Linking systems of difference sets

Jonathan Jedwab   Shuxing Li   Samuel Simon

14 August 2017 (revised 20 April 2018)

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 constructive results for linking systems of difference sets are restricted to 2-groups. We use an elementary projection argument to show that neither the McFarland/Dillon nor the Spence construction of difference sets can give rise to a linking system of difference sets in non-2-groups. We make a connection to Kerdock and bent sets, which provides large linking systems of difference sets in elementary abelian 2-groups. We 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 linking systems than before in certain 2-groups, new linking systems in other 2-groups for which no system was previously known, and the first known examples in nonabelian groups.

1   Introduction

1.1   Difference sets

The study of difference sets lies at the intersection of combinatorics, finite geometry, and coding theory [Jun92], [JS97], [JS98]. The advantageous structural properties of difference sets enable the solution of problems in radar, optical image alignment, and other areas of digital communication [DJ97]. Difference sets occur within the larger context of the theory of experimental design: a difference set in a group G is equivalent to a symmetric design with a regular automorphism group G [Lan83].

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. The cases $k = 0$ and $k = 1$ are considered trivial, and by taking the complement of a difference set if necessary we may assume that $k \leq v/2$. We shall be concerned with the following three parameter families (v, k, λ, n) of difference sets, where q is a prime power, d is a nonnegative integer, and N is a positive integer.

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}
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}
Hadamard	$4N^2$	$N(2N-1)$	$N(N-1)$	N^2

The McFarland parameters with $q = 2$ are the same as the Hadamard parameters with $N = 2^d$, and the corresponding difference sets occur in 2-groups. Theorem 1.2 shows that the parameters of all (nontrivial) difference sets in 2-groups must take this common form.

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

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

Theorem 1.3 gives necessary and sufficient conditions for the existence of a difference set in an abelian 2-group. (The *exponent* of a group G with identity $\mathbf{1}_G$ is the smallest positive integer α for which $g^\alpha = \mathbf{1}_G$ for all $g \in G$, and is written $\exp(G)$.)

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

By a common notation convention, we identify a multiset of elements of the group G with its corresponding element in the group ring $\mathbb{Z}[G]$. Given a multiset S of elements of the group G, we write $S^{(-1)}$ for the group ring element $\sum_{s \in S} s^{-1}$, where the sum is over the elements in the multiset S and the inverse is taken in G. The following result is then a direct consequence of the definition of a difference set and the relation $n = k - \lambda$.

Lemma 1.4. *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*

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

1.2 Linking systems of difference sets

Linking systems of difference sets were introduced by Davis, Martin, and Polhill [DMP14]. Such a system gives rise to a system of linked symmetric designs, as introduced by Cameron [Cam72] and studied by Cameron and Seidel [CS73], and is equivalent to a 3-class Q-antipodal cometric association scheme [vD99]. Kodalen [Kod17] recently constructed the first known examples of systems of linked symmetric designs in non-2-groups, but it remains an important open question as to whether linking systems of difference sets can exist in non-2-groups.

Definition 1.5. *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 $\mathbb{Z}[G]$:*

$$D_{h,i}D_{i,j} = (\mu - \nu)D_{h,j} + \nu G \tag{2}$$

$$D_{i,j} = D_{j,i}^{(-1)}. \tag{3}$$

The central problems are to determine which groups contain a linking system of difference sets, and how large such a system can be. Definition 1.5 is rather cumbersome. We define a simpler object in Definition 1.6 and show in Proposition 1.7 (whose proof we postpone until Section 2) that it is equivalent to a linking system of difference sets.

Definition 1.6. *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 of size ℓ 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*

$$D_i D_j^{(-1)} = (\mu - \nu)D(i,j) + \nu G \quad \text{ in } \mathbb{Z}[G]. \tag{4}$$

Note that the difference set $D(i,j)$ in (4) is not necessarily contained in the collection $\mathcal{R}$. Note also that $\{D_1, D_2, \ldots, D_\ell\}$ is a reduced $(v,k,\lambda,n;\ell)$-linking system of difference sets in G with respect to μ, ν if and only if $\{G - D_1, G - D_2, \ldots, G - D_\ell\}$ is a reduced $(v,v-k,v-2k+\lambda,n;\ell)$-linking system of difference sets in G with respect to $v - 2k + \nu$, $v - 2k + \mu$, so we may assume that $k \leq v/2$.

Proposition 1.7. *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.*

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

Example 1.8 ([DMP14, Example 6.3]). *Let $G = \mathbb{Z}_4^2 = \langle x,y \rangle$ and let $D_1 = x + x^3y + y^3 + x^3 + xy^3 + y$, $D_2 = x + x^3y + y^3 + xy^2 + xy + x^2y$, $D_3 = x + x^3y + y^3 + x^2y^3 + x^3y^3 + x^3y^2$. For each i we have $D_i D_i^{(-1)} = 4 \cdot \mathbf{1}_G + 2G$, so D_i is a difference set in G by Lemma 1.4. Furthermore*

$$D_2 D_1^{(-1)} = -2D + 3G,$$

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 $D_i D_j^{(-1)}$ for each distinct i,j shows that $\{D_1, D_2, D_3\}$ forms a reduced $(16,6,2,4;3)$-linking system of difference sets in G. The difference set D_1 is reversible, but neither D_2 nor D_3 is.

Definition 1.9. *Suppose $\mathcal{L} = \{D_{i,j} : 0 \leq i,j \leq \ell \text{ and } i \neq j\}$ is 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 1.10. *Suppose $\mathcal{R} = \{D_1, D_2, \cdots, D_\ell\}$ is 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 1.7) is reversible, then $\mathcal{R}$ is a reversible reduced $(v,k,\lambda,n;\ell)$-linking system of difference sets in G.*

3

1.3 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 1.8.

The main result of [DMP14] depends on several theorems: a base construction [DMP14, Theorem 5.3] for a reversible reduced linking system of difference sets from partial difference sets having intricate mutual properties; a product construction [DMP14, Theorem 3.1] for combining two reversible reduced linking systems of Hadamard difference sets into a larger one; and a construction for a reversible reduced linking system of difference sets using Galois rings [DMP14, Theorem 4.6]. These are combined to give the following result (in which we have corrected some typographical errors and oversights in [DMP14] following private communication with the authors). Note from Theorem 1.2 that the parameters of a difference set in a 2-group are determined by the order of the group.

Theorem 1.11 (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	$2^{\min(b_1, b_2, \ldots, b_k)} - 1$
$\mathbb{Z}_4^b$	$2^b - 1$
$G \times \mathbb{Z}_4^b$	$2^{\min(b_1, b_2, \ldots, b_k, b)} - 1$

1.4 Overview of paper

The paper [DMP14]) concludes with five open problems, of which we shall address the following (originally numbered 1, 3, 4, and 5).

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 1.8]?*

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

In Section 2 we prove the equivalence stated in Proposition 1.7, which requires particular care when the group G is nonabelian.

In Section 3 we reinterpret previous work on systems of linked symmetric designs and bent sets in order to produce a large reduced linking system of difference sets in the elementary abelian group $\mathbb{Z}_2^{2d+2}$, giving a partial answer to Q1.

In Section 4 we uncover an obstruction to the existence of a reduced linking system of McFarland difference sets having $q > 2$, and a reduced linking system of Spence difference sets, using only

elementary arguments that depend on a well-chosen modular reduction in the group ring. Since the associated groups are non-2-groups, this provides a partial answer to Q2.

In Section 5 we seek further constructions in 2-groups. Our main construction (Theorem 5.6) relies on the unexpected use of group difference matrices, which addresses Q4. We derive multiple corollaries of this construction, as summarized in Table 1 and illustrated in Table 2 for abelian groups of order 64. Tables 1 and 2 also include the constructive result of Section 3. (By Theorem 1.3, we need not consider groups of exponent greater than 2^{d+2} in Table 1, nor those of exponent greater than 16 in Table 2. 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 1.8, answering Q3. Finally, we give a detailed examination of reduced linking systems of difference sets in $\mathbb{Z}_4^2$.

In Section 6 we suggest directions for further research by posing several open problems.

Table 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 3.6)
$[2, \frac{d+3}{2}]$	$2^{\lfloor \frac{d+1}{e-1} \rfloor} - 1$	Difference matrix (Corollary 5.9)
$(\frac{d+3}{2}, d+1]$	3	Difference matrix (Corollary 5.8)
$d+2$ (so $G = \mathbb{Z}_{2^{d+2}} \times \mathbb{Z}_2^d$)	No result	

Table 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 3.6)
$\mathbb{Z}_4 \times \mathbb{Z}_2^4$	None	7	Difference matrix (Corollary 5.9)
$\mathbb{Z}_4^2 \times \mathbb{Z}_2^2$	None	7	Difference matrix (Corollary 5.9)
$\mathbb{Z}_4^3$	7 [DMP14]	7	Difference matrix (Corollary 5.9)
$\mathbb{Z}_8 \times \mathbb{Z}_2^3$	None	3	Difference matrix (Corollary 5.8)
$\mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	None	3	Difference matrix (Corollary 5.8)
$\mathbb{Z}_8^2$	None	None	
$\mathbb{Z}_{16} \times \mathbb{Z}_2^2$	None	None	
$\mathbb{Z}_{16} \times \mathbb{Z}_4$	None	None	

2 Proof of Proposition 1.7

In this section we prove Proposition 1.7. An outline of the main argument of the proof is implicit in [DMP14], although many details are omitted there and particular care is needed when the group G is nonabelian. We firstly use the classical result of Proposition 2.1 to show in Lemma 2.2 that the parameters μ, ν in a reduced linking system of difference sets are determined to within a sign. Lemma 2.2 corresponds to a result stated by Noda [Nod74, Proposition 0] for systems of linked symmetric designs.

Proposition 2.1 ([Bru55, p. 468])**.** *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.*

Lemma 2.2. *Suppose $\{D_1, D_2, \ldots, D_\ell\}$ 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 $1 \leq i, j \leq \ell$. By Definition 1.6, there is a (v, k, λ, n)-difference set $D(i, j)$ in G such that

$$D_i D_j^{(-1)} = (\mu - \nu)D(i, j) + \nu G \quad \text{in } \mathbb{Z}[G], \tag{5}$$

and so

$$\begin{aligned}
\left((\mu - \nu)D(i, j)\right)\left((\mu - \nu)D(i, j)^{(-1)}\right) &= \left(D_i D_j^{(-1)} - \nu G\right)\left(D_j D_i^{(-1)} - \nu G\right) \\
&= D_i\left(D_j^{(-1)} D_j\right)D_i^{(-1)} - 2\nu k^2 G + \nu^2 v G \tag{6}
\end{aligned}$$

because, for a subset S of G, we have $SG = GS = |S|G$ in $\mathbb{Z}[G]$. Now D_i and D_j and $D(i, j)$ are each (v, k, λ, n)-difference sets in G, and by Proposition 2.1 so is $D_j^{(-1)}$. Using Lemma 1.4 we therefore find from (6) that

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

Since the coefficients of $G - \mathbf{1}_G$ on both sides must be equal, comparison of the coefficients of $\mathbf{1}_G$ shows that

$$\mu - \nu = \mp\sqrt{n}. \tag{7}$$

Counting terms on both sides of (5) then gives

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

which together with (7) establishes the required values for μ and ν. $\qquad\square$

We can now prove Proposition 1.7.

Proof of Proposition 1.7. 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 G with respect to μ, ν. Let $D_i = D_{i,0}$ for $1 \leq i \leq \ell$ 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 (3) and (2). 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 $1 \leq i \leq \ell$. For distinct i, j not equal to 0, let $D_{i,j}$ be the difference set $D(i, j)$ given by Definition 1.6 applied to $D_{i,0}$ and $D_{j,0}$, so that

$$D_{i,0} D_{j,0}^{(-1)} = (\mu - \nu) D_{i,j} + \nu G. \tag{8}$$

We shall show that $\mathcal{L} = \{D_{i,j} : 0 \leq i, j \leq \ell \text{ and } i \neq j\}$ is a $(v, k, \lambda, n; \ell + 1)$-linking system of difference sets in G with respect to μ, ν by showing that (2) and (3) hold.

To show (3) for distinct i, j, one of which is 0, use the definition of $D_{i,0}$ and $D_{0,i}$. To show (3) for distinct i, j, both of which are not 0, apply the operation $^{(-1)}$ to both sides of (8) 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 (8), we conclude that $D_{i,j} = D_{j,i}^{(-1)}$, giving (3).

To show (2) for distinct i, j, h, all of which are not 0, use (8) to form the product

$$\left((\mu - \nu) D_{h,i} \right) \left((\mu - \nu) D_{i,j} \right) = \left(D_{h,0} D_{i,0}^{(-1)} - \nu G \right) \left(D_{i,0} D_{j,0}^{(-1)} - \nu G \right)$$
$$= D_{h,0} (D_{i,0}^{(-1)} D_{i,0}) D_{j,0}^{(-1)} - 2\nu k^2 G + \nu^2 v G. \tag{9}$$

From Lemma 2.2 we have $(\mu - \nu)^2 = n$. Since $D_{i,0}$ is a (v, k, λ, n)-difference set in G, by Proposition 2.1 so is $D_{i,0}^{(-1)}$. Using Lemma 1.4 we therefore find from (9) that

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

Counting terms on both sides shows that $\lambda k^2 - 2\nu k^2 + \nu^2 v = 0$, so that

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

using (8) again, as required for (2).

It remains to show (2) 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 (8) we have

$$(\mu - \nu) D_{0,i} D_{i,j} = D_i^{(-1)} (D_i D_j^{(-1)} - \nu G)$$
$$= (n \mathbf{1}_G + \lambda G) D_j^{(-1)} - \nu k G$$
$$= n D_{0,j} + (\lambda - \nu) k G$$
$$= (\mu - \nu)^2 D_{0,j} + (\lambda - \nu) k G, \tag{10}$$

which gives (2) provided the relation

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

holds. This relation follows by multiplying (8) by $\mu - \nu$, subtracting (10), and then counting terms on both sides.

$\square$

By Proposition 2.1, the values of the parameters μ, ν for a (non-reduced) linking system of difference sets are also as stated in Lemma 2.2. These values were noted in [DMP14, p. 94] (with a typographical error switching their values) as following from [Nod74, Proposition 0].

3 Bent sets

Bey and Kyureghyan [BK08], building on earlier work of Cameron and Seidel [CS73], Delsarte [Del73], and Noda [Nod74], provide the second of the two principal references on linking systems of difference sets. Their main result is phrased in terms of systems of linked symmetric designs, rather than linking systems of difference sets (which were not defined until 2014 in [DMP14]). In this section we rephrase the main result of [BK08] in terms of the newer terminology to give Corollary 3.6 and to clarify some of the relationships to previous work. Corollary 3.6 partially answers Q1 of Section 1.4 by showing how the construction of [DMP14, Example 6.2] can be improved using a Kerdock set.

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

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

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

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

Bent functions are closely connected to difference sets in elementary abelian 2-groups, as shown in the following result.

Theorem 3.2 ([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 3.3. *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 result of [BK08], rephrased in terms of linking systems of difference sets.

8

Theorem 3.4 (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 $\mathbb{Z}_2^{2d+2}$.*

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

Theorem 3.5 ([Ker72], [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}.*

We remark that Cameron and Seidel [CS73] used a Kerdock set to construct a system of linked symmetric designs, and that Theorem 3.4 generalizes their construction by replacing a Kerdock set with a bent set. Combining Theorems 3.4 and 3.5, we obtain the following corollary. Note that the parameters of the difference sets in Corollary 3.6 are determined by Theorem 1.2.

Corollary 3.6. *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 refer to [Sim17, Example 1.38] for an example of a bent set on $\mathbb{Z}_2^4$ of size 8 and the corresponding reduced $(16, 6, 2, 4; 7)$-linking system of difference sets in $\mathbb{Z}_2^4$.

We cannot use Theorem 3.4 to produce a reduced system of linking difference sets larger than that in Corollary 3.6, because the bent sets of Theorem 3.5 attain the maximum size by the following result.

Theorem 3.7 (Delsarte [Del73, p. 82], 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}.*

4 Nonexistence results in non-2-groups

Several authors have established constraints on the existence of systems of linked symmetric designs [Cam72], [Nod74], [Mat81], [Kod17], which in turn imply the nonexistence of corresponding linking systems of difference sets. In particular, Kodalen [Kod17, Appendix 1] determined which of the 21 known families of symmetric designs have parameters that satisfy integrality conditions (corresponding to those arising from Lemma 2.2) necessary for a system of linked symmetric designs to exist. However, nonexistence results that apply only to linking systems of difference sets have not previously been found. In this section we uncover an obstruction to the existence of a reduced linking system of difference sets in non-2-groups, both when the difference sets are constructed by the McFarland/Dillon method (Theorem 4.2) and when they are constructed by the Spence method (Theorem 4.3). The results are not restricted to abelian groups.

Our nonexistence proofs use only elementary arguments, combining properties of hyperplanes given in Proposition 4.9, modular reduction in the group ring, and projection to a subgroup. Each of these techniques is well-known; the novelty of the proof lies in recognizing the correct modular reduction, and in combining the various ingredients in the correct order.

4.1 McFarland/Dillon and Spence constructions

We first present the constructions originally given by McFarland (and later modified by Dillon) and Spence for the parameter families named after them. Both constructions rely on the properties of hyperplanes of a vector space.

Definition 4.1. *Let V be a vector space of dimension $d+1$ over* $\mathrm{GF}(q)$. *A hyperplane of V is a d-dimensional subspace of V.*

The number of hyperplanes in the vector space V of Definition 4.1 is $\frac{q^{d+1}-1}{q-1}$.

Theorem 4.2 (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 difference set in G with McFarland parameters $(v, k, \lambda, n) = (q^{d+1}(s+1), q^d s, q^d(s-q^d), q^{2d})$.

Theorem 4.3 (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* $\mathrm{GF}(3)$. *Then*

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

is a difference in G 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 the McFarland/Dillon construction of Theorem 4.2: the subgroup E has index $s+1$ in G; the subgroups $H_1, H_2, \ldots, H_s$ of G corresponding to the hyperplanes of E depend on the isomorphism ϕ when q is not a prime; and the difference set D comprises one coset of each of these s subgroups. In contrast, in the Spence construction of Theorem 4.3: the subgroup E has index s in G; the subgroups $H_1, H_2, \ldots, H_s$ of G corresponding to the hyperplanes of E are determined without reference to an isomorphism ϕ, because the construction is over the prime field $\mathrm{GF}(3)$; and the difference set D comprises a coset of the complement in E of one of the subgroups together with a coset of each of the remaining $s-1$ subgroups. Note that constructions other than Theorem 4.2 are known for difference sets with McFarland parameters [DJ97].

We now state our two nonexistence results.

Theorem 4.4. *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 4.2 with respect to the same subgroup E and the same isomorphism ϕ.

Theorem 4.5. *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 4.3.

10

The condition in Theorem 4.4, 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: 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 4.5. The condition in Theorem 4.4, that the two difference sets are constructed with respect to the same isomorphism ϕ, can be omitted when q is a prime.

By imposing the condition that d should be a positive integer in Theorems 4.4 and 4.5, we exclude trivial McFarland and Spence difference sets containing a single element. We can obtain a stronger nonexistence result than Theorem 4.5 in the case $d = 1$ 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 4.3 (for some labelling of the subgroups H_1, H_2, H_3, H_4).

Corollary 4.6. *There is no reduced linking system of $(36, 15, 6, 9)$-difference sets in an abelian group.*

The parameters of a (v, k, λ, n)-difference set in $\mathbb{Z}_2^2 \times \mathbb{Z}_3^2$ or $\mathbb{Z}_4 \times \mathbb{Z}_3^2$ satisfying $2 \leq k \leq v/2$ must be $(36, 15, 6, 9)$, by solving the difference set counting relation $k(k-1) = \lambda(v-1)$ for $v = 36$. Therefore by Corollary 4.6, each of $\mathbb{Z}_2^2 \times \mathbb{Z}_3^2$ and $\mathbb{Z}_4 \times \mathbb{Z}_3^2$ is an abelian group G for which it is known that a (v, k, λ, n)-difference set exists in G and the corresponding values of μ and ν specified in Lemma 2.2 are integers, but a (reduced) linking system of difference sets does not exist in G. The only other such abelian group we are aware of is $\mathbb{Z}_8 \times \mathbb{Z}_2$, for which we determined the nonexistence result using Theorem 1.2 and exhaustive search.

4.2 Proof of Theorems 4.4 and 4.5

We next derive some divisibility conditions (Lemmas 4.7 and 4.8), and state a well-known result on hyperplanes (Proposition 4.9).

Lemma 4.7. *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

$$s+1 \text{ divides } q^{d-1}(s-1). \tag{11}$$

Note that

$$s+1 = 2 + q + q^2 + \cdots + q^d. \tag{12}$$

Case 1: q is odd. We have $\gcd(s+1, q) = 1$ from (12) and then (11) implies that $s+1$ divides $s-1$. This is a contradiction because $s > 1$.

Case 2: $q > 2$ is a power of 2. Then s is odd and so $\gcd(s+1, s-1) = 2$. Then (11) implies that $s+1$ divides $2q^{d-1}$. This is a contradiction because $s+1$ is not a power of 2, by (12), whereas $2q^{d-1}$ is a power of 2.

$\square$

Lemma 4.8. *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 $s > 2$. $\square$

Proposition 4.9 ([McF73]). *Let H_i and H_j be hyperplanes of a vector space V of dimension $d+1$ over $\mathrm{GF}(q)$. Then in the group ring $\mathbb{Z}[V]$,*

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

We can now prove Theorems 4.4 and 4.5.

Proof of Theorem 4.4. 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, under an isomorphism ϕ, when E is regarded as a vector space of dimension $d+1$ over $\mathrm{GF}(q)$ and let

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

Suppose, for a contradiction, that there are integers μ, ν such that

$$D_1 D_2^{(-1)} = (\mu - \nu)D + \nu G \quad \text{in } \mathbb{Z}[G] \tag{13}$$

for some difference set D (having the same parameters (v, k, λ, n) as D_1, D_2) in G. By Lemma 2.2,

$$\nu = q^{d-1} \frac{s(s \pm 1)}{s+1} \quad \text{and} \quad \mu = \nu \mp q^d. \tag{14}$$

By Lemma 4.7 we cannot take the lower signs in (14), and so (13) becomes

$$D_1 D_2^{(-1)} = -q^d D + q^{d-1} s G. \tag{15}$$

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

$$D_1 D_2^{(-1)} = \sum_{i=1}^{s} f_i H_i \sum_{j=1}^{s} (g_j H_j)^{(-1)}$$

$$= \sum_{1 \leq i,j \leq s} f_i g_j^{-1} H_i H_j$$

$$= \sum_{i=1}^{s} f_i g_i^{-1} (q^d H_i) + \sum_{\substack{1 \leq i,j \leq s \\ i \neq j}} f_i g_j^{-1} (q^{d-1} E),$$

by separating into sums over $i = j$ and $i \neq j$, and using Proposition 4.9. Substitute into (15) and reduce modulo q^d to obtain

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

Therefore

$$\sum_{\substack{1 \le i,j \le s \\ i \ne j}} f_i g_j^{-1} E \equiv sG \pmod{q} \quad \text{in } \mathbb{Z}[G]. \tag{16}$$

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 $k_t e$ for some $k_t \in K$ and some $e \in E$, from which we define a projection map $\rho : G \to E$ by

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

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 $G = \sum_{t=0}^{s} \sum_{e \in E} k_t e$ so that (16) becomes

$$\sum_{\substack{1 \le i,j \le s \\ i \ne j}} \sum_{e \in E} k_{t(i,j)} e_{i,j} e \equiv s \sum_{t=0}^{s} \sum_{e \in E} k_t e \pmod{q} \quad \text{in } \mathbb{Z}[G]. \tag{17}$$

Apply ρ to both sides to give

$$\sum_{\substack{1 \le i,j \le s \\ i \ne j}} \sum_{e \in E} e_{i,j} e \equiv s \sum_{t=0}^{s} \sum_{e \in E} e \pmod{q} \quad \text{in } \mathbb{Z}[E]. \tag{18}$$

Using $\sum_{e \in E} e_{i,j} e = e_{i,j} E = E$ then 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 $q > 2$. $\qquad\square$

Proof of Theorem 4.5. The proof is similar to that of Theorem 4.4. 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.

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

13

of G corresponding to the hyperplanes of E when E is regarded as a vector space of dimension $d+1$ over $\mathrm{GF}(3)$ 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

$$D_1 D_2^{(-1)} = (\mu - \nu)D + \nu G \quad \text{in } \mathbb{Z}[G] \tag{19}$$

for some difference set D (having the same parameters (v, k, λ, n) as D_1, D_2) in G. By Lemma 2.2,

$$\nu = 3^{d-1} \frac{(s+1)(s+1 \pm 1)}{s} \quad \text{and} \quad \mu = \nu \mp 3^d. \tag{20}$$

By Lemma 4.8 we cannot take the upper signs in (20), and so (19) becomes

$$D_1 D_2^{(-1)} = 3^d D + 3^{d-1}(s+1)G. \tag{21}$$

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

$$\left(f_1(E - H_1) + \sum_{i \neq 1} f_i H_i \right) \left(g_m^{-1}(E - H_m) + \sum_{j \neq m} g_j^{-1} H_j \right) \equiv 3^{d-1}(s+1)G \pmod{3^d} \text{ in } \mathbb{Z}[G]. \tag{22}$$

By Proposition 4.9,

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

and so we need retain on the left hand side of (22) only those terms involving $H_i H_j$ for distinct i, j.

Case 1: $m = 1$. By Proposition 4.9, the congruence (22) 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 4.4, 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 Proposition 4.9, the congruence (22) becomes

$$3^{d-1} f_1 g_m^{-1} E - 3^{d-1} \sum_{j \neq 1,m} f_1 g_j^{-1} E - 3^{d-1} \sum_{i \neq 1,m} f_i g_m^{-1} E + 3^{d-1} \sum_{\substack{1 \leq i,j \leq s \\ i \neq 1, j \neq m, i \neq j}} f_i g_j^{-1} E$$

$$\equiv 3^{d-1}(s+1)G \pmod{3^d} \text{ in } \mathbb{Z}[G],$$

14

which after projection gives

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

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

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

$\square$

5 Constructions in 2-groups using group difference matrices

In this section we present a powerful construction (Theorem 5.6) of reduced linking systems of difference sets in 2-groups. The construction, which is not restricted to abelian groups, combines combinatorial properties of hyperplanes (Proposition 4.9) with the unexpected use of group difference matrices.

Theorem 5.6 has several consequences. Corollaries 5.8 and 5.9 construct infinite families of reduced linking systems of difference sets in abelian groups, simplifying and extending some of the previous results given in Theorem 1.11. Corollary 5.10 constructs an infinite family of examples in nonabelian groups, whereas not a single nonabelian example was previously known. Corollary 5.11 constructs an infinite family of nonreversible examples generalizing Example 1.8. Finally, we show in Section 5.6 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.

5.1 Group difference matrices

We first introduce group difference matrices; see [Col07] for a survey of the topic.

Definition 5.1. *Let G be a group of order $v > 1$. A (G, m, λ)-difference matrix is an $m \times \lambda v$ matrix $(b_{i,j})$ with $0 \le i \le m-1$ and $0 \le j \le \lambda v - 1$ and each entry $b_{i,j} \in G$ such that, for all distinct rows i and r, the multiset $\{b_{i,j}b_{r,j}^{-1} : 0 \le j \le \lambda v - 1\}$ contains every element of G exactly λ times.*

We shall be interested only in the case $\lambda = 1$ of Definition 5.1, 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 right-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 right-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 $\{b_{i,j} : 0 \le j \le v - 1\}$ contains every element of G exactly once. We can likewise right-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 considering the entries of column 1 of the matrix and using the pigeonhole principle, we see that the largest number of rows of a $(G, m, 1)$-difference matrix is $|G|$.

Example 5.2. *Let $G = \mathbb{Z}_2^2 = \langle x, y \rangle$. The matrix*

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

15

is a $(\mathbb{Z}_2^2, 4, 1)$-difference matrix.

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

Theorem 5.3 (Pan and Chang [PC16, Lemma 3.4])**.** *Let G be an abelian noncyclic 2-group. Then there exists a $(G, 4, 1)$-difference matrix.*

Theorem 5.4 (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.*

Note that the case $e = 1$ of Theorem 5.4 gives a $(G, m, 1)$-difference matrix for $G = \mathbb{Z}_2^{d+1}$ and $m = 2^{d+1}$, which satisfies the extremal condition $m = |G|$.

5.2 Main construction theorem

We next find sufficient conditions for the linking property (4) to hold for a pair of difference sets in a 2-group (Lemma 5.5), and then show that the rows of a difference matrix can be used to satisfy these pairwise conditions for a collection of difference sets simultaneously (Theorem 5.6). Recall that the parameters of a difference set in a group of order 2^{2d+2} are determined by Theorem 1.2, and can be regarded as McFarland parameters with $q = 2$, and that when q is prime we do not need to specify an isomorphism ϕ in Theorem 4.2.

Lemma 5.5. *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 $f_0, f_1, \ldots f_s$ and $g_0, g_1, \ldots, g_s$ are each a set of coset representatives for E in G such that $f_0 g_0^{-1}, f_1 g_1^{-1}, \ldots, f_s g_s^{-1}$ 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 $\mathrm{GF}(2)$. Then the sets*

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

are difference sets in G satisfying

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

where

$$D = \sum_{i=1}^{s} f_i g_i^{-1}(E - H_i) \tag{23}$$

is also a difference set in G.

Proof. The sets D_1 and D_2 are difference sets in G, by Theorem 4.2 with $q = 2$. Since each $H_j \subset E$ is central in G, and $H_j^{(-1)} = H_j$, by Proposition 4.9 we calculate in $\mathbb{Z}[G]$ that

$$D_1 D_2^{(-1)} = \left(\sum_{i=1}^{s} f_i H_i \right) \left(\sum_{j=1}^{s} H_j^{(-1)} g_j^{-1} \right) = \sum_{i=1}^{s} f_i g_i^{-1}(2^d H_i) + \sum_{\substack{1 \le i,j \le s \\ i \ne j}} f_i g_j^{-1}(2^{d-1} E). \tag{24}$$

16

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

$$\sum_{i=1}^{s} f_i E = G - f_0 E$$

$$\sum_{i=1}^{s} g_i^{-1} E = G - g_0^{-1} E$$

$$\sum_{i=1}^{s} f_i g_i^{-1} E = G - f_0 g_0^{-1} E. \tag{25}$$

Therefore

$$\sum_{\substack{1 \le i,j \le s \\ i \ne j}} f_i g_j^{-1} E = \sum_{i=1}^{s} f_i \sum_{j=1}^{s} g_j^{-1} E - \sum_{i=1}^{s} f_i g_i^{-1} E$$

$$= \sum_{i=1}^{s} f_i (G - g_0^{-1} E) - (G - f_0 g_0^{-1} E)$$

$$= sG - (G - f_0 E) g_0^{-1} - (G - f_0 g_0^{-1} E)$$

$$= (s - 2)G + 2 f_0 g_0^{-1} E.$$

Substitute into (24) to obtain

$$D_1 D_2^{(-1)} = 2^d \sum_{i=1}^{s} f_i g_i^{-1} H_i + 2^{d-1} \left((s - 2)G + 2 f_0 g_0^{-1} E \right) \tag{26}$$

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

$$= -2^d D + 2^{d-1} sG, \tag{27}$$

where by (25)

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

It remains to show that D is a difference set in G. For each i we may write $E - H_i = a_i H_i$ for some $a_i \in E$ because H_i has index 2 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 difference set in G by Theorem 4.2. $\qquad\square$

Lemma 5.5 shows that, subject to conditions on coset representatives, McFarland difference sets D_1, D_2 with $q = 2$ that are constructed as in Theorem 4.2 can form a reduced linking system. In view of the nonexistence result of Theorem 4.4 (also for McFarland difference sets with $q = 2$ that are constructed as in Theorem 4.2), it is natural to ask where Lemma 5.5 fails for $q > 2$. There are

17

two such places. Firstly, the expression

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

in (26) is replaced by

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

so that the corresponding expression (27) for $D_1 D_2^{(-1)}$ now involves three distinct coefficients $q^d, q^{d-1}s, 2q^{d-1}$ (where $s = \frac{q^{d+1}-1}{q-1}$). Secondly, it is no longer possible to write $E - H_i = a_i H_i$ for some $a_i \in E$, because H_i has now index q in E (where E is isomorphic to the elementary abelian group of order q^{d+1}) .

Theorem 5.6. *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 after Definition 5.1 we may assume that, for each nonzero distinct i and r, the set $\{b_{i,j}E : 0 \leq j \leq s\}$, as well as the set $\{b_{i,j}b_{r,j}^{-1}E : 0 \leq j \leq s\}$, contains 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

$$D_i = \sum_{j=1}^{s} b_{i,j}e_{i,j}H_j \quad \text{for } 1 \leq i \leq m - 1. \tag{28}$$

We shall show that $\{D_1, D_2, \ldots, D_{m-1}\}$ is a reduced linking system of difference sets in G. By Definition 1.6, 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 and r,

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

for some difference set $D(i,r)$ in G. This follows from Lemma 5.5 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 Lemma 5.5 and Theorem 5.6 in which G is not an elementary abelian 2-group.

Example 5.7. *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 5.2, the matrix* $(b_{i,j}E)$ *is a* $(G/E, 4, 1)$-*difference matrix, where*

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

Take

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

Then (28) *gives the reduced linking system of difference sets*

$$D_1 = xH_1 + yH_2 + xyH_3$$
$$D_2 = yzH_1 + x^3yH_2 + x^3H_3$$
$$D_3 = xyzH_1 + xH_2 + yH_3.$$

Furthermore, we can find the difference set $D(i,j)$ *specified in Definition 1.6 directly from* D_i *and* D_j. *For example,*

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

where by (23) *we find*

$$D(2,3) = (yz)(xyz)^{-1}(E - H_1) + (x^3y)(x)^{-1}(E - H_2) + (x^3)(y)^{-1}(E - H_3)$$
$$= x^3(zH_1) + x^2y(x^2H_2) + x^3y(zH_3)$$
$$= xzH_1 + yH_2 + xyH_3.$$

5.3 Infinite families in abelian groups

We now use Theorem 5.6 to construct infinite families of reduced linking systems of difference sets in a wide range of abelian 2-groups.

Corollary 5.8. *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 is cyclic 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 5.3 there exists a $(G/E, 4, 1)$-difference matrix and the result follows from Theorem 5.6. $\square$

Corollary 5.9. *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 5.4 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 5.6. $\qquad\square$

Table 1 in Section 1 summarizes the constructive results of Corollaries 5.8 and 5.9, together with that of Corollary 3.6. Table 2 in Section 1, and Table 3 below, illustrate the power of Corollaries 5.8 and 5.9 in comparison with the best previously known results, by considering abelian groups of order 64 and 256, respectively. Table 3 does not list those groups of order 256 having exponent 32 or rank at most 3, for which no existence results are currently known.

Table 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 3.6)
$\mathbb{Z}_4 \times \mathbb{Z}_2^6$	None	15	Difference matrix (Corollary 5.9)
$\mathbb{Z}_4^2 \times \mathbb{Z}_2^4$	3 [DMP14]	15	Difference matrix (Corollary 5.9)
$\mathbb{Z}_4^3 \times \mathbb{Z}_2^2$	None	15	Difference matrix (Corollary 5.9)
$\mathbb{Z}_4^4$	15 [DMP14]	15	Difference matrix (Corollary 5.9)
$\mathbb{Z}_8 \times \mathbb{Z}_2^5$	None	3	Difference matrix (Corollary 5.8)
$\mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2^3$	None	3	Difference matrix (Corollary 5.8)
$\mathbb{Z}_8 \times \mathbb{Z}_4^2 \times \mathbb{Z}_2$	None	3	Difference matrix (Corollary 5.8)
$\mathbb{Z}_8^2 \times \mathbb{Z}_2^2$	None	3	Difference matrix (Corollary 5.8)
$\mathbb{Z}_{16} \times \mathbb{Z}_2^4$	None	3	Difference matrix (Corollary 5.8)
$\mathbb{Z}_{16} \times \mathbb{Z}_4 \times \mathbb{Z}_2^2$	None	3	Difference matrix (Corollary 5.8)

5.4 Infinite families in nonabelian groups

We next use Theorem 5.6 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 5.10. *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 $2^{d+1} - 1$.*

20

Proof. The group K has rank at least d, and 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 5.4, there exists a $(G/E, 2^{d+1}, 1)$-difference matrix. The result follows from Theorem 5.6. □

We cannot produce a reduced linking system of difference sets of larger size than in Corollary 5.10 using the difference matrix construction of Theorem 5.6, 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 5.1).

The technique used in the proof of Corollary 5.10, of substituting the dihedral group D_4 for an abelian group of order 8, appears in other contexts (for example, [BJL99, Chapter VI, Remarks 9.10 (b)]). However, we can produce many further examples of reduced linking systems of difference sets in nonabelian 2-groups by modifying the construction of Corollary 5.10. A straightforward variation is to replace D_4 by the quaternion group of order 8. More sophisticated examples are readily available: by Theorems 5.3 and 5.6, it is sufficient to find a nonabelian group G of order 2^{2d+2} containing a central subgroup E isomorphic to $\mathbb{Z}_2^{d+1}$ for which the factor group G/E is abelian and noncyclic. The software package GAP [GAP18] shows that there are 4 such groups G of order 16, and 49 such groups G of order 64.

5.5 Infinite nonreversible family

Recall from Section 1.3 that all examples of reduced linking systems of difference sets given in [DMP14] are reversible, with the single exception of Example 1.8. We shall generalize Example 1.8 to an infinite family of nonreversible examples.

We first show that Example 1.8 can be realized using the construction (28) given in the proof of Theorem 5.6. Take $G = \mathbb{Z}_4^2 = \langle x, y \rangle$ and $E = \langle x^2, y^2 \rangle$ and $d = 1$ 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 1.8 as

$$D_1 = xH_1 + yH_2 + xy^3 H_3$$
$$D_2 = xyH_1 + xH_2 + y^3 H_3$$
$$D_3 = y^3 H_1 + x^3 y H_2 + xH_3,$$

which have the form (28) where

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

and

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

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

We now generalize Example 1.8.

Corollary 5.11. *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 5.4 there is a $(G/E, 2^{d+1}, 1)$-difference matrix $(b_{i,j}E)$, where each $b_{i,j}E$ has the form $\prod_{r \in R(i,j)} x_r E$ for some subset $R(i,j)$ of $\{1, 2, \ldots, d+1\}$. Following the proof of Theorem 5.6, 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 $H_1 = \langle x_2^2, x_3^2, \ldots, x_{d+1}^2 \rangle$. As discussed after Definition 5.1, 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 (28) 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

$$D_1 = x_1 H_1 + \sum_{j=2}^{s} b_{1,j} e_{1,j} H_j$$

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 $b_{1,j}E = \prod_{r \in R(1,j)} x_r E$, we conclude that $b_{1,j} \in x_1 E$ for some $j > 1$. This contradicts that the set $\{b_{1,j}E : 0 \leq j \leq s\}$ contains no repeated element. $\square$

5.6 The group $\mathbb{Z}_4^2$

We further illustrate the strength of the difference matrix construction of Theorem 5.6 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 $H_1 = \langle x^2 \rangle, H_2 = \langle y^2 \rangle, H_3 = \langle x^2 y^2 \rangle$, so that (28) becomes

$$\begin{aligned}
D_1 &= b_{1,1} e_{1,1} \langle x^2 \rangle + b_{1,2} e_{1,2} \langle y^2 \rangle + b_{1,3} e_{1,3} \langle x^2 y^2 \rangle \\
D_2 &= b_{2,1} e_{2,1} \langle x^2 \rangle + b_{2,2} e_{2,2} \langle y^2 \rangle + b_{2,3} e_{2,3} \langle x^2 y^2 \rangle \\
D_3 &= b_{3,1} e_{3,1} \langle x^2 \rangle + b_{3,2} e_{3,2} \langle y^2 \rangle + b_{3,3} e_{3,3} \langle x^2 y^2 \rangle.
\end{aligned} \tag{29}$$

We first show that there are at least 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. The matrices

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

for $0 \leq i, j \leq 3$ 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

22

see from (29) 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 cannot directly compare this count of reduced linking systems of difference sets with the classification of systems of linked symmetric $(16, 6, 2, 4)$ designs given by Mathon [Mat81], which counts the number of isomorphism classes rather than the number of distinct systems.)

We next consider the reversibility of these 2^{16} reduced linking systems of difference sets. We have already seen an example in Section 5.5 (namely Example 1.8) 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

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

6 Open problems

We conclude with some open problems.

1. Our main constructive result (Theorem 5.6) uses difference matrices in 2-groups as a crucial ingredient. Are there examples of difference matrices with more rows than those specified in Theorems 5.3 and 5.4, or in other 2-groups? If so, this would immediately give new reduced linking systems of difference sets.

2. Our main constructive result depends on Lemma 5.5, involving hyperplanes. Following Q4 of Section 1.4, is there a construction for reduced linking systems of difference sets involving another combinatorial object such as a partial difference set?

3. Table 1 extends some of the previous results due to Davis, Martin, and Polhill [DMP14] for abelian 2-groups (Theorem 1.11), but does not explain all their results. Can the constructive framework of this paper be broadened to do so?

4. 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?

5. 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 Section 4 and the constructions recently given by Kodalen [Kod17]. Can this question be resolved constructively, or else can its scope be narrowed by finding further nonexistence results similar to Theorems 4.4 and 4.5?

6. We have counted all reduced linking systems of difference sets in the group $\mathbb{Z}_4^2$ having maximum size (Section 5.6). Can this counting result be extended to other groups?

Acknowledgements

References

[BJL99]   T. Beth, D. Jungnickel, and H. Lenz. *Design Theory*. Cambridge University Press, Cambridge, 2nd edition, 1999. Volumes I and II.

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

[Bru55]   R.H. Bruck. Difference sets in a finite group. *Trans. Amer. Math. Soc.*, 78:464–481, 1955.

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

[Cam72]   P.J. Cameron. On groups with several doubly-transitive permutation representations. *Math. Z.*, 128:1–14, 1972.

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

[Col07]   C.J. Colbourn. Difference matrices. In C.J. Colbourn and J.H. Dinitz, editors, *Handbook of Combinatorial Designs*, pages 411–419. Chapman & Hall/CRC, Boca Raton, 2nd edition, 2007.

[CS73]   P.J. Cameron and J.J. Seidel. Quadratic forms over $GF(2)$. *Indag. Math.*, 35:1–8, 1973.

[Del73]   P. Delsarte. An algebraic approach to the assocation schemes of coding theory. *Phillips Research Reports Supplements*, 10, 1973.

[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 (A)*, 40:9–21, 1985.

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

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

[GAP18]   The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.8.10*, 2018.

[JS97]   D. Jungnickel and B. Schmidt. Difference sets: an update. In J.W.P. Hirschfeld, S.S. Magliveras, and M.J. de Resmini, editors, *Geometry, Combinatorial Designs and Related Structures*, pages 89–112. Cambridge University Press, Cambridge, 1997.

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

[Jun92]   D. Jungnickel. Difference sets. In J.H. Dinitz and D.R. Stinson, editors, *Contemporary Design Theory: a Collection of Surveys*, pages 241–324. Wiley, New York, 1992.

[Ker72]   A.M. Kerdock. A class of low-rate nonlinear binary codes. *Information and Control*, 20:182–187; erratum ibid. 21 (1972), 395, 1972.

[Kod17]   B. Kodalen. Linked systems of symmetric design. `arXiv:1712.02911v1 [math.CO]`, December 2017.

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

[Lan83]   E.S. Lander. *Symmetric Designs: an Algebraic Approach*. London Mathematical Society Lecture Notes Series 74. Cambridge University Press, Cambridge, 1983.

[Mat81]   R. Mathon. The systems of linked 2-$(16, 6, 2)$ designs. *Ars Combin.*, 11:131–148, 1981.

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

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

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

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

[Sim17]   S. Simon. Linking systems of difference sets. Master's thesis, Simon Fraser University, 2017.

[Spe77]   E. Spence. A family of difference sets. *J. Combin. Theory (A)*, 22:103–106, 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.*, 10:69–107, 1999.