As noted in [DMP14], it follows from [Nod74] that the integers μ, ν in Definition 1.15 are determined to within a sign as

$$\nu = \frac{k(k \pm \sqrt{n})}{v} \text{ and } \mu = \nu \mp \sqrt{n} \tag{1.13}$$

(where we have corrected a typographical error in [DMP14]). Definition 1.15 is rather cumbersome to work with. We define a simpler object in Definition 1.16 and show in Proposition 1.18 that it is equivalent to a linking system of difference sets. An outline of the main argument of the proof is implicit in [DMP14], although many details are omitted and particular care is needed when the group G is nonabelian.

Definition 1.16. Let G be a group of order v, written multiplicatively, and let $\ell \geq 2$. Suppose $\mathcal{R} = \{D_1, D_2, \cdots, D_\ell\}$ is a collection of size ℓ of (v, k, λ, n)-difference sets in G. Then $\mathcal{R}$ is a **reduced** $(v, k, \lambda, n; \ell)$**-linking system of difference sets in** G if there are integers μ, ν such that for all distinct i, j there is some (v, k, λ, n)-difference set $D(i, j)$ in G satisfying

$$D_i D_j^{(-1)} = (\mu - \nu)D(i, j) + \nu G \quad \text{ in } \mathbb{Z}[G]. \tag{1.14}$$

Note that the difference set $D(i, j)$ is not necessarily contained in the collection $\mathcal{R}$. We next show that the parameters μ, ν in a reduced linking system of difference sets take the same values as those in (1.13) for a (non-reduced) linking system.

Lemma 1.17. *Suppose $\{D_1, D_2, \cdots, D_\ell\}$ is a reduced $(v, k, \lambda, n; \ell)$-linking system of difference sets in a group G with respect to integers μ, ν. Then*

$$\nu = \frac{k(k \pm \sqrt{n})}{v} \text{ and } \mu = \nu \mp \sqrt{n}.$$

Proof. Choose distinct i, j satisfying $1 \le i, j \le \ell$. By Definition 1.16 there is a (v, k, λ, n)-difference set $D(i, j)$ in G such that

$$D_i D_j^{(-1)} = (\mu - \nu)D(i, j) + \nu G \quad \text{in } \mathbb{Z}[G]. \tag{1.15}$$

Apply the operation $^{(-1)}$ to both sides of (1.15) and use Lemma 1.5 and the relation $G = G^{(-1)}$ to obtain

$$D_j D_i^{(-1)} = (\mu - \nu)D(i, j)^{(-1)} + \nu G. \tag{1.16}$$

For $S \subset G$ we have $SG = GS = |S|G$ in $\mathbb{Z}[G]$. Combining (1.15) and (1.16) gives

$$\begin{aligned}\Big((\mu - \nu)D(i, j)\Big)\Big((\mu - \nu)D(i, j)^{(-1)}\Big) &= \Big(D_i D_j^{(-1)} - \nu G\Big)\Big(D_j D_i^{(-1)} - \nu G\Big) \\ &= D_i \Big(D_j^{(-1)} D_j\Big) D_i^{(-1)} - 2\nu k^2 G + \nu^2 v G. \end{aligned} \tag{1.17}$$

Now D_i and D_j and $D(i, j)$ are each (v, k, λ, n)-difference sets in G, and by Proposition 1.7 so is $D_j^{(-1)}$. Using Lemma 1.6 we therefore find from (1.17) that

$$\begin{aligned}(\mu - \nu)^2(n\mathbf{1}_G + \lambda G) &= D_i(n\mathbf{1}_G + \lambda G)D_i^{(-1)} - 2\nu k^2 G + \nu^2 v G \\ &= (n\mathbf{1}_G + \lambda G)^2 - 2\nu k^2 G + \nu^2 v G\end{aligned}$$

because $\mathbf{1}_G$ and G commute with D_i. Since the coefficients of $G - \mathbf{1}_G$ on both sides must be equal, comparison of the coefficients of $\mathbf{1}_G$ shows that

$$\mu - \nu = \mp\sqrt{n}. \tag{1.18}$$

Counting terms on both sides of (1.15) then gives

$$\begin{aligned}k^2 &= (\mu - \nu)k + \nu v \\ &= \mp\sqrt{n}k + \nu v,\end{aligned}$$

which together with (1.18) establishes the required values for μ and ν. □

Proposition 1.18. *Let μ, ν be integers. A $(v, k, \lambda, n; \ell+1)$-linking system of difference sets in a group G with respect to μ, ν is equivalent to a reduced $(v, k, \lambda, n; \ell)$-linking system of difference sets in G with respect to μ, ν.*

Proof. Let $\mathcal{L} = \{D_{i,j} : 0 \le i,j \le \ell \text{ and } i \ne j\}$ be a $(v,k,\lambda,n;\ell+1)$-linking system of difference sets in G with respect to μ,ν. Let $D_i = D_{i,0}$ for $1 \le i \le \ell$ and let $\mathcal{R} = \{D_1, D_2, \cdots, D_\ell\}$. Then for all distinct i,j,

$$D_i D_j^{(-1)} = D_{i,0} D_{j,0}^{(-1)} = D_{i,0} D_{0,j} = (\mu-\nu) D_{i,j} + \nu G$$

using (1.12) and (1.11). Therefore $\mathcal{R}$ is a reduced $(v,k,\lambda,n;\ell)$-linking system of difference sets in G with respect to μ,ν.

Conversely, let $\mathcal{R} = \{D_1, D_2, \cdots, D_\ell\}$ be a reduced $(v,k,\lambda,n;\ell)$-linking system of difference sets in G with respect to μ,ν. Let $D_{i,0} = D_i$ and $D_{0,i} = D_i^{(-1)}$ for $1 \le i \le \ell$. For distinct i,j not equal to 0, let $D_{i,j}$ be the difference set $D(i,j)$ given by Definition 1.16 applied to $D_{i,0}$ and $D_{j,0}$, so that

$$D_{i,0} D_{j,0}^{(-1)} = (\mu-\nu) D_{i,j} + \nu G. \tag{1.19}$$

We shall show that $\mathcal{L} = \{D_{i,j} : 0 \le i,j \le \ell \text{ and } i \ne j\}$ is a $(v,k,\lambda,n;\ell+1)$-linking system of difference sets in G with respect to μ,ν by showing that (1.12) and (1.11) hold.

To show (1.12) for distinct i,j, one of which is 0, use the definition of $D_{i,0}$ and $D_{0,i}$. To show (1.12) for distinct i,j both of which are not 0, apply the operation $^{(-1)}$ to both sides of (1.19) and use Lemma 1.5 to obtain

$$D_{j,0} D_{i,0}^{(-1)} = (\mu-\nu) D_{i,j}^{(-1)} + \nu G.$$

Interchange i,j to get

$$D_{i,0} D_{j,0}^{(-1)} = (\mu-\nu) D_{j,i}^{(-1)} + \nu G.$$

By comparison with (1.19), we conclude that $D_{i,j} = D_{j,i}^{(-1)}$, giving (1.12).

To show (1.11) for distinct i,j,h all of which are not 0, use (1.19) to form the product

$$\Big((\mu-\nu) D_{h,i}\Big)\Big((\mu-\nu) D_{i,j}\Big) = \Big(D_{h,0} D_{i,0}^{(-1)} - \nu G\Big)\Big(D_{i,0} D_{j,0}^{(-1)} - \nu G\Big). \tag{1.20}$$

From Lemma 1.17 we have $(\mu-\nu)^2 = n$. Since $D_{i,0}$ is a (v,k,λ,n)-difference set in G, by Proposition 1.7 so is $D_{i,0}^{(-1)}$. Therefore from Lemmas 1.5 and 1.6 we have

$$D_{i,0}^{(-1)} D_{i,0} = n\mathbf{1}_G + \lambda G.$$

Therefore (1.20) gives

$$\begin{aligned} n D_{h,i} D_{i,j} &= D_{h,0}(n\mathbf{1}_G + \lambda G) D_{j,0}^{(-1)} - 2\nu k^2 G + \nu^2 v G \\ &= n D_{h,0} D_{j,0}^{(-1)} + \lambda k^2 G - 2\nu k^2 G + \nu^2 v G. \end{aligned}$$

But from Lemma 1.17 and (1.7), ν is a solution to the quadratic equation

$$\lambda k^2 - 2\nu k^2 + \nu^2 v = 0$$

and so we conclude that

$$\begin{aligned} D_{h,i}D_{i,j} &= D_{h,0}D_{j,0}^{(-1)} \\ &= (\mu - \nu)D_{h,j} + \nu G, \end{aligned}$$

using (1.19) again, as required for (1.11).

It remains to show (1.11) for distinct i, j, h, exactly one of which is 0. The case $i = 0$ follows from the definition of $D_{h,j}$. We now outline the case $h = 0$; the case $j = 0$ is similar. From (1.19) we have

$$\begin{aligned} (\mu - \nu)D_{0,i}D_{i,j} &= D_i^{(-1)}(D_i D_j^{(-1)} - \nu G) \\ &= (n\mathbf{1}_G + \lambda G)D_j^{(-1)} - \nu k G \\ &= nD_{0,j} + k(\lambda - \nu)G \\ &= (\mu - \nu)^2 D_{0,j} + k(\lambda - \nu)G, \end{aligned}$$

which gives (1.11) provided

$$k(\lambda - \nu) = \nu(\mu - \nu).$$

This relation follows from (1.7) and Lemma 1.17 because

$$\begin{aligned} k(\lambda - \nu) &= \frac{k}{v}(k^2 - n) - k\nu \\ &= \frac{k}{v}(k \pm \sqrt{n})(k \mp \sqrt{n}) - k\nu \\ &= \nu(k \mp \sqrt{n}) - k\nu \\ &= \mp\nu\sqrt{n} \\ &= \nu(\mu - \nu). \end{aligned}$$

□

We now give an example of a reduced linking system of difference sets in $\mathbb{Z}_2^4$.

Example 1.19. Let $G = \mathbb{Z}_2^4 = \langle x, y, z, w \rangle$, and let $D_1 = \mathbf{1}_G + xy + yz + xyz + w + yw$ and $D_2 = x + xy + z + xyz + w + xw$. We represent each of the sets D_1 and D_2 by a $2 \times 2 \times 2 \times 2$ grid, highlighting the grid cells whose elements are contained in the set.

D_1

$\mathbf{1}_G$	y	z	yz
x	xy	xz	xyz
w	yw	zw	yzw
xw	xyw	xzw	$xyzw$

D_2

$\mathbf{1}_G$	y	z	yz
x	xy	xz	xyz
w	yw	zw	yzw
xw	xyw	xzw	$xyzw$

By calculation of $D_1 D_1^{(-1)}$ and $D_2 D_2^{(-1)}$ we verify that D_1 and D_2 are each a $(16, 6, 2, 4)$-difference set in G. Now compute

$$\begin{aligned} D_1 D_2^{(-1)} &= (\mathbf{1}_G + xy + yz + xyz + w + yw)\,(x + xy + z + xyz + w + xw) \\ &= (yz + xz + w + yw + zw + xzw) + \\ &\quad 3\,(\mathbf{1}_G + x + y + xy + z + xyz + xw + xyw + yzw + xyzw) \\ &= -2D + 3G, \end{aligned}$$

where $D = yz + xz + w + yw + zw + xzw$, and verify from $DD^{(-1)}$ that D is a $(16, 6, 2, 4)$-difference set in G.

D

$\mathbf{1}_G$	y	z	yz
x	xy	xz	xyz
w	yw	zw	yzw
xw	xyw	xzw	$xyzw$

It follows from Lemma 1.5 that $D_2 D_1^{(-1)} = -2D^{(-1)} + 3G$, and $D^{(-1)}$ is also a $(16, 6, 2, 4)$-difference set in G by Proposition 1.7. Therefore $\{D_1, D_2\}$ is a reduced $(16, 6, 2, 4; 2)$-linking system of difference sets in G with $\mu = 1$ and $\nu = 3$.

Definition 1.20. A difference set D satisfying $D = D^{(-1)}$ is **reversible**.

The difference sets in Example 1.19 are trivially reversible because every element of $\mathbb{Z}_2^4$ is its own inverse, so every subset S has the property $S = S^{(-1)}$. We now give an example of a reduced system of linking difference sets in $\mathbb{Z}_4^2$, not all of which are reversible.

Example 1.21 ([DMP14, Example 6.3]). Let $G = \mathbb{Z}_4^2 = \langle x, y \rangle$ and let

$$\begin{aligned} D_1 &= x + x^3y + y^3 + x^3 + xy^3 + y \\ D_2 &= x + x^3y + y^3 + xy^2 + xy + x^2y \\ D_3 &= x + x^3y + y^3 + x^2y^3 + x^3y^3 + x^3y^2. \end{aligned}$$

D_1

$\mathbf{1}_G$	y	y^2	y^3
x	xy	xy^2	xy^3
x^2	x^2y	x^2y^2	x^2y^3
x^3	x^3y	x^3y^2	x^3y^3

D_2

$\mathbf{1}_G$	y	y^2	y^3
x	xy	xy^2	xy^3
x^2	x^2y	x^2y^2	x^2y^3
x^3	x^3y	x^3y^2	x^3y^3

D_3

$\mathbf{1}_G$	y	y^2	y^3
x	xy	xy^2	xy^3
x^2	x^2y	x^2y^2	x^2y^3
x^3	x^3y	x^3y^2	x^3y^3

We check that $D_i D_i^{(-1)} = 4 \cdot \mathbf{1}_G + 2G$ for each i to verify that each D_i is a difference set in G. We then compute

$$\begin{aligned} D_2 D_1^{(-1)} &= \left(x + x^3y + y^3 + xy^2 + xy + x^2y\right)\left(x^3 + xy^3 + y + x + x^3y + y^3\right) \\ &= \left(y^3 + x + x^2y^3 + x^3y + x^3y^2 + x^3y^3\right) + \\ &\quad 3\left(\mathbf{1}_G + y + y^2 + xy + xy^2 + xy^3 + x^2 + x^2y + x^2y^2 + x^3\right) \\ &= -2D + 3G, \end{aligned}$$

where $D = y^3 + x + x^2y^3 + x^3y + x^3y^2 + x^3y^3$ is a $(16, 6, 2, 4)$-difference set in G. Similar calculation for $D_3 D_1^{(-1)}$ and $D_3 D_2^{(-1)}$, together with Proposition 1.7, verifies that $\{D_1, D_2, D_3\}$ forms a reduced $(16, 6, 4, 2; 3)$-linking system of difference sets in G.

Note that D_1 is reversible, but neither D_2 nor D_3 is.

Definition 1.22. Let $\mathcal{L} = \{D_{i,j} : 0 \leq i, j \leq \ell \text{ and } i \neq j\}$ be a $(v, k, \lambda, n; \ell + 1)$-linking system of difference sets in a group G. If each difference set $D_{i,j}$ is reversible, then $\mathcal{L}$ is a **reversible** $(v, k, \lambda, n; \ell + 1)$**-linking system of difference sets in** G.

Definition 1.23. Let $\mathcal{R} = \{D_1, D_2, \cdots, D_\ell\}$ be a reduced $(v, k, \lambda, n; \ell)$-linking system of difference sets in a group G. If the corresponding linking system $\mathcal{L}$ (as defined in the proof of Proposition 1.18) is reversible, then $\mathcal{R}$ is a **reversible reduced** $(v, k, \lambda, n; \ell)$**-linking system of difference sets in** G.

1.4 Results due to Davis-Martin-Polhill

Davis, Martin, and Polhill [DMP14] provide one of the two principal references on linking systems of difference sets. All their results construct reduced linking systems of difference sets in abelian 2-groups, and all their examples are reversible except for the one presented here as Example 1.21.

The main result of [DMP14] depends on several theorems. In outline, [DMP14] gives a base construction for a reduced linking system using partial difference sets and a product construction for combining two reduced linking systems into a larger one. We summarize the main pieces of their construction to show how their linking systems are made.

Definition 1.24. Let G be a group of order v, written multiplicatively, and let D be a subset of G with k elements. Then D is a (v, k, λ, μ)**-partial difference set (PDS)** in G if the multiset $\{d_1 d_2^{-1} : d_1, d_2 \in D : d_1 \neq d_2\}$ contains every non-identity element of D exactly λ times and contains every non-identity element of $G \setminus D$ exactly μ times.

The base construction given in the following theorem relies on the existence of multiple PDSs with intricate mutual properties.

Theorem 1.25 (Davis, Martin, and Polhill [DMP14, Theorem 5.3])**.** *Suppose that G is an abelian group of order 2^{2s}, and suppose that G contains 2^{s-r} mutually disjoint $(2^{2s}, 2^r(2^s - 1), 2^s + 2^{2r} - 3 \cdot 2^{2r}, 2^{2r} - 2^r)$ PDSs for some $0 \leq r \leq s - 2$. Suppose further that every union of 2^{s-2-r} of the PDSs is a $(2^{2s}, 2^{s-2}(2^s - 1), 2^s + 2^{2s-4} - 3 \cdot 2^{s-2}, 2^{2s-4} - 2^{s-2})$ PDS in G and that every union of 2^{s-1-r} of the PDSs is a reversible difference set in G. Then G contains a reversible reduced linking system of size $2^{s-r} - 1$.*

The product construction given in the following theorem applies when the parameters of the reduced linking system of difference sets to be combined belong to the Hadamard family.

Theorem 1.26 (Davis, Martin, and Polhill [DMP14, Theorem 3.1])**.** *Suppose that G contains a reversible reduced $(4N^2, N(2N-1), N(N-1), N^2; \ell)$-linking system $\{D_1, D_2, \ldots, D_\ell\}$ and that H contains a reversible reduced $(4M^2, M(2M-1), M(M-1), M^2; \ell)$-linking system $\{C_1, C_2, \ldots, C_\ell\}$. Then $G \times H$ contains a reversible reduced $(4(2NM)^2, (2NM)(2(2NM) - 1), 2NM(2NM - 1), (2NM)^2; \ell)$-linking system $\{F_1, F_2, \ldots, F_\ell\}$ given by*

$$F_i = D_i(H - C_i) + (G - D_i)C_i.$$

We see from Theorem 1.26 that Hadamard parameters based on N and M combine to give Hadamard parameter $2NM$. Theorems 1.25 and 1.26 are combined with another result in [DMP14, Theorem 4.6], as follows. Recall from Theorem 1.2 that the parameters of a difference set in an abelian 2-group are completely determined by the order of the group.

Theorem 1.27 (Davis, Martin, and Polhill [DMP14, Corollary 5.5])**.** *Let* $G = \mathbb{Z}_{2^{a_1}}^{2b_1} \times \cdots \times \mathbb{Z}_{2^{a_k}}^{2b_k}$ *for integers* a_i, b_i *satisfying* $a_i \geq 1$ *and* $b_i \geq 2$*, and let* $b \geq 2$*. Then the groups below contain a reversible reduced linking system of the specified size.*

Group	Size
G	$2^{\min(b_1,b_2,\ldots,b_k)} - 1$
$\mathbb{Z}_4^b$	$2^b - 1$
$G \times \mathbb{Z}_4^b$	$2^{\min(b_1,b_2,\ldots,b_k,b)} - 1$

Davis, Martin, and Polhill conclude their paper with five open problems, of which we shall address the following four (numbered 1, 3, 4, and 5 in [DMP14]).

Q1. "Investigate the relationships between the difference set constructions of linked systems [given in [DMP14]] with the constructions of the Cameron-Seidel family and the Kerdock codes."

Q2. "Can difference sets be used to construct systems of linked designs with different parameters, for instance in the Hadamard family $(4N^2, 2N^2 - N, N^2 - N)$ but with N not a power of 2?"

Q3. "Is there an infinite family that generalizes [Example 1.21]?"

Q4. "Can [generalizations of difference sets] be exploited to find other linked systems of mathematical structures?"

1.5 Boolean Functions and Bent Sets

Bey and Kyureghyan [BK08] provide the second of the two principal references on linking systems of difference sets. Their main result is phrased in terms of linked symmetric designs, rather than linking systems of difference sets (which were not defined until 2014 in [DMP14]). We show in this section that, rephrasing the main result of [BK08] in terms of the newer terminology, we can immediately answer Q1 of Section 1.4 by connecting Kerdock sets to reduced linking systems of difference sets in order to give Corollary 1.37. This use of the results of [BK08] was apparently overlooked in [DMP14]. We shall make use of Corollary 1.37 later in the thesis, but otherwise will not need to refer to the definitions and results of this section.

Definition 1.28. A **Boolean function on** $\mathbb{Z}_2^n$ is a function f from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$.

Definition 1.29. The **subset** of $\mathbb{Z}_2^n = \langle x_1, x_2, \ldots, x_n \rangle$ **corresponding to a Boolean function** f **on** $\mathbb{Z}_2^n$ is

$$S(f) = \{x_1^{y_1} x_2^{y_2} \cdots x_n^{y_n} : f(y_1, y_2, \ldots, y_n) = 1\}.$$

Example 1.30. Let $f(y_1, y_2, y_3, y_4) = y_1 y_2 + y_3 y_4$ be a Boolean function on $\mathbb{Z}_2^4$. Then $f(y_1, y_2, y_3, y_4) = 1$ exactly when

$$(y_1, y_2, y_3, y_4) \in \{(0,0,1,1), (0,1,1,1), (1,0,1,1), (1,1,0,0), (1,1,0,1), (1,1,1,0)\}.$$

The corresponding subset $S(f)$ of $\mathbb{Z}_2^4 = \langle x, y, z, w \rangle$ is

$$S(f) = zw + yzw + xzw + xy + xyw + xyz.$$

Definition 1.31. The **Walsh-Hadamard transform** of a Boolean function f on $\mathbb{Z}_2^n$ is the function $\widehat{f} : \mathbb{Z}_2^n \to \mathbb{Z}$ given by

$$\widehat{f}(u) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) + u \cdot x} \quad \text{for } u \in \mathbb{Z}_2^n,$$

where $\cdot$ is the usual inner product on $\mathbb{Z}_2^n$.

Definition 1.32. A Boolean function f on $\mathbb{Z}_2^n$ is **bent** if

$$\widehat{f}(u) \in \{2^{n/2}, -2^{n/2}\} \quad \text{for all } u \in \mathbb{Z}_2^n.$$

The close connection between bent functions and difference sets in elementary abelian 2-groups is given by the following result.

Theorem 1.33 (Dillon [Dil74])**.** *A Boolean function f on $\mathbb{Z}_2^{2d+2}$ is bent if and only if $S(f)$ is a difference set in $\mathbb{Z}_2^{2d+2}$.*

Definition 1.34. A **bent set on** $\mathbb{Z}_2^{2n}$ of size $\ell + 1$ is a set $\{f_0, f_1, \ldots, f_\ell\}$ of Boolean functions on $\mathbb{Z}_2^{2n}$ such that the Boolean function $f_i + f_j$ is bent for all distinct i, j.

We may assume (by adding one function to all the others) that one function in a bent set is the zero function. We now state the main theorem of [BK08], rephrased in terms of linking systems of difference sets.

Theorem 1.35 (Bey and Kyureghyan [BK08, Theorem 1])**.** *Let $\ell \geq 2$ and suppose $\{0, f_1, \ldots, f_\ell\}$ is a bent set on $\mathbb{Z}_2^{2d+2}$. Then $\{S(f_1), S(f_2), \ldots, S(f_\ell)\}$ is a reduced linking system of difference sets in $\mathbb{Z}_2^{2d+2}$.*

There is a well-known construction of a bent set on $\mathbb{Z}_2^{2d+2}$, due originally to Kerdock [Ker72].

Theorem 1.36 (Kerdock [Ker72], MacWilliams and Sloane [MS77, page 456])**.** *For each integer $d \geq 0$, there exists a bent set on $\mathbb{Z}_2^{2d+2}$ of size 2^{2d+1}.*

Combining Theorems 1.35 and 1.36, we obtain the following corollary. Note that the parameters of the difference sets in Corollary 1.37 are determined by Theorem 1.2.

Corollary 1.37. *For each integer $d \geq 1$, there exists a reduced linking system of difference sets in $\mathbb{Z}_2^{2d+2}$ of size $2^{2d+1} - 1$.*

We now give an example of a reduced linking system of difference sets in $\mathbb{Z}_2^4$ of size 7 obtained from a bent set on $\mathbb{Z}_2^4$ of size 8.

Example 1.38. A bent set on $\mathbb{Z}_2^4$ of size 8 is given by the Boolean functions $\{0, f_1, f_2, f_3, f_4, f_5, f_6, f_7\}$, where

$$\begin{aligned}
f_1(y_1, y_2, y_3, y_4) &= y_1y_4 + y_2y_3 + y_3y_4 \\
f_2(y_1, y_2, y_3, y_4) &= y_1y_3 + y_2y_3 + y_2y_4 + y_3y_4 \\
f_3(y_1, y_2, y_3, y_4) &= y_1y_3 + y_1y_4 + y_2y_4 + y_3y_4 \\
f_4(y_1, y_2, y_3, y_4) &= y_1y_2 + y_3y_4 \\
f_5(y_1, y_2, y_3, y_4) &= y_1y_2 + y_1y_4 + y_2y_3 + y_2y_4 \\
f_6(y_1, y_2, y_3, y_4) &= y_1y_2 + y_1y_3 + y_2y_4 \\
f_7(y_1, y_2, y_3, y_4) &= y_1y_2 + y_1y_3 + y_1y_4 + y_2y_3.
\end{aligned}$$

The subsets $S(f_1), S(f_2), \ldots, S(f_7)$ form a reduced $(16, 6, 2, 4; 7)$-linking system of difference sets in $\mathbb{Z}_2^4 = \langle x, y, z, w \rangle$, where

$$\begin{aligned}
S(f_1) &= xw + xyw + zw + yz + xyz + xyzw \\
S(f_2) &= yw + xyw + zw + xz + yz + yzw \\
S(f_3) &= xw + yw + zw + xz + xzw + xyz \\
S(f_4) &= xy + xyw + zw + xzw + yzw + xyz \\
S(f_5) &= xw + yw + xy + xyw + xzw + yz \\
S(f_6) &= yw + xy + xz + xzw + yzw + xyzw \\
S(f_7) &= xw + xy + xz + yz + yzw + xyz.
\end{aligned}$$

We cannot use Theorem 1.35 to produce a reduced system of linking difference sets larger than that in Corollary 1.37, because the following result shows that the bent sets of Theorem 1.36 attain the maximum size.

Theorem 1.39 (Bey and Kyureghyan [BK08, Theorem 2])**.** *For each integer $d \geq 0$, there is no bent set on $\mathbb{Z}_2^{2d+2}$ of size greater than 2^{2d+1}.*

1.6 Overview of Thesis

A central motivation of this thesis is to address questions Q1 to Q4 as listed in Section 1.4. We have already answered Q1 in Section 1.5 by connecting Kerdock sets to reduced linking systems of difference sets.

In Chapter 2 we provide the mathematical toolkit required for the rest of the thesis.

In Chapter 3 we uncover an obstruction to the existence of a reduced linking system of difference sets in certain groups that are not 2-groups, using only elementary arguments that depend on a well-chosen reduction in the group ring. This provides a partial answer to Q2.

In Chapter 4 we therefore return to 2-groups and seek new constructions. Our main construction (Theorem 4.2) relies on the unexpected use of difference matrices, which addresses Q4. We derive multiple corollaries of this construction, as summarized in Table 1.2 and illustrated in Table 1.3. (By Theorem 1.3 we need not consider groups of exponent greater than 2^{d+2} in Table 1.2, and not greater than 16 in Table 1.3. An abelian 2-group is isomorphic to $\mathbb{Z}_{2^{a_1}} \times \mathbb{Z}_{2^{a_2}} \times \cdots \times \mathbb{Z}_{2^{a_t}}$ for some integers a_i and t, and its **rank** is then t.) We construct an infinite family of examples in nonabelian groups, whereas not a single nonabelian example was previously known. We obtain an infinite family of nonreversible examples generalizing Example 1.21, answering Q3.

Table 1.2: Constructions of a reduced linking system of difference sets in an abelian group G of order 2^{2d+2}, rank at least $d+1$, and exponent 2^e.

Range of e	Size of System	Source
1	$2^{2d+1}-1$	Bent Set (Corollary 1.37)
$[2, \frac{d+3}{2}]$	$2^{\lfloor \frac{d+1}{e-1} \rfloor}-1$	Difference Matrix (Corollary 4.5)
$(\frac{d+3}{2}, d+1]$	3	Difference Matrix (Corollary 4.4)
$d+2$ (so $G = \mathbb{Z}_{2^{d+2}} \times \mathbb{Z}_2^d$)	No Result	

In Chapter 5 we suggest directions for further research by posing several open problems.

The results of this thesis were partially presented at the CanaDAM 2017 conference.

Table 1.3: Comparison of maximum known sizes of reduced linking systems of difference sets in abelian groups of order 64.

Group	Previous Maximum Known Size	Current Maximum Known Size	Source
$\mathbb{Z}_2^6$	31 [BK08]	31	Bent Set (Corollary 1.37)
$\mathbb{Z}_4 \times \mathbb{Z}_2^4$	None	7	Difference Matrix (Corollary 4.5)
$\mathbb{Z}_4^2 \times \mathbb{Z}_2^2$	None	7	Difference Matrix (Corollary 4.5)
$\mathbb{Z}_4^3$	7 [DMP14]	7	Difference Matrix (Corollary 4.5)
$\mathbb{Z}_8 \times \mathbb{Z}_2^3$	None	3	Difference Matrix (Corollary 4.4)
$\mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	None	3	Difference Matrix (Corollary 4.4)
$\mathbb{Z}_8^2$	None	None	
$\mathbb{Z}_{16} \times \mathbb{Z}_2^2$	None	None	
$\mathbb{Z}_{16} \times \mathbb{Z}_4$	None	None	

Chapter 2

Mathematical Toolkit

In this chapter, we describe the mathematical tools and background required to establish our nonexistence and constructive results.

2.1 Hyperplanes

Definition 2.1. Let V be a vector space of dimension $d+1$ over $\mathrm{GF}(q)$. The **hyperplanes** of V are the $\frac{q^{d+1}-1}{q-1}$ subspaces of V of dimension d.

We now prove a fundamental relationship between the hyperplanes of a vector space. Since we wish to reserve "+" for addition in the group ring $\mathbb{Z}[G]$, we state the result using multiplication for vector space addition (but present the proof in additive notation).

Theorem 2.2. *Let H_i and H_j be hyperplanes of a vector space V of dimension $d+1$ over* $\mathrm{GF}(q)$. *Then*

$$H_i H_j = \begin{cases} q^d H_i & \text{if } H_i = H_j \\ q^{d-1} V & \text{if } H_i \neq H_j. \end{cases}$$

Proof. Using additive notation for vector space addition, the required relationship is

$$H_i + H_j = \begin{cases} q^d H_i & \text{if } H_i = H_j \\ q^{d-1} V & \text{if } H_i \neq H_j. \end{cases} \tag{2.1}$$

For $h \in H_i$ we have $h + H_i = H_i$ since H_i is a subspace. Therefore,

$$H_i + H_i = |H_i| H_i = q^d H_i,$$

which proves the first statement of (2.1).

Now take $H_i \neq H_j$ and so the sum

$$H_i + H_j = \{a + b : a \in H_i, b \in H_j\}$$

has dimension at least $d+1$ over GF(q), is a subspace of V, and so contains every element of V. Furthermore, the subspace $H_i \cap H_j$ has dimension $d-1$ over GF(q). Then for every element $h = a + b$ with a in H_i and b in H_j, we can represent h as

$$h = (a + c) + (b - c) \quad \text{for } c \in H_i \cap H_j.$$

Thus each element in V is obtained exactly $|H_i \cap H_j| = q^{d-1}$ times as the sum of an element in H_i and an element in H_j, which proves the second statement of (2.1). □

We now give two examples illustrating Theorem 2.2, the first when q is a prime and the second when q is not prime. When q is not a prime, we see that care is required to express the hyperplanes as subgroups of the elementary abelian group of order q^{d+1} corresponding to V.

Example 2.3. Let $q = 3$ and $d = 1$ and let $V = \mathrm{GF}(3)^2$ be a vector space of dimension 2 over GF(3). Consider V as a group $G = \mathbb{Z}_3^2 = \langle x, y \rangle$. Let $H_1 = \mathbf{1}_G + x + x^2 = \langle x \rangle$ and $H_2 = \mathbf{1}_G + y + y^2 = \langle y \rangle$. Then

$$H_1 H_2 = \langle x \rangle \langle y \rangle = \langle x, y \rangle = G.$$

We can view this pictorially using the representation

H_1

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

H_2

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

We break the product $H_1 H_2$ into three terms

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

$\times$

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

$=$

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

$\times$

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

$=$

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

$\times$

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

$=$

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

Putting the three terms together gives

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

$\times$

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

$=$

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

Example 2.4. Let $q = 4$ and $d = 1$ and let V be a vector space of dimension 2 over $\mathrm{GF}(4) = \{0, 1, \delta, \delta^2\}$ where $\delta^2 = 1 + \delta$. The additive group of $\mathrm{GF}(4)$ is isomorphic to $\mathbb{Z}_2^2$ and can be written as all linear combinations of 1 and δ taking coefficients from $\mathrm{GF}(2)$. Therefore

$$V = \langle (1,0), (\delta,0), (0,1), (0,\delta) \rangle.$$

The hyperplanes of V are the subspaces of V of dimension 1, namely

$$\begin{aligned}
H_1 &= \langle (1,0) \rangle = \{\alpha(1,0) : \alpha \in \mathrm{GF}(4)\} = \{(0,0), (1,0), (\delta,0), (\delta^2,0)\} \\
H_2 &= \langle (0,1) \rangle = \{\alpha(0,1) : \alpha \in \mathrm{GF}(4)\} = \{(0,0), (0,1), (0,\delta), (0,\delta^2)\} \\
H_3 &= \langle (1,1) \rangle = \{\alpha(1,1) : \alpha \in \mathrm{GF}(4)\} = \{(0,0), (1,1), (\delta,\delta), (\delta^2,\delta^2)\} \\
H_4 &= \langle (\delta,1) \rangle = \{\alpha(\delta,1) : \alpha \in \mathrm{GF}(4)\} = \{(0,0), (\delta,1), (\delta^2,\delta), (1,\delta^2)\} \\
H_5 &= \langle (\delta^2,1) \rangle = \{\alpha(\delta^2,1) : \alpha \in \mathrm{GF}(4)\} = \{(0,0), (\delta^2,1), (1,\delta), (\delta,\delta^2)\}.
\end{aligned}$$

Now we interpret the elements of V as elements of $\mathbb{Z}_2^4$ under the isomorphism ϕ from V to $G = \mathbb{Z}_2^4 = \langle x, y, z, w \rangle$ given by

$$\phi((1,0)) = x, \quad \phi((\delta,0)) = y, \quad \phi((0,1)) = z, \quad \phi((0,\delta)) = w.$$

Under the isomorphism ϕ, the hyperplanes of V map to the following subgroups of G:

$$\begin{aligned}
H_1 &= \langle x, y \rangle = \{\mathbf{1}_G, x, y, xy\} \\
H_2 &= \langle z, w \rangle = \{\mathbf{1}_G, z, w, wz\} \\
H_3 &= \langle xz, yw \rangle = \{\mathbf{1}_G, xz, yw, xyzw\} \\
H_4 &= \langle yz, xyw \rangle = \{\mathbf{1}_G, yz, xyw, xzw\} \\
H_5 &= \langle xyz, xw \rangle = \{\mathbf{1}_G, xyz, xw, yzw\}.
\end{aligned}$$

The visual verification of Theorem 2.2 in Figure 2.1 is then similar to that of Example 2.3.

Figure 2.1: The subgroups of $\mathbb{Z}_2^4$ corresponding to hyperplanes of $\mathrm{GF}(4)^2$.

H_1

$\mathbf{1}_G$	y	z	yz
x	xy	xz	xyz

w	yw	zw	yzw
xw	xyw	xzw	$xyzw$

H_2

$\mathbf{1}_G$	y	z	yz
x	xy	xz	xyz

w	yw	zw	yzw
xw	xyw	xzw	$xyzw$

H_3

$\mathbf{1}_G$	y	z	yz
x	xy	xz	xyz

w	yw	zw	yzw
xw	xyw	xzw	$xyzw$

H_4

$\mathbf{1}_G$	y	z	yz
x	xy	xz	xyz

w	yw	zw	yzw
xw	xyw	xzw	$xyzw$

H_5

$\mathbf{1}_G$	y	z	yz
x	xy	xz	xyz

w	yw	zw	yzw
xw	xyw	xzw	$xyzw$

2.2 McFarland/Dillon and Spence Constructions

We now present the constructions originally given by McFarland [McF73] (and later modified by Dillon [Dil85]) and Spence [Spe77] for the parameter families named after them. Write the McFarland parameter family given in Table 1.1 in the form

$$(v,k,\lambda,n) = \left(q^{d+1}(s+1), q^d s, q^d(s-q^d), q^{2d}\right), \text{ where } s = \frac{q^{d+1}-1}{q-1}.$$

Theorem 2.5 (Existence of McFarland difference sets, McFarland [McF73], Dillon [Dil85])**.** *Let q be a prime power and d a nonnegative integer, and let $s = \frac{q^{d+1}-1}{q-1}$. Let G be a group containing a central subgroup E of index $s+1$ isomorphic to the elementary abelian group of order q^{d+1}. Let $g_0, g_1, \ldots, g_s$ be a set of coset representatives for E in G. Let $H_1, H_2, \ldots, H_s$ be the subgroups of G corresponding to the hyperplanes of E under an isomorphism ϕ when E is regarded as a vector space of dimension $d+1$ over $\mathrm{GF}(q)$. Then*

$$D = \sum_{i=1}^{s} g_i H_i$$

is a $(q^{d+1}(s+1), q^d s, q^d(s-q^d), q^{2d})$-difference set in G.

Proof. Note that D is a subset of G because $g_0, g_1, \ldots, g_s$ is a set of coset representatives of E in G and $H_i \subseteq E$. We calculate

$$\begin{aligned}
DD^{(-1)} &= \left(\sum_{i=1}^{s} g_i H_i\right)\left(\sum_{j=1}^{s} H_j^{(-1)} g_j^{-1}\right) \\
&= \sum_{1\le i,j\le s} g_i H_i H_j g_j^{-1} \\
&= \sum_{1\le i,j\le s} g_i g_j^{-1} H_i H_j \\
&= \sum_{i=1}^{s} H_i H_i + \sum_{\substack{1\le i,j\le s \\ i\neq j}} g_i g_j^{-1} H_i H_j \\
&= q^d \sum_{i=1}^{s} H_i + q^{d-1} \sum_{\substack{1\le i,j\le s \\ i\neq j}} g_i g_j^{-1} E. \qquad (2.2)
\end{aligned}$$

The second equality follows from $H_i^{(-1)} = H_i$ since H_i is a subgroup. The third equality uses that $H_i \subset E$ which is central in G. The fourth equality is just splitting the sum up by $i = j$ and $i \neq j$. Lastly, we use Theorem 2.2. The identity element of E is in each subgroup, so we count that each non-identity element of E is contained in exactly $\frac{q^d-1}{q-1} = s - q^d$

subgroups H_i. Therefore

$$\sum_{i=1}^{s} H_i = s\mathbf{1}_G + (s - q^d)(E - \mathbf{1}_G). \tag{2.3}$$

Now regard the cosets g_iE as elements of the factor group G/E. Then the elements $g_1E, g_2E, \ldots, g_sE$ form a trivial $(s+1, s, s-1, 1)$-difference set in G/E (the complement of the trivial $(s+1, 1, 0, 1)$-difference set $\{g_0E\}$ in G/E). By Lemma 1.6 we have

$$\left(\sum_{i=1}^{s} g_iE\right)\left(\sum_{j=1}^{s} g_jE\right)^{(-1)} = \mathbf{1}_{G/E} + (s-1)G/E \quad \text{in } \mathbb{Z}[G/E].$$

The left hand side is

$$\begin{aligned}\left(\sum_{i=1}^{s} g_iE\right)\left(\sum_{j=1}^{s} (g_jE)^{-1}\right) &= \sum_{i,j} (g_iE)(g_jE)^{-1} \\ &= \sum_{i,j} g_ig_j^{-1}E \quad \text{in } \mathbb{Z}[G/E],\end{aligned}$$

and so we have

$$\sum_{i,j} g_ig_j^{-1}E = \mathbf{1}_{G/E} + (s-1)G/E \quad \text{in } \mathbb{Z}[G/E].$$

Now interpret the element g_iE in G/E as $|E|$ elements in G, so that in the group ring $\mathbb{Z}[G]$ the above equation becomes

$$\sum_{i,j} g_ig_j^{-1}E = E + (s-1)G$$

and so

$$\sum_{i\neq j} g_ig_j^{-1}E = E + (s-1)G - sE = (s-1)(G-E).$$

Substitute this and (2.3) into (2.2) to get

$$DD^{(-1)} = q^d\left(s\mathbf{1}_G + (s-q^d)(E-\mathbf{1}_G)\right) + q^{d-1}(s-1)(G-E).$$

By the definition of s, the coefficient of E on the right hand side evaluates to 0. Combining terms and simplifying gives

$$DD^{(-1)} = q^{2d}\mathbf{1}_G + q^d(s-q^d)G,$$

as required by Lemma 1.6. □

Figure 2.2: McFarland difference set in $G = \mathbb{Z}_3^2 \times \mathbb{Z}_5$

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

z	zy	zy^2
zx	zxy	zxy^2
zx^2	zx^2y	zx^2y^2

z^2	z^2y	z^2y^2
z^2x	z^2xy	z^2xy^2
z^2x^2	z^2x^2y	$z^2x^2y^2$

z^3	z^3y	z^3y^2
z^3x	z^3xy	z^3xy^2
z^3x^2	z^3x^2y	$z^3x^2y^2$

z^4	z^4y	z^4y^2
z^4x	z^4xy	z^4xy^2
z^4x^2	z^4x^2y	$z^4x^2y^2$

Example 2.6. Let $q = 3$ and $d = 1$, so $s = 4$. We construct a McFarland difference set in $G = \mathbb{Z}_3^2 \times \mathbb{Z}_5$ according to Theorem 2.5. We consider the subgroup $E \cong \mathbb{Z}_3^2$ of G as a vector space of dimension 2 over GF(3). The subgroups of G corresponding to the hyperplanes of E are

$$\begin{aligned} H_1 &= \mathbf{1}_G + y + y^2 = \langle y \rangle \\ H_2 &= \mathbf{1}_G + x + x^2 = \langle x \rangle \\ H_3 &= \mathbf{1}_G + xy + x^2y^2 = \langle xy \rangle \\ H_4 &= \mathbf{1}_G + x^2y + xy^2 = \langle x^2y \rangle. \end{aligned}$$

A set of coset representatives for E in G is

$$(g_0, g_1, g_2, g_3, g_4) = (\mathbf{1}_G, zx, z^2y, z^3y, z^4y).$$

Figure 2.2 shows the resulting McFarland $(45, 12, 3, 9)$-difference set in G.

We remark that there are constructions, different from that of Theorem 2.5, for difference sets with McFarland parameters [DJ97].

Write the Spence parameter family given in Table 1.1 in the form

$$(v,k,\lambda,n) = \left(3^{d+1}s, 3^d(s+1), 3^d(s+1-3^d), 3^{2d}\right), \quad \text{where } s = \frac{3^{d+1}-1}{2}.$$

Theorem 2.7 (Existence of Spence difference sets, Spence [Spe77])**.** *Let $d \geq 0$ and let $s = \frac{3^{d+1}-1}{2}$. Let G be a group containing a central subgroup E of index s isomorphic to $\mathbb{Z}_3^{d+1}$. Let $g_1, \ldots, g_s$ be a set of coset representatives for E in G. Let $H_1, H_2, \ldots, H_s$ be the subgroups of G corresponding to the hyperplanes of E when E is regarded as a vector space of dimension $d+1$ over* GF(3)*. Then*

$$D = g_1(E - H_1) + \sum_{i=2}^{s} g_i H_i$$

is a Spence difference set in G.

Proof. The proof follows from similar calculations as in the proof of Theorem 2.5. □

Example 2.8. Let $d = 1$, so $s = 4$. We construct a Spence difference set in $G = \mathbb{Z}_3^2 \times \mathbb{Z}_4$ according to Theorem 2.7. We consider the subgroup $E \cong \mathbb{Z}_3^2$ of G as a vector space of dimension 2 over GF(3). The subgroups H_1, H_2, H_3, H_4 of G corresponding to the hyperplanes of E are as given in Example 2.6. A set of coset representatives for E in G is

$$(g_1, g_2, g_3, g_4) = (x, zy, z^2y, z^3y).$$

Figure 2.3 shows the resulting Spence $(36, 15, 6, 9)$-difference set in G.

Note that in the McFarland/Dillon construction, the subgroup E has index $s+1$ in G and the difference set D takes cosets of s of the subgroups corresponding to hyperplanes. In contrast, in the Spence construction, the subgroup E has index s in G, but the difference set D takes a coset of the complement in E of one of the subgroups corresponding to a hyperplane together with cosets of all $s-1$ of the remaining such subgroups. Also note that the subgroups $H_1, H_2, \ldots, H_s$ of G corresponding to hyperplanes of E depend on the isomorphism ϕ in the McFarland/Dillon construction (in the case that q is not prime), but are completely determined in the Spence construction (which uses the field GF(3)).

2.3 Difference Matrices

Definition 2.9. Let G be a group of order v. A (G, m, λ)**-difference matrix** is an $m \times \lambda v$ matrix $(b_{i,j})$ with $0 \leq i \leq m-1$ and $0 \leq j \leq \lambda v - 1$ and each entry $b_{i,j} \in G$ such that, for all distinct rows i and r, the multiset $\{b_{i,j}b_{r,j}^{-1} : 0 \leq j \leq \lambda v - 1\}$ contains every element of G exactly λ times.

Figure 2.3: Spence difference set in $G = \mathbb{Z}_3^2 \times \mathbb{Z}_4$

$\mathbf{1}_G$	y	y^2
x	xy	xy^2
x^2	x^2y	x^2y^2

z	zy	zy^2
zx	zxy	zxy^2
zx^2	zx^2y	zx^2y^2

z^2	z^2y	z^2y^2
z^2x	z^2xy	z^2xy^2
z^2x^2	z^2x^2y	$z^2x^2y^2$

z^3	z^3y	z^3y^2
z^3x	z^3xy	z^3xy^2
z^3x^2	z^3x^2y	$z^3x^2y^2$

We shall be interested only in the case $\lambda = 1$ of Definition 2.9, so that for each distinct i, r the set $\{b_{i,j}b_{r,j}^{-1} : 0 \le j \le v-1\}$ contains every element of G exactly once. We can multiply all entries of a column of a $(G, m, 1)$-difference matrix by a fixed $a \in G$ without changing the defining property of the matrix, because $(b_{i,j}a)(b_{r,j}a)^{-1} = b_{i,j}b_{r,j}^{-1}$. By multiplying all entries of each column j by $b_{0,j}^{-1}$, we may therefore assume that each entry of row 0 of the matrix is $\mathbf{1}_G$. The difference property of the matrix then implies that, for each $i \ge 1$, the set $\{b_{i,j} : 0 \le j \le v-1\}$ also contains every element of G exactly once. We can likewise multiply all entries of each row by $b_{i,0}^{-1}$, so that each entry of column 0 of the matrix is $\mathbf{1}_G$. By the pigeonhole principle, the largest number of rows of a $(G, m, 1)$-difference matrix is therefore $|G|$.

We shall make use of two constructive results for difference matrices in abelian 2-groups.

Theorem 2.10 (Pan and Chang [PC16, Lemma 3.4])**.** *Let G be an abelian 2-group of rank at least 2. Then there exists a $(G, 4, 1)$-difference matrix.*

Theorem 2.11 (Buratti [Bur98, Theorem 2.11])**.** *Let G be an abelian group of order 2^{d+1} and exponent 2^e. Then there exists a $(G, 2^{\lfloor \frac{d+1}{e} \rfloor}, 1)$-difference matrix.*

The case $e = 1$ of Theorem 2.11 gives a $(G, m, 1)$-difference matrix for $G = \mathbb{Z}_2^{d+1}$ and $m = 2^{d+1}$, which satisfies the extremal condition $m = |G|$.

Example 2.12. Let $G = \mathbb{Z}_2^2 = \langle x, y \rangle$. The matrix

$$(b_{i,j}) = \begin{pmatrix} \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G \\ \mathbf{1}_G & x & y & xy \\ \mathbf{1}_G & y & xy & x \\ \mathbf{1}_G & xy & x & y \end{pmatrix}$$

is a $(\mathbb{Z}_2^2, 4, 1)$-difference matrix. We verify the difference property for $(i, r) = (1, 2)$, for example, as

$$\{b_{1,j} b_{2,j}^{-1} : 0 \leq j \leq 3\} = \{\mathbf{1}_G(\mathbf{1}_G)^{-1}, x(y)^{-1}, y(xy)^{-1}, xy(x)^{-1}\} = \{\mathbf{1}_G, xy, x, y\} = \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Example 2.13. Let $\mathbb{Z}_{15} = \langle x \rangle$. The matrix $(a_{i,j}) = x^{b_{i,j}}$ where

$$(b_{i,j}) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 0 & 2 & 5 & 7 & 9 & 12 & 4 & 1 & 14 & 11 & 3 & 6 & 8 & 10 & 13 \\ 0 & 6 & 3 & 14 & 10 & 7 & 13 & 4 & 11 & 2 & 8 & 5 & 1 & 12 & 9 \\ 0 & 10 & 6 & 1 & 11 & 2 & 7 & 12 & 3 & 8 & 13 & 4 & 14 & 9 & 5 \end{pmatrix}$$

is a $(\mathbb{Z}_{15}, 5, 1)$-difference matrix.

Chapter 3

Nonexistence Results

Recall Q2 of Section 1.4, which asks whether there are reduced linking systems of difference sets in groups other than 2-groups. In this chapter, we uncover an obstruction to the existence of such a system, both when the difference sets are constructed by the McFarland/Dillon method (Theorem 2.5) and when they are constructed by the Spence method (Theorem 2.7).

Our nonexistence proof method uses only elementary arguments and is not restricted to abelian groups. It combines the hyperplane properties of Theorem 2.2, modular reduction in the group ring, and projection to a subgroup. The novelty of the proof method lies in recognizing the correct modular reduction which allows these properties to be successfully combined. We state these nonexistence results below.

Theorem 3.1. *Let $q > 2$ be a prime power and d a positive integer, and let $s = \frac{q^{d+1}-1}{q-1}$. Then there is no reduced linking system of difference sets with McFarland parameters*

$$(v, k, \lambda, n) = \left(q^{d+1}(s+1), q^d s, q^d(s-q^d), q^{2d}\right)$$

in which two of the difference sets are constructed as in Theorem 2.5 with respect to the same subgroup E and the same isomorphism ϕ.

Theorem 3.2. *Let d be a positive integer and let $s = \frac{3^{d+1}-1}{2}$. Then there is no reduced linking system of difference sets with Spence parameters*

$$(v, k, \lambda, n) = \left(3^{d+1}s, 3^d(s+1), 3^d(s+1-3^d), 3^{2d}\right)$$

in which two of the difference sets are constructed as in Theorem 2.7.

The condition in Theorem 3.1, that the two difference sets are constructed with respect to the same subgroup E, can be omitted when $q = p^r$ for an odd prime p: in this case the central subgroup E is then a Sylow p-subgroup of the group G of order $q^{d+1}(s+1)$ because $\gcd(p, s+1) = 1$, and so is unique by Sylow's Third Theorem. Similarly, this condition is

not needed in Theorem 3.2. The condition in Theorem 3.1, that the two difference sets are constructed with respect to the same isomorphism ϕ, can be omitted when q is prime.

By imposing the condition $d > 0$ in Theorems 3.1 and 3.2 we exclude trivial McFarland and Spence difference sets containing a single element. In the case $d = 1$, we can remove the condition in Theorem 3.2 referring to Theorem 2.7 when the group is abelian, because the classification result given by Turyn [Tur65, Theorem 10] and completed by Spence [Spe77, Section 2] states that every $(36, 15, 6, 9)$-difference set in an abelian group of order 36 is constructed as in Theorem 2.7 (for some labelling of the subgroups corresponding to hyperplanes H_1, H_2, H_3, H_4).

Corollary 3.3. *There is no reduced linking system of* $(36, 15, 6, 9)$*-difference sets in an abelian group.*

We give preliminary divisibility conditions in Section 3.1, and use them in the nonexistence proofs presented in Section 3.2.

3.1 Divisibility Conditions

Lemma 3.4. *Let* $q > 2$ *be a prime power and* d *a positive integer, and let* $s = \frac{q^{d+1}-1}{q-1}$. *Then* $s + 1$ *does not divide* $q^{d-1}s(s-1)$.

Proof. Suppose, for a contradiction, that $s+1$ divides $q^{d-1}s(s-1)$. Since $\gcd(s+1, s) = 1$, this implies that

$$s + 1 \text{ divides } q^{d-1}(s-1). \tag{3.1}$$

Note that

$$s + 1 = 2 + q + q^2 + \cdots + q^d. \tag{3.2}$$

Case 1: q **is odd.** We have $\gcd(s+1, q) = 1$ from (3.2) and then (3.1) implies the contradiction that $s + 1$ divides $s - 1$.

Case 2: $q > 2$ **is a power of 2.** Then s is odd and so $\gcd(s + 1, s - 1) = 2$. Then (3.1) implies that $s + 1$ divides $2q^{d-1}$. This is a contradiction because $s + 1$ is not a power of 2, by (3.2), whereas $2q^{d-1}$ is a power of 2.

□

Lemma 3.5. *Let* d *be a positive integer and let* $s = \frac{3^{d+1}-1}{2}$. *Then* s *does not divide* $3^{d-1}(s+1)(s+2)$.

Proof. Suppose, for a contradiction, that s divides $3^{d-1}(s+1)(s+2)$. Since $\gcd(s, s+1) = 1$, this implies that s divides $3^{d-1}(s+2)$. Writing $s = 1+3+3^2+\cdots+3^d$ shows that $\gcd(s, 3) = 1$ and we therefore deduce that s divides $s + 2$. This is a contradiction because $s > 2$. □

3.2 Proof of Theorems 3.1 and 3.2

Proof of Theorem 3.1. Let G be a group containing a central subgroup E of index $s+1$ isomorphic to the elementary abelian group of order q^{d+1}. Let $f_0, f_1, \ldots, f_s$ and $g_0, g_1, \ldots, g_s$ each be a set of coset representatives for E in G. Let $H_1, H_2, \ldots, H_s$ be the subgroups of G corresponding to the hyperplanes of E when E is regarded as a vector space of dimension $d+1$ over GF(q). The isomorphism ϕ uniquely determines the subgroups $H_1, H_2, \ldots H_s$. Let

$$D_1 = \sum_{i=1}^{s} f_i H_i \quad \text{and} \quad D_2 = \sum_{i=1}^{s} g_i H_i$$

and suppose, for a contradiction, that there are integers μ, ν such that

$$D_1 D_2^{(-1)} = (\mu - \nu)D + \nu G \quad \text{in } \mathbb{Z}[G] \tag{3.3}$$

for some difference set D (having the same parameters (v, k, λ, n) as D_1, D_2) in G. By Lemma 1.17,

$$\nu = q^{d-1}\frac{s(s \pm 1)}{s+1} \quad \text{and} \quad \mu = \nu \mp q^d. \tag{3.4}$$

By Lemma 3.4 we cannot take the lower signs in (3.4), and so (3.3) becomes

$$D_1 D_2^{(-1)} = -q^d D + q^{d-1} s G. \tag{3.5}$$

Now, E is a central subgroup containing each H_i, and $H_i = H_i^{(-1)}$, so

$$\begin{aligned} D_1 D_2^{(-1)} &= \sum_{i=1}^{s} f_i H_i \sum_{j=1}^{s} (g_j H_j)^{(-1)} \\ &= \sum_{1 \le i,j \le s} f_i g_j^{-1} H_i H_j \\ &= q^d \sum_{i=1}^{s} f_i g_i^{-1} H_i + q^{d-1} \sum_{\substack{1 \le i,j \le s \\ i \ne j}} f_i g_j^{-1} E, \end{aligned}$$

by separating into sums over $i = j$ and $i \ne j$, and using Theorem 2.2. Substitute into (3.5) and reduce modulo q^d to obtain

$$q^{d-1} \sum_{\substack{1 \le i,j \le s \\ i \ne j}} f_i g_j^{-1} E \equiv q^{d-1} s G \pmod{q^d} \quad \text{in } \mathbb{Z}[G].$$

Therefore

$$\sum_{\substack{1\le i,j\le s\\ i\neq j}} f_i g_j^{-1} E \equiv sG \pmod{q} \quad \text{in } \mathbb{Z}[G]. \tag{3.6}$$

Let $K = \{k_0, k_1, \ldots, k_s\}$ be a set of coset representatives for E in G. Each $g \in G$ may be uniquely represented as $k_i e$ for some $k_i \in K$ and some $e \in E$, from which we define a projection map $\rho : G \to E$ by

$$\rho(k_i e) = e \quad \text{for } k_i \in K \text{ and } e \in E.$$

The map ρ induces a projection from $\mathbb{Z}[G]$ to $\mathbb{Z}[E]$. For each distinct i, j, write $f_i g_j^{-1} \in G$ uniquely as

$$f_i g_j^{-1} = k_{t(i,j)} e_{i,j} \quad \text{where } k_{t(i,j)} \in K \text{ and } e_{i,j} \in E,$$

and write $G = \sum_{i=0}^{s} \sum_{e\in E} k_i e$ so that (3.6) becomes

$$\sum_{\substack{1\le i,j\le s\\ i\neq j}} \sum_{e\in E} k_{t(i,j)} e_{i,j} e \equiv s \sum_{i=0}^{s} \sum_{e\in E} k_i e \pmod{q} \quad \text{in } \mathbb{Z}[G]. \tag{3.7}$$

Apply ρ to both sides to give

$$\sum_{\substack{1\le i,j\le s\\ i\neq j}} \sum_{e\in E} e_{i,j} e \equiv s \sum_{i=0}^{s} \sum_{e\in E} e \pmod{q} \quad \text{in } \mathbb{Z}[E]. \tag{3.8}$$

Using $\sum_{e\in E} e_{i,j} e = e_{i,j} E = E$ gives

$$s(s-1)E \equiv s(s+1)E \pmod{q} \quad \text{in } \mathbb{Z}[E].$$

Compare the coefficient of $\mathbf{1}_E$ on both sides to give

$$s(s-1) \equiv s(s+1) \pmod{q}.$$

Since $s = 1 + q + q^2 + \cdots + q^d$, this implies

$$0 \equiv 2 \pmod{q},$$

which is a contradiction because $q > 2$. □

Proof of Theorem 3.2. The proof is similar to that of Theorem 3.1. We use the same strategy of expanding the product $D_1 D_2^{(-1)}$, taking a modular reduction, and taking a projection

map. We highlight the places in which additional care is needed, in particular that there are two cases which must be evaluated separately.

Let G be a group containing a central subgroup E of index s isomorphic to $\mathbb{Z}_3^{d+1}$. Let $f_1, \ldots, f_s$ and $g_1, \ldots, g_s$ each be a set of coset representatives for E in G. Let $H_1, H_2, \ldots, H_s$ be the subgroups of G corresponding to the hyperplanes of E when E is regarded as a vector space of dimension $d+1$ over GF(3) and let

$$D_1 = f_1(E - H_1) + \sum_{i \neq 1} f_i H_i, \quad \text{and} \quad D_2 = g_m(E - H_m) + \sum_{j \neq m} g_j H_j,$$

where D_1 involves the complement in E of subgroup H_1, and D_2 involves the complement in E of subgroup H_m: we must examine both the cases $m = 1$ and $m \neq 1$. Suppose, for a contradiction, that there are integers μ, ν such that

$$D_1 D_2^{(-1)} = (\mu - \nu)D + \nu G \quad \text{in } \mathbb{Z}[G] \tag{3.9}$$

for some difference set D (having the same parameters (v, k, λ, n) as D_1, D_2) in G. By Lemma 1.17,

$$\nu = 3^{d-1}\frac{(s+1)(s+1 \pm 1)}{s} \quad \text{and} \quad \mu = \nu \mp 3^d. \tag{3.10}$$

By Lemma 3.5 we cannot take the upper signs in (3.10), and so (3.9) becomes

$$D_1 D_2^{(-1)} = 3^d D + 3^{d-1}(s+1)G. \tag{3.11}$$

Substitute for D_1 and D_2, and reduce modulo 3^d to give

$$\left(f_1(E - H_1) + \sum_{i \neq 1} f_i H_i\right)\left(g_m^{-1}(E - H_m) + \sum_{j \neq m} g_j^{-1} H_j\right) \equiv 3^{d-1}(s+1)G \pmod{3^d} \text{ in } \mathbb{Z}[G]. \tag{3.12}$$

Since $eE = E$ for $e \in E$, and $|H_i| = 3^d$, and $|E| = 3^{d+1}$, by Theorem 2.2 we have

$$H_i E \equiv EE \equiv H_i H_i \equiv 0 \pmod{3^d} \text{ in } \mathbb{Z}[G].$$

We therefore need retain on the left hand side of (3.12) only those terms involving $H_i H_j$ for distinct i, j.

Case 1: $m = 1$**.** By Theorem 2.2, the congruence (3.12) becomes

$$-3^{d-1}\sum_{j\neq 1} f_1 g_j^{-1} E - 3^{d-1}\sum_{i\neq 1} f_i g_1^{-1} E + 3^{d-1}\sum_{\substack{2\leq i,j\leq s\\ i\neq j}} f_i g_j^{-1} E \\ \equiv 3^{d-1}(s+1)G \pmod{3^d} \text{ in } \mathbb{Z}[G].$$

Applying a projection map ρ from G to E as in the proof of Theorem 3.1, we deduce that

$$-(s-1)E - (s-1)E + (s-1)(s-2)E \equiv (s+1)sE \pmod 3 \text{ in } \mathbb{Z}[E].$$

Since $s \equiv 1 \pmod 3$, this gives the contradiction

$$0 \equiv 2 \pmod 3.$$

Case 2: $m \neq 1$**.** By Theorem 2.2, the congruence (3.12) becomes

$$3^{d-1} f_1 g_m^{-1} E - 3^{d-1}\sum_{j\neq 1,m} f_1 g_j^{-1} E - 3^{d-1}\sum_{i\neq 1,m} f_i g_m^{-1} E + 3^{d-1}\sum_{\substack{1\leq i,j\leq s\\ i\neq 1, j\neq m, i\neq j}} f_i g_j^{-1} E \\ \equiv 3^{d-1}(s+1)G \pmod{3^d} \text{ in } \mathbb{Z}[G],$$

which after projection gives

$$E - (s-2)E - (s-2)E + \Big((s-1)^2 - (s-2)\Big)E \equiv (s+1)sE \pmod 3 \text{ in } \mathbb{Z}[E].$$

Since $s \equiv 1 \pmod 3$, this gives the contradiction

$$1 \equiv 2 \pmod 3.$$

□

Chapter 4

Construction in 2-Groups using Difference Matrices

In this chapter, we present a powerful construction (Theorem 4.2) of reduced linking systems of difference sets in 2-groups. Our construction relies on the unexpected use of difference matrices, which addresses Q4 of Section 1.4. In Section 4.1 we introduce the construction, combining combinatorial properties of hyperplanes (Theorem 2.2) and difference matrices (Section 2.3). The construction is not restricted to abelian groups; it is verified in the group ring without using character theory.

We then derive multiple corollaries of Theorem 4.2. In Section 4.2 we construct infinite families of reduced linking systems of difference sets in abelian groups, simplifying and extending some of the results of Theorem 1.27 due to Davis, Martin, and Polhill. In Section 4.3 we construct an infinite family of examples in nonabelian groups, whereas not a single nonabelian example was previously known. In Section 4.4 we obtain an infinite family of nonreversible examples generalizing Example 1.21, answering Q3 of Section 1.4. In Section 4.5 we show that the construction produces all possible examples of maximum size in the group $\mathbb{Z}_4^2$, and allows significant control over which difference sets in the reduced linking system are reversible.

4.1 Main Construction Theorem

In this section, we find sufficient conditions for the linking property (1.14) to hold for a pair of (McFarland) difference sets in a 2-group (Lemma 4.1). We then show that the rows of a difference matrix can be used to satisfy the sufficient pairwise conditions for a collection of difference sets simultaneously (Theorem 4.2).

Lemma 4.1. *Let d be a nonnegative integer and let $s = 2^{d+1} - 1$. Let G be a group of order 2^{2d+2} which contains a central subgroup E isomorphic to $\mathbb{Z}_2^{d+1}$. Suppose that $f_0, f_1, \dots f_s$ and $g_0, g_1, \dots, g_s$ are each a set of coset representatives for E in G such that*

$f_0g_0^{-1}, f_1g_1^{-1}, \ldots, f_sg_s^{-1}$ is also a set of coset representatives for E in G. Let $H_1, H_2, \ldots, H_s$ be the subgroups of G corresponding to the hyperplanes of E when E is regarded as a vector space of dimension $d+1$ over GF(2). *Then the sets*

$$D_1 = \sum_{i=1}^{s} f_i H_i \quad \text{and} \quad D_2 = \sum_{i=1}^{s} g_i H_i$$

are McFarland difference sets in G satisfying

$$D_1 D_2^{(-1)} = -2^d D + 2^{d-1} sG \quad \text{in } \mathbb{Z}[G],$$

where

$$D = \sum_{i=1}^{s} f_i g_i^{-1}(E - H_i) \tag{4.1}$$

is also a McFarland difference set in G.

Proof. The sets D_1 and D_2 are McFarland difference sets in G, by Theorem 2.5 with $q = 2$. Since each $H_i \subset E$ is central in G, we calculate in $\mathbb{Z}[G]$ that

$$D_1 D_2^{(-1)} = \left(\sum_{i=1}^{s} f_i H_i\right)\left(\sum_{j=1}^{s} H_j^{(-1)} g_j^{-1}\right) = \sum_{i=1}^{s} f_i g_i^{-1}(2^d H_i) + \sum_{\substack{1 \le i,j \le s \\ i \ne j}} f_i g_j^{-1}(2^{d-1} E) \tag{4.2}$$

using $H_j^{(-1)} = H_j$ and Theorem 2.2. By assumption, each of $\{f_i : 0 \le i \le s\}$ and $\{g_i : 0 \le i \le s\}$ and $\{f_i g_i^{-1} : 0 \le i \le s\}$ is a set of coset representatives for E in G and so

$$\begin{aligned} \sum_{i=1}^{s} f_i E &= G - f_0 E \\ \sum_{i=1}^{s} g_i^{-1} E &= G - g_0^{-1} E \\ \sum_{i=1}^{s} f_i g_i^{-1} E &= G - f_0 g_0^{-1} E. \end{aligned} \tag{4.3}$$

Therefore, by elementary manipulations,

$$\begin{aligned}\sum_{\substack{1\le i,j\le s\\ i\neq j}} f_i g_j^{-1} E &= \sum_{i=1}^{s} f_i \sum_{j=1}^{s} g_j^{-1} E - \sum_{i=1}^{s} f_i g_i^{-1} E \\ &= \sum_{i=1}^{s} f_i (G - g_0^{-1} E) - (G - f_0 g_0^{-1} E) \\ &= sG - (G - f_0 E) g_0^{-1} - (G - f_0 g_0^{-1} E) \\ &= (s-2)G + 2 f_0 g_0^{-1} E.\end{aligned}$$

Substitute into (4.2) to obtain

$$\begin{aligned}D_1 D_2^{(-1)} &= 2^d \sum_{i=1}^{s} f_i g_i^{-1} H_i + 2^{d-1} \left((s-2)G + 2 f_0 g_0^{-1} E \right) \qquad (4.4) \\ &= 2^d \left(-G + \sum_{i=1}^{s} f_i g_i^{-1} H_i + f_0 g_0^{-1} E \right) + 2^{d-1} sG \\ &= -2^d D + 2^{d-1} sG, \qquad (4.5)\end{aligned}$$

where

$$D = \sum_{i=1}^{s} f_i g_i^{-1} (E - H_i)$$

using (4.3).

It remains to show that D is a McFarland difference set in G. For each i we may write $E - H_i = a_i H_i$ for some $a_i \in E \cong \mathbb{Z}_2^{d+1}$ and then $D = \sum_{i=1}^{s} f_i g_i^{-1} a_i H_i$. Since $\{f_i g_i^{-1} : 0 \le i \le s\}$ is a set of coset representatives for E in G, so is $\{f_i g_i^{-1} a_i : 0 \le i \le s\}$ and therefore D is a McFarland difference set in G by Theorem 2.5. □

Lemma 4.1 shows that, subject to conditions on coset representatives, McFarland difference sets D_1, D_2 with $q = 2$ that are constructed as in Theorem 2.5 can form a reduced linking system. In view of the nonexistence result given in Theorem 3.1, it is natural to ask where Lemma 4.1 fails for $q > 2$. There are two such places. First, the expression

$$2^d \sum_{i=1}^{s} f_i g_i^{-1} H_i + 2^{d-1} \left((s-2)G + 2 f_0 g_0^{-1} E \right)$$

in (4.4) is replaced by

$$q^d \sum_{i=1}^{s} f_i g_i^{-1} H_i + q^{d-1} \left((s-2)G + 2 f_0 g_0^{-1} E \right),$$

so that the expression (4.5) for $D_1 D_2^{(-1)}$ now involves three distinct coefficients $-q^d, q^{d-1}s$, and $-2q^{d-1}$ (where $s = \frac{q^{d+1}-1}{q-1}$). Second, it is no longer possible to write $E - H_i = a_i H_i$ for some $a_i \in E$ because H_i has index q in E (where E is now isomorphic to the elementary abelian group of order q^{d+1}) .

We now illustrate aspects of the proof of Lemma 4.1 by reference to Example 1.19: a reduced $(16, 6, 2, 4; 2)$-linking system $\{D_1, D_2\}$ in $G = \mathbb{Z}_2^4 = \langle x, y, z, w \rangle$.

D_1

$\mathbf{1}_G$	y
x	xy

z	yz
xz	xyz

w	yw
xw	xyw

zw	yzw
xzw	$xyzw$

D_2

$\mathbf{1}_G$	y
x	xy

z	yz
xz	xyz

w	yw
xw	xyw

zw	yzw
xzw	$xyzw$

Let $E = \langle x, y \rangle$ and $H_1 = \langle x \rangle, H_2 = \langle y \rangle, H_3 = \langle xy \rangle$, and then we may represent D_1 and D_2 in the form

$$D_1 = yzH_1 + wH_2 + H_3$$
$$D_2 = wH_1 + xH_2 + zH_3.$$

Using this representation we may calculate $D_1 D_2^{(-1)} = D_1 D_2$ as the sum of contributions of terms involving $H_i H_j$ for $i \neq j$ and contributions of terms involving $H_i H_i$, and visualize these contributions using the usual grid form.

Terms in $H_i H_j$ with $i \neq j$

$3 \cdot \mathbf{1}_G$	$3y$
$3x$	$3xy$

z	yz
xz	xyz

w	yw
xw	xyw

zw	yzw
xzw	$xyzw$

Terms in H_iH_i

$0\cdot\mathbf{1}_G$	$0y$	$2z$	$0yz$
$0x$	$0xy$	$0xz$	$2xyz$

$0w$	$0yw$	$0zw$	$2yzw$
$2xw$	$2xyw$	$0xzw$	$2xyzw$

Total $D_1D_2^{(-1)}$

$3\cdot\mathbf{1}_G$	$3y$	$3z$	yz
$3x$	$3xy$	xz	$3xyz$

w	yw	zw	$3yzw$
$3xw$	$3xyw$	xzw	$3xyzw$

Theorem 4.2. *Let G be a group of order 2^{2d+2} which contains a central subgroup E isomorphic to $\mathbb{Z}_2^{d+1}$. Let $m \geq 3$ and suppose there exists a $(G/E, m, 1)$-difference matrix. Then G contains a reduced linking system of difference sets of size $m-1$.*

Proof. Let $s = 2^{d+1} - 1$ and let $H_1, H_2, \ldots, H_s$ be the subgroups of G corresponding to the hyperplanes of E when E is regarded as a vector space of dimension $d+1$ over GF(2). Let the $(G/E, m, 1)$-difference matrix be $B = (b_{i,j}E)$ for $0 \leq i \leq m-1$ and $0 \leq j \leq s$ and $b_{i,j} \in G$. As noted in Section 2.3, we may assume that for each distinct nonzero i, r, the sets $\{b_{i,j}E : 0 \leq j \leq s\}$ and $\{b_{i,j}b_{r,j}^{-1}E : 0 \leq j \leq s\}$ both contain every element of G/E exactly once. Therefore, the sets $\{b_{i,j} : 0 \leq j \leq s\}$ and $\{b_{i,j}b_{r,j}^{-1} : 0 \leq j \leq s\}$ are both a set of coset representatives for E in G. Choose $e_{i,j} \in E$ for each $1 \leq i \leq m-1$ and $1 \leq j \leq s$ arbitrarily. Since E is central in G, it follows that the sets $\{b_{i,j}e_{i,j} : 0 \leq j \leq s\}$ and $\{(b_{i,j}e_{i,j})(b_{r,j}e_{r,j})^{-1} : 0 \leq j \leq s\}$ are both a set of coset representatives for E in G.

Let

$$D_i = \sum_{j=1}^{s} b_{i,j}e_{i,j}H_j \quad \text{for } 1 \leq i \leq m-1. \tag{4.6}$$

We shall show that $\{D_1, D_2, \ldots, D_{m-1}\}$ is a reduced linking system of difference sets in G. By Definition 1.16 we require that each D_i is a difference set in G and that there are integers μ, ν such that for all distinct nonzero i, r,

$$D_iD_r^{(-1)} = (\mu - \nu)D(i, r) + \nu G$$

for some difference set $D(i, r)$ in G. This follows from Lemma 4.1 by taking $f_j = b_{i,j}e_{i,j}$ and $g_j = b_{r,j}e_{r,j}$. □

We now give an example of the construction method of Theorem 4.2 in which G is not an elementary abelian 2-group.

Example 4.3. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \langle x, y, z \rangle$ and let $E = \langle x^2, z \rangle$. The subgroups of G corresponding to the hyperplanes of E when E is regarded as a vector space of dimension 2 over GF(2) are $H_1 = \langle x^2 \rangle, H_2 = \langle z \rangle, H_3 = \langle x^2 z \rangle$. By Example 2.12,

$$(b_{i,j}) = \begin{pmatrix} \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G \\ \mathbf{1}_G & x & y & xy \\ \mathbf{1}_G & y & xy & x \\ \mathbf{1}_G & xy & x & y \end{pmatrix} \text{ for } 0 \leq i, j \leq 3$$

is a $(\mathbb{Z}_2^2, 4, 1)$-difference matrix and so $(b_{i,j}E)$ is a $(G/E, 4, 1)$-difference matrix. Take

$$(e_{i,j}) = \begin{pmatrix} \mathbf{1}_E & \mathbf{1}_E & \mathbf{1}_E \\ z & x^2 & x^2 \\ z & \mathbf{1}_E & \mathbf{1}_E \end{pmatrix} \text{ for } 1 \leq i, j \leq 3.$$

Then (4.6) gives the reduced linking system of McFarland difference sets

$$\begin{aligned} D_1 &= xH_1 + yH_2 + xyH_3 \\ D_2 &= yzH_1 + x^3yH_2 + x^3H_3 \\ D_3 &= xyzH_1 + xH_2 + yH_3, \end{aligned}$$

which we can represent as

D_1

$\mathbf{1}_G$	y
x	xy
x^2	x^2y
x^3	x^3y

z	yz
xz	xyz
x^2z	x^2yz
x^3z	x^3yz

D_2

$\mathbf{1}_G$	y
x	xy
x^2	x^2y
x^3	x^3y

z	yz
xz	xyz
x^2z	x^2yz
x^3z	x^3yz

D_3

$\mathbf{1}_G$	y
x	xy
x^2	x^2y
x^3	x^3y

z	yz
xz	xyz
x^2z	x^2yz
x^3z	x^3yz

One benefit of the construction method of Lemma 4.1 and Theorem 4.2 is that we can find the difference set $D(i,j)$ specified in Definition 1.16 directly from D_i and D_j. For example,

$$D_2 D_3^{(-1)} = -2D + 3G$$

where by (4.1) and (4.6) we obtain D as

$$\begin{aligned} D &= \sum_{j=1}^{3} (b_{2,j}e_{2,j})(b_{3,j}e_{3,j})^{-1}(E - H_j) \\ &= (yz)(xyz)^{-1}(E - H_1) + (x^3y)(x)^{-1}(E - H_2) + (x^3)(y)^{-1}(E - H_3) \\ &= x^3(zH_1) + x^2y(x^2H_2) + x^3y(zH_3) \\ &= xzH_1 + yH_2 + xyH_3. \end{aligned}$$

D

$\mathbf{1}_G$	y
x	xy
x^2	x^2y
x^3	x^3y

z	yz
xz	xyz
x^2z	x^2yz
x^3z	x^3yz

4.2 Infinite Families in Abelian Groups

In this section, we use Theorem 4.2 to construct infinite families of reduced linking systems of difference sets in a wide range of abelian 2-groups.

Corollary 4.4. *Let G be an abelian group of order 2^{2d+2}, rank at least $d+1$, and exponent at most 2^{d+1}. Then G contains a reduced linking system of difference sets of size 3.*

Proof. Write $G = \mathbb{Z}_{2^{a_1}} \times \cdots \times \mathbb{Z}_{2^{a_{d+1+t}}}$, where $t \geq 0$ and $a_1 \geq a_2 \geq \cdots \geq a_{d+1+t} \geq 1$ and $\sum_i a_i = 2d+2$. The first $d+1$ direct factors of G contain a subgroup E isomorphic to $\mathbb{Z}_2^{d+1}$, and

$$G/E \cong \mathbb{Z}_{2^{a_1-1}} \times \cdots \times \mathbb{Z}_{2^{a_{d+1}-1}} \times \mathbb{Z}_{2^{a_{d+2}}} \times \cdots \times \mathbb{Z}_{2^{a_{d+1+t}}}.$$

Now G/E has rank 1 only if $t = 0$ and $(a_1 - 1, a_2 - 1, \ldots, a_{d+1} - 1) = (d+1, 0, \ldots, 0)$, which is excluded by the assumption $\exp(G) \leq 2^{d+1}$. Therefore by Theorem 2.10 there exists a $(G/E, 4, 1)$-difference matrix and the result follows from Theorem 4.2. □

Corollary 4.5. *Let G be an abelian group of order 2^{2d+2}, rank at least $d+1$, and exponent 2^e, where $2 \leq e \leq \frac{d+3}{2}$. Then G contains a reduced linking system of difference sets of size $2^{\lfloor \frac{d+1}{e-1} \rfloor} - 1$.*

Proof. Write $G = \mathbb{Z}_{2^{a_1}} \times \cdots \times \mathbb{Z}_{2^{a_{d+1+t}}}$, where $t \geq 0$ and $e = a_1 \geq a_2 \geq \cdots \geq a_{d+1+t} \geq 1$ and $\sum_i a_i = 2d+2$. The first $d+1$ direct factors of G contain a subgroup E isomorphic to

$\mathbb{Z}_2^{d+1}$, and

$$G/E \cong \mathbb{Z}_{2^{a_1-1}} \times \cdots \times \mathbb{Z}_{2^{a_{d+1}-1}} \times \mathbb{Z}_{2^{a_{d+2}}} \times \cdots \times \mathbb{Z}_{2^{a_{d+1+t}}}.$$

Now $\exp(G/E) = \max(2^{a_1-1}, 2^{a_{d+2}})$, and $a_{d+2} \geq a_1$ only if $t = d+1$ and $a_1 = a_2 = \cdots = a_{2d+2} = 1$, which is excluded by the assumption $e \geq 2$. Therefore $\exp(G/E) = 2^{a_1-1} = 2^{e-1}$, and so by Theorem 2.11 there exists a $(G/E, 2^{\lfloor \frac{d+1}{e-1} \rfloor}, 1)$-difference matrix. The assumption $e \leq \frac{d+3}{2}$ implies that $2^{\lfloor \frac{d+1}{e-1} \rfloor} \geq 4$, and the result follows from Theorem 4.2.

□

Corollaries 4.4 and 4.5, together with Corollary 1.37, comprise the constructive results described in this thesis for reduced linking systems of difference sets in abelian groups. Table 4.1 summarizes these three results. In Tables 4.2 and 4.3 we illustrate the power of Corollaries 4.4 and 4.5 in relation to the best previously known results, by considering abelian groups of order 64 and 256. There are no known existence results for the groups of order 256 which are omitted from Table 4.3 (having rank at most 3 or exponent 32).

Table 4.1: Constructions of a reduced linking system of difference sets in an abelian group G of order 2^{2d+2}, rank at least $d+1$, and exponent 2^e.

Range of e	Size of System	Source
1	$2^{2d+1} - 1$	Bent Set (Corollary 1.37)
$[2, \frac{d+3}{2}]$	$2^{\lfloor \frac{d+1}{e-1} \rfloor} - 1$	Difference Matrix (Corollary 4.5)
$(\frac{d+3}{2}, d+1]$	3	Difference Matrix (Corollary 4.4)
$d+2$ (so $G = \mathbb{Z}_{2^{d+2}} \times \mathbb{Z}_2^d$)	No Result	

Table 4.2: Comparison of maximum known sizes of reduced linking systems of difference sets in abelian groups of order 64.

Group	Previous Maximum Known Size	Current Maximum Known Size	Source
$\mathbb{Z}_2^6$	31 [BK08]	31	Bent Set (Corollary 1.37)
$\mathbb{Z}_4 \times \mathbb{Z}_2^4$	None	7	Difference Matrix (Corollary 4.5)
$\mathbb{Z}_4^2 \times \mathbb{Z}_2^2$	None	7	Difference Matrix (Corollary 4.5)
$\mathbb{Z}_4^3$	7 [DMP14]	7	Difference Matrix (Corollary 4.5)
$\mathbb{Z}_8 \times \mathbb{Z}_2^3$	None	3	Difference Matrix (Corollary 4.4)
$\mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	None	3	Difference Matrix (Corollary 4.4)
$\mathbb{Z}_8^2$	None	None	
$\mathbb{Z}_{16} \times \mathbb{Z}_2^2$	None	None	
$\mathbb{Z}_{16} \times \mathbb{Z}_4$	None	None	

Table 4.3: Comparison of maximum known sizes of reduced linking systems of difference sets in abelian groups of order 256.

Group	Previous Maximum Known Size	Current Maximum Known Size	Source
$\mathbb{Z}_2^8$	127 [BK08]	127	Bent Set (Corollary 1.37)
$\mathbb{Z}_4 \times \mathbb{Z}_2^6$	None	15	Difference Matrix (Corollary 4.5)
$\mathbb{Z}_4^2 \times \mathbb{Z}_2^4$	3 [DMP14]	15	Difference Matrix (Corollary 4.5)
$\mathbb{Z}_4^3 \times \mathbb{Z}_2^2$	None	15	Difference Matrix (Corollary 4.5)
$\mathbb{Z}_4^4$	15 [DMP14]	15	Difference Matrix (Corollary 4.5)
$\mathbb{Z}_8 \times \mathbb{Z}_2^5$	None	3	Difference Matrix (Corollary 4.4)
$\mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2^3$	None	3	Difference Matrix (Corollary 4.4)
$\mathbb{Z}_8 \times \mathbb{Z}_4^2 \times \mathbb{Z}_2$	None	3	Difference Matrix (Corollary 4.4)
$\mathbb{Z}_8^2 \times \mathbb{Z}_2^2$	None	3	Difference Matrix (Corollary 4.4)
$\mathbb{Z}_{16} \times \mathbb{Z}_2^4$	None	3	Difference Matrix (Corollary 4.4)
$\mathbb{Z}_{16} \times \mathbb{Z}_4 \times \mathbb{Z}_2^2$	None	3	Difference Matrix (Corollary 4.4)

4.3 Infinite Family in Nonabelian Groups

We next use Theorem 4.2 to construct an infinite family of reduced linking systems of difference sets in nonabelian 2-groups. No example of a linking system of difference sets in a nonabelian group was previously known.

Corollary 4.6. *Let d be a positive integer, and let D_4 be the dihedral group of order 8. Let K be an abelian group of order 2^{2d-1} and exponent at most 4. Then $G = D_4 \times K$ contains a reduced linking system of difference sets of size $2^{d+1} - 1$.*

Proof. The group K contains a subgroup $E' \cong \mathbb{Z}_2^d$ such that $K/E' \cong \mathbb{Z}_2^{d-1}$. Write $D_4 = \langle a, b : a^4 = b^2 = 1, a^{-1} = bab^{-1} \rangle$. The center of D_4 is $\langle a^2 \rangle \cong \mathbb{Z}_2$, and $D_4/\langle a^2 \rangle \cong \mathbb{Z}_2^2$. Therefore $E = \langle a^2 \rangle \times E'$ is a central subgroup of G isomorphic to $\mathbb{Z}_2^{d+1}$ and $G/E \cong \mathbb{Z}_2^{d+1}$. By Theorem 2.11, there exists a $(G/E, 2^{d+1}, 1)$-difference matrix. The result follows from Theorem 4.2. □

Furthermore, we cannot produce a reduced linking system of difference sets of larger size than in Corollary 4.6 using the difference matrix construction of Theorem 4.2, because the $(G/E, 2^{d+1}, 1)$-difference matrix used in its proof satisfies the extremal condition $2^{d+1} = |G/E|$ (see Section 2.3). There are numerous variations of Corollary 4.6 which produce further examples in nonabelian 2-groups.

4.4 Infinite Nonreversible Family

Recall from Section 1.4 that all examples of reduced linking systems of difference sets given in [DMP14] are reversible (see the construction of Theorem 1.27), with the single exception

of Example 1.21. The authors of [DMP14] asked (Q3 of Section 1.4) whether there is an infinite family generalizing this example. In this section we show the answer is yes.

We first show that Example 1.21 can be realized using the construction (4.6) given in the proof of Theorem 4.2. Take $G = \mathbb{Z}_4^2 = \langle x, y \rangle$ and $E = \langle x^2, y^2 \rangle$ and $m = 4$, and let $H_1 = \langle x^2 \rangle, H_2 = \langle y^2 \rangle, H_3 = \langle x^2 y^2 \rangle$. Then we may represent the difference sets D_1, D_2, D_3 of Example 1.21 as

$$\begin{aligned} D_1 &= xH_1 + yH_2 + xy^3 H_3 \\ D_2 &= xyH_1 + xH_2 + y^3 H_3 \\ D_3 &= y^3 H_1 + x^3 y H_2 + xH_3, \end{aligned}$$

which have the form (4.6) when

$$(b_{i,j}) = \begin{pmatrix} \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G \\ \mathbf{1}_G & x & y & xy \\ \mathbf{1}_G & xy & x & y \\ \mathbf{1}_G & y & xy & x \end{pmatrix} \quad \text{for } 0 \le i, j \le 3$$

and

$$(e_{i,j}) = \begin{pmatrix} \mathbf{1}_E & \mathbf{1}_E & y^2 \\ \mathbf{1}_E & \mathbf{1}_E & y^2 \\ y^2 & x^2 & \mathbf{1}_E \end{pmatrix} \quad \text{for } 1 \le i, j \le 3.$$

D_1

$\mathbf{1}_G$	y	y^2	y^3
x	xy	xy^2	xy^3
x^2	x^2y	x^2y^2	x^2y^3
x^3	x^3y	x^3y^2	x^3y^3

D_2

$\mathbf{1}_G$	y	y^2	y^3
x	xy	xy^2	xy^3
x^2	x^2y	x^2y^2	x^2y^3
x^3	x^3y	x^3y^2	x^3y^3

D_3

$\mathbf{1}_G$	y	y^2	y^3
x	xy	xy^2	xy^3
x^2	x^2y	x^2y^2	x^2y^3
x^3	x^3y	x^3y^2	x^3y^3

This example has the property that D_1 is reversible, but neither D_2 nor D_3 is.

We now generalize Example 1.21.

Corollary 4.7. *The group $\mathbb{Z}_4^{d+1}$ contains a reduced linking system of difference sets of size $2^{d+1}-1$, at least one of whose difference sets is not reversible.*

Proof. Let $G = \mathbb{Z}_4^{d+1} = \langle x_1, x_2, \ldots, x_{d+1}\rangle$ and $E = \langle x_1^2, x_2^2, \ldots, x_{d+1}^2\rangle \cong \mathbb{Z}_2^{d+1}$. Then $G/E \cong \mathbb{Z}_2^{d+1}$ and by Theorem 2.11 there is a $(G/E, 2^{d+1}, 1)$-difference matrix $(b_{i,j}E)$, where each $b_{i,j}$ has the form $\prod_{r\in R(i,j)} x_r$ for some subset $R(i,j)$ of $\{1,2,\ldots,d+1\}$. Following the proof of Theorem 4.2, let $s = 2^{d+1}-1$ and let $H_1, H_2, \ldots, H_s$ be the subgroups of G corresponding to hyperplanes of E when E is regarded as a vector space of dimension $d+1$ over GF(2). We may take $H_1 = \langle x_2^2, x_3^2, \ldots, x_{d+1}^2\rangle$. We may also assume that for each $i \geq 1$, the set $\{b_{i,j}E : 0 \leq j \leq s\}$ contains no repeated element and that $b_{1,1} = x_1$. Now define D_i as in (4.6) for $m = 2^{d+1}$, taking $e_{1,1} = \mathbf{1}_E$. This gives a reduced linking system of difference sets in G of size $2^{d+1}-1$.

We now show that

$$D_1 = x_1H_1 + \sum_{j=2}^{s} b_{1,j}e_{1,j}H_j$$

is not reversible. Since $x_1 \in D_1$, it is sufficient to show that $x_1^3 \notin D_1$. Suppose, for a contradiction, that $x_1^3 \in D_1$. Since $x_1^2 \notin H_1$, this implies that $x_1^3 \in b_{1,j}e_{1,j}H_j$ for some $j > 1$. But $e_{1,j}H_j \subset E = \langle x_1^2, x_2^2, \ldots, x_{d+1}^2\rangle$, so by considering the parity of the exponent of each x_r in $b_{1,j} = \prod_{r\in R(1,j)} x_r$, we conclude that $b_{1,j}E = x_1E$ for some $j > 1$. This contradicts that the set $\{b_{i,j}E : 0 \leq j \leq s\}$ contains no repeated element. □

4.5 The Group $\mathbb{Z}_4^2$

We further illustrate the strength of the difference matrix construction of Theorem 4.2 by examining reduced linking systems of difference sets in $\mathbb{Z}_4^2 = \langle x, y\rangle$ of size 3. Let $m = 4$ and $E = \langle x^2, y^2\rangle$ and $H_1 = \langle x^2\rangle, H_2 = \langle y^2\rangle, H_3 = \langle x^2y^2\rangle$, so that (4.6) becomes

$$\begin{aligned} D_1 &= b_{1,1}e_{1,1}\langle x^2\rangle + b_{1,2}e_{1,2}\langle y^2\rangle + b_{1,3}e_{1,3}\langle x^2y^2\rangle \\ D_2 &= b_{2,1}e_{2,1}\langle x^2\rangle + b_{2,2}e_{2,2}\langle y^2\rangle + b_{2,3}e_{2,3}\langle x^2y^2\rangle \\ D_3 &= b_{3,1}e_{3,1}\langle x^2\rangle + b_{3,2}e_{3,2}\langle y^2\rangle + b_{3,3}e_{3,3}\langle x^2y^2\rangle. \end{aligned} \tag{4.7}$$

We first show that there are 2^{16} distinct reduced linking systems $\{D_1, D_2, D_3\}$ of this form; an exhaustive computer search shows that this accounts for all reduced linking systems of difference sets in $\mathbb{Z}_4^2$ of size 3, and that no larger system exists.

Each $e_{i,j} \in E$ can be chosen arbitrarily, and exactly 2 of the 4 choices for each $e_{i,j}$ give distinct values for the coset $e_{i,j}H_j$. This counts 2^9 choices. For $0 \le i, j \le 3$, the matrices

$$(b_{i,j}) = \begin{pmatrix} \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G \\ \mathbf{1}_G & x & y & xy \\ \mathbf{1}_G & y & xy & x \\ \mathbf{1}_G & xy & x & y \end{pmatrix} \text{ and } (b'_{i,j}) = \begin{pmatrix} \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G \\ \mathbf{1}_G & x & xy & y \\ \mathbf{1}_G & y & x & xy \\ \mathbf{1}_G & xy & y & x \end{pmatrix}$$

correspond to $(G/E, 4, 1)$-difference matrices $(b_{i,j}E)$ and $(b'_{i,j}E)$. We can multiply all entries of a row of either $(G/E, 4, 1)$-difference matrix by a fixed $a \in \{\mathbf{1}_G E, xE, yE, xyE\}$ without changing the defining property of the difference matrix. This gives 4^3 possible row multiples for rows $1, 2, 3$ of each of the matrices $(b_{i,j}E)$ and $(b'_{i,j}E)$, and so counts $2 \cdot 4^3 = 2^7$ choices. Moreover, we see from (4.7) that each of the resulting $2^9 \cdot 2^7 = 2^{16}$ choices gives a distinct reduced linking system $\{D_1, D_2, D_3\}$.

We next consider the reversibility of these 2^{16} reduced linking systems. We have already seen an example in Section 4.4 for which exactly one of the three difference sets is reversible. We can readily specify a reduced linking system for which none of the difference sets is reversible, for example by taking

$$(b_{i,j}) = \begin{pmatrix} \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G \\ \mathbf{1}_G & x & xy & y \\ \mathbf{1}_G & y & x & xy \\ \mathbf{1}_G & xy & y & x \end{pmatrix} \text{ and } (e_{i,j}) \text{ arbitrary,}$$

and a reduced linking system for which all three difference sets are reversible, for example by taking

$$(b_{i,j}) = \begin{pmatrix} \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G & \mathbf{1}_G \\ x & \mathbf{1}_G & y & xy \\ y & x & \mathbf{1}_G & xy \\ xy & x & y & \mathbf{1}_G \end{pmatrix} \text{ and } (e_{i,j}) \text{ arbitrary.}$$

Chapter 5

Open Problems

- Our main constructive result (Theorem 4.2) uses difference matrices as a crucial ingredient. Are there example of difference matrices in 2-groups other than those covered by Theorems 2.10 and 2.11? If so, this would immediately give new reduced linking systems of difference sets.
- Our main constructive result depends on Lemma 4.1, involving hyperplanes. Following Q4 of Section 1.4, is there a construction for reduced linking systems of difference sets involving a combinatorial object such as a partial difference set?
- Table 1.2 extends some of the previous results due to Davis, Martin, and Polhill [DMP14] for abelian 2-groups (Theorem 1.27), but does not explain all their results. Can the constructive framework of this paper be broadened to do so?
- There is a recursive construction for difference sets in the five known families whose parameters satisfy $\gcd(v, n) > 1$ (namely the Hadamard, McFarland, Spence, Davis-Jedwab, and Chen families) [DJ97], [Che97]. Is there an analogous recursive construction for reduced linking systems of difference sets?
- Q2 of Section 1.4 asks whether there is a linking system of difference sets in a non-2-group, and this question remains open despite the nonexistence results of Chapter 3. Can this question be resolved constructively, or else can its scope be narrowed by finding further nonexistence results similar to Theorems 3.1 and 3.2?
- We have counted all reduced linking systems of difference sets in the group $\mathbb{Z}_4^2$ having maximum size (Section 4.5). Can this counting result be extended to other groups?

Bibliography

[Ass89] E. F. Assmus, Jr. On the theory of designs. In *Surveys in Combinatorics, 1989 (Norwich, 1989)*, volume 141 of *London Math. Soc. Lecture Note Ser.*, pages 1–21. Cambridge Univ. Press, Cambridge, 1989.

[BJL99] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1999.

[BK08] C. Bey and G. M. Kyureghyan. On Boolean functions with the sum of every two of them being bent. *Des. Codes Cryptogr.*, 49(1-3):341–346, 2008.

[Bur98] M. Buratti. Recursive constructions for difference matrices and relative difference families. *J. Combin. Des.*, 6(3):165–182, 1998.

[Che97] Y. Q. Chen. On the existence of abelian Hadamard difference sets and a new family of difference sets. *Finite Fields Appl.*, 3(3):234–256, 1997.

[Che98] Y. Q. Chen. A construction of difference sets. *Des. Codes Cryptogr.*, 13(3):247–250, 1998.

[Dil74] J. F. Dillon. *Elementary Hadamard Difference-Sets*. PhD thesis, University of Maryland, 1974.

[Dil85] J. F. Dillon. Variations on a scheme of McFarland for noncyclic difference sets. *J. Combin. Theory Ser. A*, 40(1):9–21, 1985.

[DJ97] J. A. Davis and J. Jedwab. A unifying construction for difference sets. *J. Combin. Theory Ser. A*, 80(1):13–78, 1997.

[DMP14] J. A. Davis, W. J. Martin, and J. B. Polhill. Linking systems in nonelementary abelian groups. *J. Combin. Theory Ser. A*, 123:92–103, 2014.

[Fis26] R. A. Fisher. The arrangement of field experiments. 1926. Reprinted in Breakthroughs in Statistics, pages 82–91. Springer, 1992.

[Hal67] M. Hall, Jr. *Combinatorial Theory*. Blaisdell Publishing Co. Ginn and Co., Waltham, Mass.-Toronto, Ont.-London, 1967.

[JS97] D. Jungnickel and B. Schmidt. Difference sets: an update. In *Geometry, combinatorial designs and related structures (Spetses, 1996)*, volume 245 of *London Math. Soc. Lecture Note Ser.*, pages 89–112. Cambridge Univ. Press, Cambridge, 1997.

[JS98] D. Jungnickel and B. Schmidt. Difference sets: a second update. *Rend. Circ. Mat. Palermo (2) Suppl.*, (53):89–118, 1998. Combinatorics '98 (Mondello).

[Jun92] D. Jungnickel. Difference sets. *Contemporary Design Theory: A Collection of Surveys*, pages 241–324, 1992.

[Ker72] A. M Kerdock. A class of low-rate nonlinear binary codes. *Information and control*, 20(2):182–187, 1972.

[Kra93] R. G. Kraemer. Proof of a conjecture on Hadamard 2-groups. *J. Combin. Theory Ser. A*, 63(1):1–10, 1993.

[Lam01] T. Y. Lam. *A First Course in Noncommutative Rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.

[McF73] R. L. McFarland. A family of difference sets in non-cyclic groups. *J. Combin. Theory Ser. A*, 15:1–10, 1973.

[Men62] P. K. Menon. On difference sets whose parameters satisfy a certain relation. *Proc. Amer. Math. Soc.*, 13(5):739–745, 1962.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Elsevier, 1977.

[MS97] S. L. Ma and B. Schmidt. A sharp exponent bound for McFarland difference sets with $p = 2$. *J. Combin. Theory Ser. A*, 80(2):347–352, 1997.

[Nod74] R. Noda. On homogeneous systems of linked symmetric designs. *Math. Z.*, 138:15–20, 1974.

[Pal33] R. Paley. On orthogonal matrices. *Studies in Applied Mathematics*, 12(1-4):311–320, 1933.

[PC16] R. Pan and Y. Chang. A note on difference matrices over non-cyclic finite abelian groups. *Discrete Math.*, 339(2):822–830, 2016.

[Rys63] H. J. Ryser. *Combinatorial Mathematics*. The Carus Mathematical Monographs, No. 14. Published by The Mathematical Association of America; distributed by John Wiley and Sons, Inc., New York, 1963.

[Sin38] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43(3):377–385, 1938.

[Spe77] E. Spence. A family of difference sets. *J. Combin. Theory Ser. A*, 22(1):103–106, 1977.

[Tur65] R. J. Turyn. Character sums and difference sets. *Pacific J. Math.*, 15:319–346, 1965.

[vD99] E. R. van Dam. Three-class association schemes. *J. Algebraic Combin.*, 10(1):69–107, 1999.