Linking systems in nonelementary abelian groups

James A. Davis
Department of Mathematics and Computer Science
University of Richmond
Richmond, VA 23173
email: jdavis@richmond.edu

William J. Martin*
Department of Mathematical Sciences and Department of Computer Science
Worcester Polytechnic Institute
Worcester, MA 01609
email: martin@WPI.EDU

John B. Polhill†
Department of Mathematics, Computer Science, and Statistics
Bloomsburg University
Bloomsburg, PA 17815
email : jpolhill@bloomu.edu

Abstract

Linked systems of symmetric designs are equivalent to 3-class Q-antipodal association schemes. Only one infinite family of examples is known, and this family has interesting origins and is connected to important applications. In this paper, we define linking systems, collections of difference sets that correspond to systems of linked designs, and we construct linking systems in a variety of nonelementary abelian groups using Galois rings, partial difference sets, and a product construction. We include some partial results in the final section.

1 Introduction

A *symmetric* (v, k, λ) *design* is an incidence structure consisting of v points and v blocks; each point is incident with k distinct blocks and each block is incident with k distinct points; any pair of points is incident with λ blocks and any pair of blocks are incident with λ common points. The *incidence graph of a symmetric design* is a graph with $2v$ vertices, one for each point P and one for each block B, with an edge joining a point P to a block B precisely when the two are incident.

Making use of this graph-theoretic notion, we define the central object of our study.

Definition 1.1 *A* system of ℓ linked symmetric[1] (v, k, λ) designs *[4, Sec. 2] is a graph* $\mathcal{G} = (X, R)$ *defined on a vertex set*

$$X = \Omega_0 \cup \Omega_1 \cup \cdots \cup \Omega_\ell$$

*Support provided by NSA grant H98230-12-1-0243
†Support provided by NSA grant H98230-10-1-0216

[1]Note that, in the original paper [4], the term "projective design" is used for what is known today by the term "symmetric design". Moreover, the original definition of linked projective designs stipulated only that all pairs of fibers induce symmetric designs, but not necessarily with the same values of v, k and λ.

where $\pi = \{\Omega_0, \Omega_1, \ldots, \Omega_\ell\}$ is a partition of X into $\ell + 1$ sets of size v each (we say the system has $f = \ell + 1$ fibers*), having the following properties:*

(1) the partition π is a proper coloring of $\mathcal{G}$: no edge of $\mathcal{G}$ has both ends in the same class Ω_i;

(2) for any $i \neq j$, the subgraph of $\mathcal{G}$ induced on $\Omega_i \cup \Omega_j$ is the incidence graph of a symmetric (v, k, λ) design;

(3) for any three distinct classes $\Omega_i, \Omega_j, \Omega_m$, the number of common neighbors of a vertex x in Ω_i and a vertex y in Ω_j which lie in Ω_m depends only on whether x and y are adjacent in $\mathcal{G}$ or not; it does not depend on the choice of x and y nor on the choice of i, j, and m.

A system of linked symmetric designs is exactly equivalent [6] to a 3-class Q-antipodal cometric association scheme. Moreover, such a linked system with the appropriate parameters can be used to construct a 4-class Q-antipodal Q-bipartite cometric association scheme [13, Theorem 3.6] and real mutually unbiased bases [11, Theorem 4.2]. Goethals is credited (private communication) in a paper by Cameron and Seidel [5] as having constructed a system of $\ell = 2^{2t+1} - 1$ linked symmetric $(2^{2t+2}, 2^{2t+1} - 2^t, 2^{2t} - 2^t)$ designs for t any positive integer. We construct new examples of systems of linked designs with these parameters by using difference sets (but with smaller ℓ).

The paper is organized as follows. Section 2 provides background information in difference sets and association schemes and it also introduces the idea of a linking system of difference sets. Section 3 gives a general product construction that will be useful in future sections. Section 4 uses Galois Rings to construct examples of linking systems of difference sets. One of the examples in this section is shown to be inequivalent to the Cameron-Seidel examples. Section 5 uses partial difference sets to construct examples. Finally, Section 6 provides a few more examples and presents some unsolved problems to consider. One of these examples is extendable to that of Cameron-Seidel.

2 Preliminaries

A *symmetric d-class association scheme* consists of a finite set X together with a partition $\mathcal{R} = \{R_0, R_1, \ldots, R_d\}$ of $X \times X$ into symmetric binary relations satisfying

- R_0 is the identity relation;
- for each choice of $i, j, k \in \{0, \ldots, d\}$, there exists an integer p_{ij}^k such that, whenever $(x, y) \in R_k$, we have
$$|\{z \in X \mid (x, z) \in R_i,\ (z, y) \in R_j\}| = p_{ij}^k \ .$$

We refer the reader to [1, 3] for background material. Our focus is a special class of association schemes of current research interest known as the *Q-polynomial* (or "cometric") *association schemes* (see [3, Chap. 2]). An association scheme $(X, \mathcal{R})$ is *imprimitive* if at least one of the graphs (X, R_i) $(i \neq 0)$ is disconnected. It is known that an imprimitive 3-class Q-polynomial association scheme is either a Taylor graph (this is the Q-bipartite case [13]) or a system of linked symmetric designs [6] (this is the Q-antipodal case [13]). With little further reference to the association schemes themselves, this paper deals with this latter case.

Our goal in this paper is to introduce the use of difference sets to construct systems of linked symmetric designs: see [2] for more background on difference sets.

Definition 2.1 *A subset $D \subset G$ of a group G is a (v, k, λ) difference set if $|D| = k, |G| = v$, and for every $g \neq e \in G$, $\left|\{(d, d') \in D^2 \mid g = d(d')^{-1}\}\right| = \lambda$. The difference set is called reversible if $D^{(-1)} := \{d^{-1} \mid d \in D\} = D$.*

The *development* of a difference set D in a group G is the set of all translates $gD, g \in G$ (we will use multiplication for the group operation unless otherwise noted). A simple exercise shows that the incidence structure whose points are the elements of the group G and whose blocks are the translates in the development of D will be a symmetric (v, k, λ) design with regular automorphism group G. Our strategy will be to construct a collection of reversible difference sets whose developments form a system of linked designs.

Difference sets are often studied using the language of the group ring $\mathbb{Z}[G]$. If we allow the standard abuse of notation by identifying the sets D, $D^{(-1)}$, and G with the group ring elements $D = \sum_{d\in D} d$, $D^{(-1)} = \sum_{d\in D} d^{-1}$, and $G = \sum_{g\in G} g$ (and we also identify the identity element 1_G of G with the group ring element 1_G), then the subset D is a (v, k, λ) difference set in G if

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

The next definition is the main object we will aim to construct for the rest of the paper.

Definition 2.2 *Let G be a finite group of order v and let $\ell \geq 1$. A collection $\{D_{i,j} \mid 0 \leq i, j \leq \ell,\ i \neq j\}$ of (v, k, λ) difference sets in G is a $(v, k, \lambda; \ell + 1)$-linking system if there exist $\mu, \nu \in \mathbb{Z}$ such that*

(1) $D_{j,i} = (D_{i,j})^{(-1)}$ for all $i \neq j$;

(2) for all distinct $h, i, j \in \{0, \ldots, \ell\}$, $D_{h,i}D_{i,j} = \mu D_{h,j} + \nu(G - D_{h,j})$.

Remarks.

- Extending Cameron, Noda [16, Proposition 0] gives expressions for μ and ν in terms of v, k and $n := k - \lambda$:
$$\mu = k(k \pm \sqrt{n})/v, \qquad \nu = k(k \pm \sqrt{n})/v \mp \sqrt{n}\ .$$
- We note that, in Cameron's original setting [4], the designs formed by different pairs of fibres were permitted to have different parameters. With all pairs giving rise to (v, k, λ) designs, the fibre Ω_0 no longer plays a distinguished role and so, while the total number of symmetric designs present in the structure is $\binom{\ell+1}{2}$ (or double that), the number of fibres $f = \ell + 1$ seems a more accurate parameter for our system than ℓ itself.
- Note that, in our conditions on the collection $\{D_{i,j} \mid 0 \leq i, j \leq \ell,\ i \neq j\}$, it suffices to specify difference sets on some directed spanning tree of the complete graph $K_{\ell+1}$; e.g., if we specify $\{D_{j,0} \mid 1 \leq j \leq \ell\}$, then we may recover each $D_{i,j}$ from the above equation by simplifying $D_{i,0}(D_{j,0})^{(-1)}$.
- Finally, when we impose the additional restriction that each difference set be reversible, we have another simplification; we call this a *reversible linking system*. All examples in this paper will be of this type with one exception, Example 6.3.

Suppose $\{D_{i,j} \mid 0 \leq i, j \leq \ell,\ i \neq j\}$ is a $(v, k, \lambda; \ell + 1)$-reversible linking system in a group G of order v. Let $\Omega_0, \Omega_1, \ldots, \Omega_\ell$ be $\ell + 1$ disjoint copies of G. On the base set $X = \Omega_0 \cup \cdots \cup \Omega_\ell$ define four binary relations R_0, R_1, R_2, R_3 as follows. Relation zero is the identity relation: $R_0 = \{(x, x) \mid x \in X\}$. Relation two is the union of $\ell + 1$ complete graphs of size v: $R_2 = \left(\bigcup_{i=0}^{\ell} \Omega_i \times \Omega_i\right) - R_0$. For $a \in \Omega_i$ and $b \in \Omega_j$, $j \neq i$, we put $(a, b) \in R_1$ if $a^{-1}b \in D_{i,j}$ and we put $(a, b) \in R_3$ otherwise. Since $(D_{i,j})^{(-1)} = D_{j,i}$, these relations are both symmetric, so (X, R_1), (X, R_3) constitutes a partition of the complete multipartite graph into two undirected graphs.

We next point out that $(X, \{R_0, R_1, R_2, R_3\})$ is a symmetric 3-class association scheme. Such an association scheme is referred to as a *system of linked symmetric designs* [6, 13], but – as stated in the Introduction – we also use this term for the graph (X, R_1) which clearly determines all others

in the partition $\{R_0, R_1, R_2, R_3\}$. Assuming (X, R_1) satisfies Definition 1.1, one easily checks that this partition of $X \times X$ forms an association scheme with intersection numbers [3, Sec. 2.1]

$$[p^i_{1,j}]_{i,j} = \begin{bmatrix} 0 & \ell k & 0 & 0 \\ 1 & (\ell-1)\mu & k-1 & (\ell-1)(k-\mu) \\ 0 & \ell\lambda & 0 & \ell(k-\lambda) \\ 0 & (\ell-1)\nu & k & (\ell-1)(k-\nu) \end{bmatrix}, \quad [p^i_{2,j}]_{i,j} = \begin{bmatrix} 0 & 0 & v-1 & 0 \\ 0 & k-1 & 0 & v-k \\ 1 & 0 & v-2 & 0 \\ 0 & k & 0 & v-k-1 \end{bmatrix},$$

$$[p^i_{3,j}]_{i,j} = \begin{bmatrix} 0 & 0 & 0 & \ell(v-k) \\ 0 & (\ell-1)(k-\mu) & v-k & (\ell-1)(v-2k+\mu) \\ 0 & \ell(k-\lambda) & 0 & \ell(v-2k+\lambda) \\ 1 & (\ell-1)(k-\nu) & v-k-1 & (\ell-1)(v-2k+\nu) \end{bmatrix}.$$

Theorem 2.3 *Suppose $\{D_{1,0}, D_{2,0}, \ldots, D_{\ell,0}\}$ is a collection of (v,k,λ) reversible difference sets from the group G with the property that $D_{i,0}\,(D_{j,0})^{(-1)} = \mu D_{i,j} + \nu(G - D_{i,j})$ for some (reversible) (v,k,λ) difference set, $D_{i,j}$, for each $i \neq j$. Then this collection $\{D_{i,j} \mid 0 \leq i,j \leq \ell,\ i \neq j\}$ forms a $(v,k,\lambda;\ell+1)$-reversible linking system in G and the configuration $(X, \{R_0, R_1, R_2, R_3\})$ defined above from this system is a 3-class association scheme determining a system of linked symmetric designs.*

The proof of the above theorem follows from Theorem 2 in [4], so we have omitted the proof.

Only one infinite family of systems of linked symmetric designs is known; this was reported by Cameron and Seidel [5]. Using bent functions arising from Kerdock codes, they found a construction of a system of $2^{2t+1}-1$ linked symmetric $(2^{2t+2}, 2^{2t+1}-2^t, 2^{2t}-2^t)$-designs. The first non-trivial case (i.e., $t=1$) is $v=16$. In [14], Mathon carried out a systematic classification of linked systems of symmetric $(16,6,2)$ designs. Mathon identified 12 triples of such linked systems, only one of which was extendable to a system of 7 linked designs, this latter configuration being the one found earlier by Cameron and Seidel. Our purpose in this paper is to find more infinite families of such linked systems of designs via the use of linking systems as defined above; to begin this approach via difference sets, we state the only general construction known prior to the present work.

Theorem 2.4 (Cameron & Seidel [5]) *There is a $(2^{2t+2}, 2^{2t+1}-2^t, 2^{2t}-2^t; 2^{2t+1})$-reversible linking system in the elementary abelian group of order 2^{2t+2} for all $t \geq 2$.*

3 Product construction

We will show in this section that if one has linking systems in nonelementary abelian groups so that the difference sets have the parameters $(4N^2, 2N^2-N, N^2-N)$, then we may employ the following product construction to get new infinite families of linking systems in nonelementary abelian groups. (Cf. Noda [16, Cor. 3], where $\ell < v/2$ is proved for this case.)

Theorem 3.1 *Suppose that G has a $(4N^2, 2N^2-N, N^2-N; \ell+1)$-reversible linking system formed by difference sets $\{D_{1,0}, D_{2,0}, \ldots, D_{\ell,0}\}$ and suppose that G' has a $(4M^2, 2M^2-M, M^2-M; \ell+1)$-reversible linking system formed by difference sets $\{E_{1,0}, E_{2,0}, \ldots, E_{\ell,0}\}$. Then $\{F_{1,0}, F_{2,0}, \ldots, F_{\ell,0}\}$ is a collection of $(4(2NM)^2, 2(2NM)^2-(2NM), (2NM)^2-(2NM))$-reversible difference sets in $G \times G'$ that forms a $(4(2NM)^2, 2(2NM)^2-(2NM), (2NM)^2-(2NM); \ell+1)$-reversible linking system, where $F_{i,0} = D_{i,0} \times (G' - E_{i,0}) \cup (G - D_{i,0}) \times E_{i,0}$, $1 \leq i \leq \ell$ and $F_{i,j}$ is recovered from $F_{i,0}F_{j,0}$ as above.*

Proof: That the $F_{i,0}$ are reversible difference sets with the parameters listed in the theorem follows from the well-known product construction for Hadamard Difference Sets (see [2] for details). Thus, we simply need to show that the collection $\{F_{i,j} \mid 0 \leq i \neq j \leq \ell\}$ forms a linking system with the correct parameters. The following equations follow from the fact that $\{D_{i,j} \mid 0 \leq i \neq j \leq \ell\}$ forms a $(4N^2, 2N^2-N, N^2-N; \ell+1)$-linking system in G (in this case $D_{i,j}$ is a reversible difference set in G when $i \neq j$).

$$D_{i,0}D_{j,0} = \frac{2N^2-3N}{2}D_{i,j} + \frac{2N^2-N}{2}(G-D_{i,j}) \quad (1)$$

$$D_{i,0}(G-D_{j,0}) = (G-D_{i,0})D_{j,0} = \frac{2N^2+N}{2}D_{i,j} + \frac{2N^2-N}{2}(G-D_{i,j}) \quad (2)$$

$$(G-D_{i,0})(G-D_{j,0}) = \frac{2N^2+N}{2}D_{i,j} + \frac{2N^2+3N}{2}(G-D_{i,j}) \quad (3)$$

There are analogous equations for $E_{i,0}$ and $E_{j,0}$ in G'. By using equations (1), (2), and (3) and their analogues together with some straightforward computations, we get the following.

$$\begin{aligned}
F_{i,0}F_{j,0} = {} & (D_{i,0}\times(G'-E_{i,0}) + (G-D_{i,0})\times E_{i,0})(D_{j,0}\times(G'-E_{j,0}) + (G-D_{j,0})\times E_{j,0}) \\
= {} & D_{i,0}D_{j,0}\times(G'-E_{i,0})(G'-E_{j,0}) + D_{i,0}(G-D_{j,0})\times(G'-E_{i,0})E_{j,0} \\
& + (G-D_{i,0})D_{j,0}\times E_{i,0}(G'-E_{j,0}) + (G-D_{i,0})(G-D_{j,0})\times E_{i,0}E_{j,0} \\
= {} & \left[\frac{2N^2-3N}{2}D_{i,j} + \frac{2N^2-N}{2}(G-D_{i,j})\right]\times\left[\frac{2M^2+M}{2}E_{i,j} + \frac{2M^2+3M}{2}(G'-E_{i,j})\right] \\
& + 2\left[\frac{2N^2+N}{2}D_{i,j} + \frac{2N^2-N}{2}(G-D_{i,j})\right]\times\left[\frac{2M^2+M}{2}E_{i,j} + \frac{2M^2-M}{2}(G'-E_{i,j})\right] \\
& + \left[\frac{2N^2+N}{2}D_{i,j} + \frac{2N^2+3N}{2}(G-D_{i,j})\right]\times\left[\frac{2M^2-3M}{2}E_{i,j} + \frac{2M^2-M}{2}(G'-E_{i,j})\right] \\
= {} & \left(\frac{2N^2-3N}{2}\frac{2M^2+M}{2} + 2\frac{2N^2+N}{2}\frac{2M^2+M}{2} + \frac{2N^2+N}{2}\frac{2M^2-3M}{2}\right)D_{i,j}\times E_{i,j} \\
& + \left(\frac{2N^2-3N}{2}\frac{2M^2+3M}{2} + 2\frac{2N^2+N}{2}\frac{2M^2-M}{2} + \frac{2N^2+N}{2}\frac{2M^2-M}{2}\right)(G-D_{i,j})\times E_{i,j} + \\
& \left(\frac{2N^2-3N}{2}\frac{2M^2+3M}{2} + 2\frac{2N^2+N}{2}\frac{2M^2-M}{2} + \frac{2N^2+N}{2}\frac{2M^2-M}{2}\right)D_{i,j}\times(G'-E_{i,j}) + \\
& \left(\frac{2N^2-3N}{2}\frac{2M^2+M}{2} + 2\frac{2N^2+N}{2}\frac{2M^2+M}{2} + \frac{2N^2+N}{2}\frac{2M^2-3M}{2}\right)(G-D_{i,j})\times(G'-E_{i,j}) \\
= {} & \frac{2(2NM)^2-3(2NM)}{2}[(G-D_{i,j})\times E_{i,j} + D_{i,j}\times(G'-E_{i,j})] + \\
& \frac{2(2NM)^2-(2NM)}{2}[D_{i,j}\times E_{i,j} + (G-D_{i,j})\times(G'-E_{i,j})]
\end{aligned}$$

The set corresponding to the group ring element $(G-D_{i,j})\times E_{i,j} + D_{i,j}\times(G'-E_{i,j})$ is a reversible Hadamard difference set in $G\times G'$ by the product theorem for Hadamard difference sets. Since i and j were arbitrary, we have shown that $\{F_{1,0}, F_{2,0}, \ldots, F_{\ell,0}\}$ forms a $(4(2NM)^2, 2(2NM)^2 - (2NM), (2NM)^2 - (2NM); \ell+1)$-linking system of reversible difference sets in $G\times G'$. □

4 Galois Ring construction and consequences

In this section we follow the treatment found in [7]. A polynomial $\Phi_2(x) \in \mathrm{GF}(2)[x]$ of degree t is *primitive* if $\Phi_2(x)$ is irreducible and $x \oplus \Phi_2(x)$ has degree $2^t - 1$ in the multiplicative group of $\mathrm{GF}(2)[x]/\langle\Phi_2(x)\rangle$ (notation for this section: we will use $\oplus$ for the addition in the fields and rings to distinguish from the $+$ being used for group ring addition). There is a unique polynomial $\Phi(x) \in \mathbb{Z}_4[x]$ of degree t so that (i) $\Phi(x) \equiv \Phi_2(x) \bmod 2$ and (ii) $\Phi(x)$ divides $x^{2^t-1}-1 \bmod 4$. Such a polynomial $\Phi(x)$ is called a *basic primitive polynomial* in $\mathbb{Z}_4[x]$. A *Galois Ring over $\mathbb{Z}_4$ of degree*

t, $t \geq 2$, denoted GR(4,t), is the quotient ring $\mathbb{Z}_4[x]/\langle\Phi(x)\rangle$. If h is a root of $\Phi(x)$ in GR(4,t), then GR(4,t) $= \mathbb{Z}_4[h]$ and the multiplicative order of h is 2^t-1. The ring GR(4,t) is a finite local ring with unique maximal ideal $2\text{GR}(4,t) = \{2h^i | 0 \leq i \leq 2^t-2\} \cup \{0\}$, and GR(4,$t$)/2GR(4,$t$) is isomorphic to the finite field GF(2^t). The natural epimorphism $\pi : \text{GR}(4,t) \to \text{GF}(2^t), \pi(r) = r \oplus 2\text{GR}(4,t)$ has the property that $g = \pi(h)$ is a primitive element of GF(2^t).

We will use tr: GF(2^t) $\to$ GF(2) to denote the usual trace map, and define $H_0 = \{x \in \text{GF}(2^t) | \text{tr}(x) = 0\}$. A classical result of Singer states that the hyperplanes of GF(2^t) are $H_0, H_1 = gH_0, \ldots, H_{2^t-2} = g^{2^t-2}H_0$. If we define the isomorphism ϕ from 2GR(4,t) to GF(2^t) by $\phi(2h^i) = g^i$ and $\phi(0) = 0$, then the "hyperplanes" of 2GR(4,t) are $K_i = \phi^{-1}(H_i)$, or $K_i = h^iK_0$ for $K_0 = \{x \in 2\text{GR}(4,t) | \text{tr}(\phi(x)) = 0\}$. A standard difference set construction leads to the following result.

Theorem 4.1 *If $g_0, g_1, \ldots, g_{2^t-2}$ are elements of* GR*(4,t) so that $g_i \ominus g_j \notin$ 2*GR*(4,t) for $i \neq j$, then $D = \cup_{j=0}^{2^t-2} g_j \oplus K_j$ is a $(2^{2t}, 2^{2t-1} - 2^{t-1}, 2^{2t-2} - 2^{t-1})$-difference set in* GR*(4,t). Moreover, if $2g_j \in K_j$ for $0 \leq j \leq 2^t - 2$, then D is a reversible $(2^{2t}, 2^{2t-1} - 2^{t-1}, 2^{2t-2} - 2^{t-1})$-difference set in* GR*(4,t).*

Proof: The fact that $D = \cup_{j=0}^{2^t-2} g_j \oplus K_j$ is a $(2^{2t}, 2^{2t-1} - 2^{t-1}, 2^{2t-2} - 2^{t-1})$-difference set in GR(4,$t$) follows directly from the Dillon generalization of McFarland's hyperplane construction [8], [15]. Suppose $2g_j \in K_j$ for $0 \leq j \leq 2^t - 2$ and let $g_j \oplus k_j \in g_j \oplus K_j$ be an arbitrary element of D. Since $k_j \in 2\text{GR}(4,t)$, we have that $\ominus k_j = k_j$ (all elements of 2GR(4,t) are their own additive inverses). This implies that $\ominus(g_j \oplus k_j) = 3g_j \oplus k_j = g_j \oplus (2g_j \oplus k_j)$, and $(2g_j \oplus k_j)$ is an element of K_j. Thus, $\ominus(g_j \oplus k_j) \in D$ and D is reversible. □

The notation for the coset $h^i \oplus h^{2i-j} \oplus K_j = \{h^i \oplus h^{2i-j} \oplus k_j | k_j \in K_j\}$ will also be used for the group ring element $h^i \oplus h^{2i-j} \oplus K_j = \sum_{k_j \in K_j} h^i \oplus h^{2i-j} \oplus k_j = (h^i \oplus h^{2i-j} \oplus k_{j_0}) + (h^i \oplus h^{2i-j} \oplus k_{j_1}) + \cdots + (h^i \oplus h^{2i-j} \oplus k_{j_{2^{t-1}-1}})$. The context will make clear which meaning we intend. Define the sets $E_{i,0} = E_i = \cup_{j=0}^{2^t-2}(h^i \oplus h^{2i-j} \oplus K_j), i = 0, 1, \ldots, 2^t - 2$. We claim that the set $\{E_0, E_1, \ldots, E_{2^t-2}\}$ will be a $(2^{2t}, 2^{2t-1} - 2^{t-1}, 2^{2t-2} - 2^{t-1}; 2^t)$-linking system in the additive group of GR$(4,t)$. We first need to show that the sets are reversible difference sets.

Corollary 4.2 *Let G be the additive group of* GR$(4,t)$ *and let E_i be the sets defined above. Then the E_i are reversible $(2^{2t}, 2^{2t-1} - 2^{t-1}, 2^{2t-2} - 2^{t-1})$ difference sets in G.*

Proof: For a given i and $j \neq j'$, we have that $(h^i \oplus h^{2i-j}) \ominus (h^i \oplus h^{2i-j'}) = (h^{2i})(h^{-j} \oplus h^{-j'})$. If we apply π to this group element we get $\pi((h^{2i})(h^{-j} \oplus h^{-j'})) = g^{2i}(g^{-j} \oplus g^{-j'}) \neq 0$, so $(h^i \oplus h^{2i-j}) \ominus (h^i \oplus h^{2i-j'}) \notin 2\text{GR}(4,t)$. Theorem 4.1 shows that E_i is a $(2^{2t}, 2^{2t-1} - 2^{t-1}, 2^{2t-2} - 2^{t-1})$-difference set in GR(4,$t$).

To see that E_i is reversible, since $tr(g^{i-j}) = tr(g^{2(i-j)})$, we have $2(h^{i-j} \oplus h^{2i-2j}) \in K_0$, or $2(h^i \oplus h^{2i-j}) \in h^jK_0 = K_j$. Thus, Theorem 4.1 implies that E_i is reversible. □

We are left with showing that the E_i indeed give rise to a linking system $\{E_{i,j} \mid i, j\}$ where $E_{i,j} = E_i[E_j]^{(-1)}$ as above. The group ring equations $(a \oplus K_j)[b \oplus K_j]^{(-1)} = 2^{t-1}((a \ominus b) \oplus K_j)$ and $(a \oplus K_j)[b \oplus K_{j'}]^{(-1)} = 2^{t-2}[(a \ominus b) \oplus 2\text{GR}(4,t)]$ for $j \neq j'$ lead to the following.

$$
\begin{aligned}
E_i[E_{i'}]^{(-1)} = & \sum_{j=0}^{2^t-2} (h^i \oplus h^{2i-j} \oplus K_j)[\sum_{j'=0}^{2^t-2} (h^{i'} \oplus h^{2i'-j'} \oplus K_{j'})]^{(-1)} \\
= & \; 2^{t-1} \sum_{j=j'} ((h^i \oplus h^{2i-j}) \ominus (h^{i'} \oplus h^{2i'-j}) \oplus K_j) \\
& + 2^{t-2} \sum_{j \neq j'} \Big((h^i \oplus h^{2i-j}) \ominus (h^{i'} \oplus h^{2i'-j'}) \oplus [2\text{GR}(4,t)] \Big)
\end{aligned}
$$

We need several technical lemmas to show that this group ring equation is what we want. Our ultimate goal is to show that the right hand side of the equation is $\mu E_{i,i'} + \nu(G - E_{i,i'})$ for $E_{i,i'}$ a reversible difference set in G. We first need to show that the coset representatives $((h^i \oplus h^{2i-j}) \ominus (h^{i'} \oplus h^{2i'-j}))$ are in distinct cosets of 2GR(4,t) for $i \neq j$, allowing us to apply Theorem 4.1 to the term $\sum_{j=j'}((h^i \oplus h^{2i-j}) \ominus (h^{i'} \oplus h^{2i'-j}) \oplus K_j)$.

Lemma 4.3 *Fix i and i' so that $i \neq i'$. For every $j \neq j'$, we have that $((h^i \oplus h^{2i-j}) \ominus (h^{i'} \oplus h^{2i'-j})) \ominus ((h^i \oplus h^{2i-j'}) \ominus (h^{i'} \oplus h^{2i'-j'})) \notin 2\mathrm{GR}(4,t)$.*

Proof: A simple calculation yields $((h^i \oplus h^{2i-j}) \ominus (h^{i'} \oplus h^{2i'-j})) \ominus ((h^i \oplus h^{2i-j'}) \ominus (h^{i'} \oplus h^{2i'-j'})) = (h^{-j} \ominus h^{-j'})(h^{2i} \oplus h^{2i'})$. When we apply π to this, we get $(g^{-j} \ominus g^{-j'})(g^{2i} \oplus g^{2i'})$, which is not 0 since $i \neq i'$ and $j \neq j'$, so $((h^i \oplus h^{2i-j}) \ominus (h^{i'} \oplus h^{2i'-j})) \ominus ((h^i \oplus h^{2i-j'}) \ominus (h^{i'} \oplus h^{2i'-j'}))$ is not in 2GR(4,t). □

We now turn our attention to the term $\sum_{j \neq j'} \left(h^i \oplus h^{2i-j} \ominus h^{i'} \ominus h^{2i'-j'} \oplus [2\mathrm{GR}(4,t)]\right)$. We first want to show that there are $2^t - 1$ terms $h^i \ominus h^{i'} \oplus [2\mathrm{GR}(4,t)]$ in this sum.

Lemma 4.4 *For a fixed j there is exactly one j' so that $\pi(h^i \oplus h^{2i-j} \ominus h^{i'} \ominus h^{2i'-j'}) = g^i \oplus g^{i'}$.*

Proof: If $\pi(h^i \oplus h^{2i-j} \ominus h^{i'} \ominus h^{2i'-j'}) = g^i \oplus g^{i'}$, then $g^{2i-j} = g^{2i'-j'}$, or $g^{j'} = g^{2i'-2i+j}$, so $j' = 2i' - 2i + j \bmod 2^t - 1$ is the unique j' □

Define the set $S_j = \left\{y \in \mathrm{GF}(2^t) \mid g^{2i-j} \oplus g^{2i'-j'} = y \text{ for some } j' \neq j, 0 \leq j' \leq 2^t - 2\right\}$. We observe that S_j has $2^t - 2$ distinct elements, and Lemma 4.4 states that $0 \in S_j$ for every j.

Lemma 4.5 *With the sets S_j defined above, $S_j = g^{-j}S_0$. For a given $r \in \mathrm{GR}(4,t)$ and given fixed values for $i, i', i \neq i'$, the number of distinct solutions to $\pi(r) = \pi(h^i \oplus h^{2i-j} \ominus h^{i'} \ominus h^{2i'-j'}), j \neq j'$ is $2^t - 3$ except $\pi(r) = \pi(h^i \ominus h^{i'})$ in which case the number of solutions is $2^t - 1$.*

Proof: Suppose $y \in S_0$. By definition this means that there is a $j' \neq 0$ so that $y = g^{2i} \oplus g^{2i'-j'}$. Multiply this equation by g^{-j} to get $yg^{-j} = g^{2i-j} \oplus g^{2i'-(j+j')}$. This shows that $g^{-j}S_0 \subset S_j$. The opposite inclusion is similar.

For the claim about the number of distinct solutions, each S_j is missing precisely 2 of the nonzero elements of the field. When we consider all of the sets S_j, each nonzero element γ of the field will be missing in precisely 2 of those sets and hence γ will appear in precisely $2^t - 3$ of the sets. □

Lemma 4.5 implies that every distinct coset representative in the group ring sum $\sum_{j \neq j'}(h^i \oplus h^{2i-j} \ominus h^{i'} \ominus h^{2i'-j'} \oplus [2\mathrm{GR}(4,t)])$ will appear exactly $2^t - 3$ times except $h^i \ominus h^{i'}$ which will appear $2^t - 1$ times.

We are now ready to state the main result of this section.

Theorem 4.6 *The sets $\{E_0, E_1, \ldots, E_{2^t-2}\}$ defined above form a $(2^{2t}, 2^{2t-1} - 2^{t-1}, 2^{2t-2} - 2^{t-1}; 2^t)$-reversible linking system in the additive group $G = (\mathrm{GR}(4,t))^+$ with $\mu = 2^{t-2}(2^t - 3)$ and $\nu = \mu + 2^{t-1}$.*

Proof: Lemmas 4.4 and 4.5 imply that $2^{t-2}\sum_{j \neq j'}(h^i \oplus h^{2i-j} \ominus (h^{i'} \oplus h^{2i'-j'}) \oplus [2\mathrm{GR}(4,t)]) = 2^{t-2}(2(h^i \oplus h^{i'} \oplus [2\mathrm{GR}(4,t)]) + (2^t - 3)G)$. Lemma 4.3 shows that $2^{t-1}\sum_{j=j'}(h^i \oplus h^{2i-j} \oplus h^{i'} \oplus h^{2i'-j} \oplus K_j) = 2^{t-1}D_{i,i'}$ for $D_{i,i'}$ a reversible $(2^{2t}, 2^{2t-1} - 2^{t-1}, 2^{2t-2} - 2^{t-1})$ difference set in the additive group of $\mathrm{GR}(4,t)$. We observe that $D_{i,i'} \cap (h^i \oplus h^{i'} \oplus [\mathrm{GR}(4,t)]) = \emptyset$. For otherwise, one of the coset representatives satisfies $\pi(h^i \oplus h^{2i-j} \oplus h^{i'} \oplus h^{2i'-j}) = \pi(h^i \oplus h^{i'})$, then $g^{2i-j} \oplus g^{2i'-j} = 0$,

or $g^{-j}(g^{2i} \oplus g^{2i'}) = 0$. Since g^{-j} is never 0, we would then conclude that $i = i'$, but that is not the case. Thus, $2^{t-2}(2(h^i \oplus h^{i'} \oplus [2\mathrm{GR}(4,t)]) + 2^{t-1}D_{i,i'} = 2^{t-1}(G - E_{i,i'})$ for $E_{i,i'} = G - D_{i,i'}$ a reversible $(2^{2t}, 2^{2t-1} - 2^{t-1}, 2^{2t-2} - 2^{t-1})$ difference set. Combining all of this gives $E_iE_{i'} = (2^{t-2}(2^t - 3) + 2^{t-1})(G - E_{i,i'}) + 2^{t-2}(2^t - 3)E_{i,i'}$. □

We remark that initial evidence suggests that the linked systems of symmetric designs resulting from Theorem 4.6 are new. Indeed, for $t = 2$, the $(16, 6, 2; 3)$-linking system arising from our theorem gives rise to an association scheme on 48 vertices which, while having the same parameters as the scheme coming from the Cameron-Seidel construction, is not isomorphic to the Cameron-Seidel scheme: the 48×48 matrix for relation R_1 defined in Section 2 has 2-rank 16 while the corresponding matrix for the Cameron-Seidel construction (using Kerdock sets) has 2-rank equal to 14.

Combining Theorems 2.4, 4.6, and 3.1, we get the following infinite family of linking systems.

Corollary 4.7 *Let G be the additive group of $\mathrm{GR}(4,t)$ and let G' be the elementary abelian group of order 2^{2t}. Then $\mathcal{G}_{r,s} = G^r \times G'^s$ contains a $\left(2^{2t}, 2^{2t-1} - 2^{t-1}, 2^{2t-2} - 2^{t-1}; 2^t\right)$-reversible linking system.*

As described earlier in this paper, Theorem 2.3 can be used to construct a system of linked symmetric designs once we have a linking system of difference sets, and systems of linked symmetric designs are equivalent to 3-class Q-antipodal cometric association schemes due to van Dam's theorem [6]. Any such association scheme can be doubled to yield a 4-class cometric association scheme which is both Q-antipodal and Q-bipartite, using a result of Martin, Muzychuk and Williford [13, Theorem 3.6]. These, in turn, give rise to real mutually unbiased bases by a result of LeCompte, Martin and Owens [11, Theorem 4.2].

5 Partial Difference Set constructions

In the previous section we were able to construct linking systems for groups with exponent 4 by using Galois Rings and the product construction. In this section, we will construct linking systems in higher exponent groups, still within 2-groups. In order to do this, we need a definition of a Partial Difference Set (PDS), [12]. We will only do this in a special case.

Definition 5.1 *A subset $D \subset G$ of a group G is a $(4N^2, t(2N-1), 2N + t^2 - 3t, t^2 - t)$ partial difference set for $1 \leq t \leq N, t|N, N$ even, if $|D| = t(2N-1), |G| = 4N^2$, and for every $g \in D, |\{(d,d') \in D^2 | g = d(d')^{-1}\}| = 2N + t^2 - 3t$ and for every $g \notin D, |\{(d,d') \in D^2 | g = d(d')^{-1}\}| = t^2 - t$. The partial difference set is called regular if the identity is not in D.*

For more background on PDSs see [12]. We are interested in PDSs with the parameters listed above due to the connection to Hadamard difference sets: if we can find a collection of $m \geq 2t$ mutually disjoint $(4N^2, t(2N-1), 2N + t^2 - 3t, t^2 - t)$ PDSs with the property that any union of N/t of those PDSs will be a reversible Hadamard difference set, then we can use the PDSs to construct a linking system in G. The following example illustrates the construction we will use in this section.

Example 5.2 *Consider $V = (\mathrm{GF}(8))^2$, the vector space of dimension 2 over $\mathrm{GF}(8)$. There are nine 1-dimensional subspaces of V: once we remove the 0 vector from each these subspaces we label them $H_0, H_1, \ldots, H_8$ (these can be thought of as the hyperplanes of V). Each of the H_i is a $(64, 7, 6, 0)$ PDS in the additive group of G, so this matches the parameters in Definition 5.1 with $N = 4, t = 1$. We can use the translates of the difference set $\{1, 2, 4\}$ in $\mathbb{Z}_7$ to identify subscripts of the H_i to include in the following sets: $D_i = H_8 \cup H_{1+i} \cup H_{2+i} \cup H_{4+i}, 0 \leq i \leq 6$ (the subscripts are read* mod7*). The D_i are $(64, 28, 12)$-difference sets by the partial spread construction method [8]. We claim that $\{D_0, D_1, \ldots, D_6\}$ forms a $(64, 28, 12; 8)$- reversible linking system in the additive*

group of V. (Here, as earlier, we abbreviate $D_{i,0}$ to D_i when convenient.) To see this, we need to compute the group ring equation D_iD_j for $i \neq j$:

$$\begin{aligned} D_iD_j = & \quad (H_8 + H_{1+i} + H_{2+i} + H_{4+i})(H_8 + H_{1+j} + H_{2+j} + H_{4+j}) \\ = & \quad H_8^2 + H_8H_{1+j} + \cdots + H_{4+i}H_{4+j} \end{aligned}$$

We claim that $H_iH_j = V - H_i - H_j - 0_V$ if $i \neq j$ and $H_iH_i = 6H_i + 7 \cdot 0_V$. Since the sets $\{1+i, 2+i, 4+i\}$ and $\{1+j, 2+j, 4+j\}$ have precisely one element in common by the difference set property, we will have one term in the sum that is H_kH_k for the k that is the overlap, and we have H_8H_8 as the first term, and the other fourteen terms will be H_iH_j for $i \neq j$. If the nonoverlap subscripts are a, b, c, and d, then we get the following sum.

$$\begin{aligned} D_iD_j = & \quad 6H_8 + 7 \cdot 0_V + 6H_k + 7 \cdot 0_V + 14V - 4H_a - 4H_b - 4H_c - 4H_d - 6H_8 - 6H_k - 14 \cdot 0_V \\ = & \quad 10(H_a + H_b + H_c + H_d) + 14(V - (H_a + H_b + H_c + H_d)) \end{aligned}$$

This verifies that the product of two of our difference sets will yield 10 copies of a difference set (by the partial spread construction $H_a \cup H_b \cup H_c \cup H_d$ is a reversible $(64, 28, 12)$ difference set in the additive group of V) and 14 copies of the complement, so $\{D_0, D_1, \ldots, D_6\}$ forms a $(64, 28, 12; 8)$-reversible linking system in V.

The group $\mathbb{Z}_{2^s-1}$ has a $(2^s - 1, 2^{s-1} - 1, 2^{s-2} - 1)$ difference set for all $s \geq 2$. Example 5.2 used the $s = 3$ example to identify which hyperplanes to use in building the difference sets in V. We will use the difference set in this group to identify the PDSs that will be pasted together to construct our linking system. The following theorem generalizes Example 5.2 (cf. [10]).

Theorem 5.3 *Suppose G is an abelian group of order 2^{2s}, and suppose that G contains at least 2^{s-r} mutually disjoint $(2^{2s}, 2^r(2^s-1), 2^s+2^{2r}-3\cdot 2^r, 2^{2r}-2^r)$ PDSs $\{P_0, P_1, \ldots, P_{2^{s-r}-1}\}, 0 \leq r \leq s-2$. Suppose further that any union of 2^{s-2-r} of the PDSs will be 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 and that any union of 2^{s-1-r} of the PDSs will be a reversible $(2^{2s}, 2^{2s-1}-2^{s-1}, 2^{2s-2}-2^{s-1})$ difference set in G. Then G contains a $\left(2^{2s}, 2^{2s-1}-2^{s-1}, 2^{2s-2}-2^{s-1}; 2^{s-r}\right)$-reversible linking system.*

Proof: We need to identify the Hadamard difference sets that will form the linking system. If $\Gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_{2^{s-r-1}-1}\}$ is a $(2^{s-r} - 1, 2^{s-r-1} - 1, 2^{s-r-2} - 1)$ difference set in $\mathbb{Z}_{2^{s-r}-1}$, then define $D_i = P_{2^{s-r}-1} \cup P_{i+\gamma_1} \cup P_{i+\gamma_2} \cup \cdots \cup P_{i+\gamma_{2^{s-r-1}-1}}$ where the subscripts are read $\bmod 2^{s-r} - 1$. By the conditions listed above, each of the D_i is a reversible difference set. Before verifying that D_iD_j satisfies condition *(2)* of Definition 2.2, we make a few observations. Any two translates of Γ intersect in exactly $2^{s-r-2} - 1$ elements and hence $D_i \cap D_j$ will have 2^{s-r-2} subsets P_k in common (they both have $P_{2^{s-r}-1}$ as well as the other intersections). Thus, if we call $D_i \cap D_j = A$, then we can write $D_i = A \cup B$ and $D_j = A \cup C$ for B, C subsets of G that are both the unions of 2^{s-r-2} sets P_k. The set A is a PDS by the assumptions in the theorem and hence will satisfy the group ring equation $A^2 = 2^{s-2}(2^s - 1)0_G + (2^s + 2^{2s-4} - 3 \cdot 2^{s-2})A + (2^{2s-4} - 2^{s-2})(G - A - 0_G)$. Similarly the sets B and C are PDSs and will satisfy a similar group ring equation. The fact that $D_i = A + B$ is a $(2^{2s}, 2^{2s-1} - 2^{s-1}, 2^{2s-2} - 2^{s-1})$ reversible difference set in G implies that $D_i^2 = (A+B)^2 = A^2 + 2AB + B^2 = (2^{2s-1} - 2^{s-1})0_G + (2^{2s-2} - 2^{s-1})(G - 0_G)$. Solving for AB we get $AB = \frac{D_i^2 - A^2 - B^2}{2}$, and we can also get $AC = \frac{D_i^2 - A^2 - C^2}{2}$ and $BC = \frac{D_i^2 - B^2 - C^2}{2}$ (note that we should replace D_i^2 by the appropriate difference set, but the squares of all the difference sets are equal and hence we simply use D_i^2 for all of them). Putting all this together, we get the following.

$$
\begin{aligned}
D_iD_j = & (A+B)(A+C)\\
= & A^2+AB+AC+BC\\
= & \frac{2A^2+3D_i^2-2A^2-2B^2-2C^2}{2}\\
= & \frac{3}{2}\left[(2^{2s-1}-2^{s-1})0_G+(2^{2s-2}-2^{s-1})(G-0_G)\right]-\\
& \left[(2^{s-2}(2^s-1)0_G+(2^s+2^{2s-4}-3\cdot 2^{s-2})B+(2^{2s-4}-2^{s-2})(G-B-0_G))\right]-\\
& \left[(2^{s-2}(2^s-1)0_G+(2^s+2^{2s-4}-3\cdot 2^{s-2})C+(2^{2s-4}-2^{s-2})(G-C-0_G)\right])\\
= & \left[\frac{3}{2}(2^{2s-1}-2^{s-1})-2^{s-2}(2^s-1)-2^{s-1}(2^s-1)\right]0_G+\\
& \left[\frac{3}{2}(2^{2s-2}-2^{s-1})-(2^s+2^{2s-4}-3\cdot 2^{s-2})-(2^{2s-4}-2^{s-2})\right](B+C)+\\
& \left[\frac{3}{2}(2^{2s-2}-2^{s-1})-(2^{2s-4}-2^{s-2})-(2^{2s-4}-2^{s-2})\right](G-B-C-0_G)\\
= & 2^{s-2}(2^s-1)(G-B-C)+2^{s-2}(2^s-3)(B+C)
\end{aligned}
$$

□

The construction in Theorem 5.3 depends on having a family of disjoint PDSs with the appropriate parameters. We note that a partition of the group into a partition of PDSs can be put into the context of amorphic Cayley association schemes of Latin square type, see [10].

As with Example 5.2, in the elementary abelian case ${\mathbb{Z}_2}^{2s} = \mathrm{GF}(2^s)^2$ we can partition the nonzero elements into 2^s+1 hyperplanes. The hyperplanes with the identity removed serve as the needed PDSs to apply Theorem 5.3 with $r=0$ in this case. The methods of Polhill [17] can be used to partition $(\mathbb{Z}_{2^a})^{2s}$ into 2^s PDSs with the appropriate parameters for all integers $a>1$ and $s\geq 1$. We note that the number of reversible Hadamard difference sets in the linking system does not increase with a in this construction, which leads one to wonder whether this can be improved for arbitrary a.

Theorem 5.4 *Let G be the group $(\mathbb{Z}_{2^a})^{2s}$. Then there are 2^s mutually disjoint $(2^{2as}, 2^{as-s}(2^{as}-1), 2^{as}+(2^{as-s})^2-3(2^{as-s}), (2^{as-s})^2-(2^{as-s})$- PDSs in G for all integers $a,s\geq 1$. Moreover, the union of any 2^{s-2} of these PDSs will be a $(2^{2as}, 2^{as-2}(2^{as}-1), 2^{as}+2^{2as-4}-3\cdot 2^{as-2}, 2^{2as-4}-2^{as-2})$ PDS in G, and the union of any 2^{s-1} of these PDSs will be a reversible $(2^{2as}, 2^{as-1}(2^{as}-1), 2^{2as-2}-2^{as-1})$ difference set in G.*

Combining Theorems 3.1, 5.4, and 4.6 we get the following result on linking systems.

Corollary 5.5 *Let G be group $(\mathbb{Z}_{2^{a_1}})^{2b_1}\times\cdots\times(\mathbb{Z}_{2^{a_k}})^{2b_k}\times {\mathbb{Z}_4}^b$ for positive integers a_i, b_i, b and write $|G|=4N^2$. Then G has a $(4N^2, 2N^2-N, N^2-N; \ell+1)$-reversible linking system, where $\ell=\min(b_1,b_2,...,b_k,b)$.*

6 Other results and some open problems

In this section we collect a few other results and questions of interest on this topic. The first of these follows from the work of Noda [16].

Theorem 6.1 *Suppose G has subsets D_1, D_2, and D_3, all of which are reversible $(4N^2, 2N^2-N, N^2-N)$ difference sets, and suppose also that $D_1D_2=\mu D_3+\nu(G-D_3)$ for $\mu,\nu\in\mathbb{Z}$. If N is even, then $\mu=N^2-\frac{3N}{2}$ and $\nu=N^2-\frac{N}{2}$. If N is odd, then $\mu=N^2-\frac{N-1}{2}$ and $\nu=N^2-\frac{3N-1}{2}$.*

So far all known examples have N a power of 2, but Theorem 6.1 points to the parameters we need if we are to find linking systems for N odd. It also shows that the parameters we have been using in the case when N is even are in fact necessarily the parameters.

Our second result in this section is actually an example. So far the maximum number of difference sets in a linking system for a group of order 2^{2t} is $2^t - 1$. We show that there can be more, at least in one case, in the following example.

Example 6.2 *Consider the group* $G = \mathbb{Z}_2^4$ *and the subsets*
$D_1 = \{(1,0,0,0),(0,1,0,0),(1,1,0,0),(0,0,1,0),(0,0,0,1),(0,0,1,1)\}$,
$D_2 = \{(1,0,0,0),(0,1,0,0),(1,1,0,0),(1,0,1,0),(0,1,0,1),(1,1,1,1)\}$,
$D_3 = \{(1,0,0,0),(0,1,0,0),(1,1,0,0),(1,0,0,1),(0,1,1,1),(1,1,1,0)\}$, *and*
$D_4 = \{(1,0,0,0),(0,1,0,0),(1,1,0,0),(1,0,1,1),(0,1,1,0),(1,1,0,1)\}$.
An easy computation verifies that this forms a $(16,6,2;5)$*-reversible* $(1,3,4)$*-reversible linking system in* G*. This is built in much the same way as Example 5.2 by using the hyperplanes of the vector space of dimension 2 over* GF(4)*. There are 5 such hyperplanes, and the difference sets all have* $H_0 = \{(1,0,0,0),(0,1,0,0),(1,1,0,0)\}$ *in common. Since this is a system of 4 linked designs on 16 points, by the work of Mathon, [14], we know that it must be the unique system that extends to a system of 7 designs, which is the same as the Cameron-Seidel system.*

Our final example is one in which the difference sets have the same linking property but are not all reversible.

Example 6.3 *Let* $G = \mathbb{Z}_4^2$*, and consider* $D_1 = \{(1,0),(3,1),(0,3),(3,0),(1,3),(0,1)\}, D_2 = \{(1,0),(3,1),(0,3),(1,2),(1,1),(2,1)\}$*, and* $D_3 = \{(1,0),(3,1),(0,3),(2,3),(3,3),(3,2)\}$*. The first of these,* D_1*, is a reversible* $(16,6,2)$ *difference set in* G*, and the second two are* $(16,6,2)$ *difference sets but are not reversible. These sets have the property that for distinct* i,j *it follows that* $D_iD_j = D + 3(G - D)$ *for some difference set* D*.*

We conclude with some open problems, and note that we believe this to be the first paper that directly relates difference sets to systems of linked symmetric designs. As a result, there is the potential to exploit difference sets and related algebraic sets to provide new examples of linked systems.

1 All of the systems of linked symmetric designs in this paper fit the parameters for the Cameron-Seidel family. Moreover, Cameron and Seidel's construction corresponds to the Kerdock codes viewed over GF(2). Since that time, these codes have famously been shown to be linear over $GR(4,t)$, [9]. One problem, then, is to investigate the relationships between the difference set constructions of linked systems over both GF(2) and $GR(4,t)$ with the constructions of the Cameron-Seidel family and the Kerdock codes.

2 Some of the linked systems constructed through difference sets are equivalent to the Cameron-Seidel example, while others are not. Can the Cameron-Seidel family be described with a difference set construction? Are there other infinite families that can be constructed with difference sets?

3 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?

4 Is there an infinite family that generalizes Example 6.3? To obtain systems of linked symmetric designs, we need for the difference sets to be reversible. From a design point of view, what are the properties of the linked systems when the difference sets are not reversible?

5 There are numerous generalizations of difference sets, such as partial difference sets and relative difference sets. Can these be exploited to find other linked systems of mathematical structures?

References

[1] E. Bannai and T. Ito. *Algebraic Combinatorics I: Association Schemes*. Benjamin-Cummings, Menlo Park, 1984.

[2] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Cambridge University Press, 1999.

[3] A. E. Brouwer, A. M. Cohen and A. Neumaier. *Distance-Regular graphs*. Springer-Verlag, Berlin, 1989.

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

[5] P.J. Cameron, J.J.Seidel, Quadratic forms over GF(2), *Proc. Koninkl. Nederl. Akademie van Wetenschappen, Series A*, Vol. 76 Indag. Math., **35** (1973), 1–8.

[6] E.R. van Dam, Three-class association schemes. *J. Alg. Combin.* **10**, 1999, 69–107.

[7] J.A. Davis, Q. Xiang, Constructions of low rank relative difference sets in 2-groups using Galois Rings, *Finite Fields and their Applications*, **6**, Issue 2, April 2000, 130–145.

[8] J.F. Dillon, Difference sets in 2-groups, *Finite Geometries and Combinatorial Designs. Contemp. Math.* **111**, 1990, 65–72.

[9] R.A. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory*, **40**, Issue 2, 1994, 301–319.

[10] T. Ito, A. Munemasa, M. Yamada, Amorphic association schemes over the Galois rings of characteristic 4, *European J. Combin.*,**12**, 1991, 513–526.

[11] N. LeCompte, W.J. Martin, W. Owens, On the equivalence between real mutually unbiased bases and a certain class of association schemes. *European J. Combin.* **31**, no. 6, 2010, 1499–1512.

[12] S.L. Ma, A survey of partial difference sets, *Des. Codes Crypt.* **4** Issue 3, 1994, 221–261.

[13] W. Martin, M. Muzychuk, J.Williford, Imprimitive cometric association schemes: construction and analysis, *J. of Alg. Comb.*, **25**, 2007, 399–415.

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

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

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

[17] J.B. Polhill, A construction of layered relative difference sets using Galois Rings, *Ars Combin.*, **78**, 2006, 83–94.