A new structure for difference matrices over abelian p-groups

Koen van Greevenbroek   Jonathan Jedwab

8 June 2018 (revised 28 November 2018)

Abstract

A difference matrix over a group is a discrete structure that is intimately related to many other combinatorial designs, including mutually orthogonal Latin squares, orthogonal arrays, and transversal designs. Interest in constructing difference matrices over 2-groups has been renewed by the recent discovery that these matrices can be used to construct large linking systems of difference sets, which in turn provide examples of systems of linked symmetric designs and association schemes. We survey the main constructive and nonexistence results for difference matrices, beginning with a classical construction based on the properties of a finite field. We then introduce the concept of a contracted difference matrix, which generates a much larger difference matrix. We show that several of the main constructive results for difference matrices over abelian p-groups can be substantially simplified and extended using contracted difference matrices. In particular, we obtain new linking systems of difference sets of size 7 in infinite families of abelian 2-groups, whereas previously the largest known size was 3.

1   Introduction

Let G be a non-trivial group. A (G, m, λ) *difference matrix over* G is an $m \times \lambda|G|$ matrix (a_{ij}) with $0 \le i \le m-1$ and $0 \le j \le \lambda|G|-1$ and each entry $a_{ij} \in G$ such that, for all distinct rows i and ℓ, the multiset of "differences"

$$\{a_{ij}a_{\ell j}^{-1} : 0 \le j \le \lambda|G|-1\}$$

contains each element of G exactly λ times. When the group G is abelian, we shall (except in Section 4) use additive rather than multiplicative group notation.

Example 1.1. *Let* $G = \mathbb{Z}_2^3$ *and represent the element* $(u, v, w) \in G$ *in the compressed form uvw. The matrix*

$$\begin{bmatrix} 000 & 000 & 000 & 000 & 000 & 000 & 000 & 000 \\ 000 & 101 & 111 & 010 & 110 & 011 & 001 & 100 \\ 000 & 100 & 010 & 110 & 001 & 101 & 011 & 111 \\ 000 & 111 & 110 & 001 & 011 & 100 & 101 & 010 \\ 000 & 001 & 101 & 100 & 111 & 110 & 010 & 011 \end{bmatrix}$$

Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada.
J. Jedwab is supported by NSERC.
Email: kvangree@sfu.ca, jed@sfu.ca

is a $(G, 5, 1)$ difference matrix. For example, the differences between corresponding entries of the two shaded rows are

$$000, 010, 001, 011, 101, 111, 100, 110,$$

in which each element of G appears exactly once.

Difference matrices are related to many other combinatorial designs, including mutually orthogonal Latin squares, orthogonal arrays, transversal designs, whist tournaments, generalized Steiner triple systems, and optical orthogonal codes [Col07], [PC16]. Recently, difference matrices over 2-groups were used as the key ingredient in a new construction of linking systems of difference sets [JLS18]. The central objective is to determine, for a given group G and parameter λ, the largest number of rows m for which a (G, m, λ) difference matrix exists. Colbourn [Col07] gives a concise summary of known existence and nonexistence results as of 2007.

This paper is organized so that the material up to the end of Section 4 is a survey, whereas that from Section 5 onwards presents new ideas and results. In Section 2 we describe some basic properties of difference matrices, including nonexistence results and connections to other combinatorial structures. In Section 3 we review the major constructions for difference matrices, principally: a classical construction over elementary abelian p-groups based on finite fields; a composition construction based on the Kronecker product; and a construction of 4-row difference matrices over abelian noncyclic groups. In Section 4 we explain how difference matrices with $\lambda = 1$ over certain 2-groups were recently used to construct linking systems of difference sets.

In Section 5 we introduce the concept of a contracted difference matrix over an abelian p-group, which generates a much larger difference matrix over the same group. We derive a finite field construction, a composition construction, and an abelian noncyclic 2-group construction for contracted difference matrices. These constructions are significantly simpler and more compact than the corresponding constructions for difference matrices given in Section 3, but we show that they can often be used to produce results for difference matrices that are just as powerful as those obtained in Section 3. In Section 6 we present four examples of contracted difference matrices found by computer search. These examples generate new infinite families of (contracted) difference matrices over abelian 2-groups with more rows than previously known, from which we in turn construct larger linking systems of difference sets than previously known. In Section 7 we present some open questions about (contracted) difference matrices. Appendix A contains an example of the largest known contracted difference matrix over each abelian 2-group of order at most 64. Python 3 code for checking and searching for (contracted) difference matrices is available at https://gitlab.com/koenvg/contracted-difference-matrices.

2   Basic properties

In this section we present some basic properties of difference matrices, including nonexistence results and connections to other combinatorial designs.

If G is a group and $A = (a_{ij})$ is a (G, m, λ) difference matrix, then the difference matrix property is preserved when each entry of a column of A is right-multiplied by a fixed $g \in G$, because $(a_{ij}g)(a_{\ell j}g)^{-1} = a_{ij}a_{\ell j}^{-1}$. By right-multiplying all entries of each column j of A by a_{0j}^{-1}, we may therefore assume that each entry of row 0 of A is 1_G. The difference property of the matrix then implies that, for each $i \geq 1$, row i of G contains every element of G exactly λ times. We may likewise right-multiply all entries of each row i by a_{i0}^{-1}, so that each entry of column 0 of A is also 1_G. The resulting matrix is in *normalized form*.

2

If a (G, m, λ) difference matrix with $m \geq 2$ exists, then deleting one row gives a $(G, m - 1, \lambda)$ difference matrix.

The existence of a (G, m, λ) difference matrix implies the existence of a resolvable orthogonal array $\mathrm{OA}_\lambda(m, |G|)$ and a transversal design $\mathrm{TD}_\lambda(m + 1, |G|)$, and is a generalized Bhaskar Rao design $\mathrm{GBRD}(m, m, \lambda|G|; G)$ [Col07].

A trivial $(G, 2, \lambda)$ difference matrix exists for every group G and every integer $\lambda \geq 1$, for example comprising a first row containing $\lambda|G|$ copies of the identity 1_G and a second row containing each element of G exactly λ times. The number of rows m in a nontrivial (G, m, λ) difference matrix therefore satisfies $m \geq 3$, and by the following counting result it also satisfies $m \leq \lambda|G|$.

Theorem 2.1 (Jungnickel [Jun79, Theorem 2.2]). *Let G be a group, and suppose there exists a (G, m, λ) difference matrix. Then $m \leq \lambda|G|$.*

Proof. The following self-contained argument is adapted from the proof of a more general result given in [Jun79, Proposition 3.1]. By assumption there exists a (G, m, λ) difference matrix $A = (a_{ij})$, and we may assume that A is in normalized form. For $g \in G$ and $0 \leq j \leq \lambda|G| - 1$, let n_{gj} be the number of times g occurs in column j of A, so that

$$n_{gj} = \sum_{i=0}^{m-1} I[a_{ij} = g]$$

where $I[X]$ is the indicator function of event X. Then

$$\sum_{j>0} \sum_{g \in G} n_{gj} = \sum_{j>0} \sum_{i} \sum_{g \in G} I[a_{ij} = g]$$
$$= \sum_{j>0} \sum_{i} 1$$
$$= (\lambda|G| - 1)m, \tag{1}$$

whereas

$$\sum_{j>0} \sum_{g \in G} n_{gj}^2 = \sum_{j>0} \sum_{g \in G} \sum_{i,\ell} I[a_{ij} = a_{\ell j} = g]$$
$$= \sum_{j>0} \sum_{g \in G} \left(\sum_{i} I[a_{ij} = g] + \sum_{i \neq \ell} I[a_{ij} = a_{\ell j} = g] \right)$$
$$= \sum_{j>0} \sum_{i} \sum_{g \in G} I[a_{ij} = g] + \sum_{i \neq \ell} \sum_{j>0} \sum_{g \in G} I[a_{ij} = a_{\ell j} = g]$$
$$= \sum_{j>0} \sum_{i} 1 + \sum_{i \neq \ell} \sum_{j>0} I[a_{ij} = a_{\ell j}]$$
$$= \sum_{j>0} \sum_{i} 1 + \sum_{i \neq \ell} (\lambda - 1)$$

because the normalization of A gives $a_{i0} = a_{\ell 0}$ for all distinct i and ℓ. Therefore

$$\sum_{j>0} \sum_{g \in G} n_{gj}^2 = (\lambda|G| - 1)m + m(m - 1)(\lambda - 1), \tag{2}$$

3

and the result follows by substituting (1) and (2) into the Cauchy-Schwarz inequality

$$\Big(\sum_{j>0}\sum_{g\in G} n_{gj}\Big)^2 \leq (\lambda|G|-1)|G|\sum_{j>0}\sum_{g\in G} n_{gj}^2$$

and simplifying. □

If the upper bound $m = \lambda|G|$ in Theorem 2.1 is attained, then the resulting $(G, \lambda|G|, \lambda)$ difference matrix is a square matrix known as a *generalized Hadamard matrix* $\mathrm{GH}(|G|, \lambda)$ *over G* (see [Lau07] for a survey). In particular, a $\mathrm{GH}(2, 2\lambda)$ over the group $(\{-1, 1\}, \cdot)$ is a *Hadamard matrix* of order 4λ (see [Hor06] or [CK07], for example, for background on this much-studied topic). In all known examples of a $\mathrm{GH}(|G|, \lambda)$ over G, the group order $|G|$ is a prime power and, if G is not elementary abelian, then $|G|$ is a square [Lau07, p. 303].

We shall be mostly concerned with (G, m, λ) difference matrices for which $m < \lambda|G|$, and especially those with $\lambda = 1$ because of several connections to other combinatorial objects. In particular, a $(G, m, 1)$ difference matrix is equivalent to a G-regular set of $m-1$ mutually orthogonal Latin squares of order $|G|$ [Jun80, Theorem 1], and to a set of $m-2$ pairwise orthogonal orthomorphisms of G [Eva07, p. 195]. Moreover, a crucial ingredient in a recent construction of reduced linking systems of difference sets [JLS18] is a $(G, m, 1)$ difference matrix for certain 2-groups G, as described in Section 4. We shall therefore pay special attention to $(G, m, 1)$ difference matrices over 2-groups. A further reason for regarding the case $\lambda = 1$ as fundamental is that there are many methods for composing two difference matrices (the composition constructions of Theorems 3.7, 3.8, 3.21, and 3.22), and for constructing a new difference matrix from another (the homomorphism construction of Lemma 3.4), under all of which the value of λ increases or remains the same; in particular, we can use Theorem 3.22 to produce a (G, m, λ) difference matrix for each $\lambda > 1$ from a $(G, m, 1)$ matrix.

The following nonexistence result rules out, as a special case, the existence of a $(G, 3, 1)$ difference matrix when G is a cyclic 2-group. Indeed, we shall see (for example in Theorem 3.12 and from Table 2) that the currently known existence pattern for $(G, m, 1)$ difference matrices over a 2-group G of fixed order and for fixed m appears to favor groups of smaller exponent and larger rank.

Theorem 2.2 (Hall and Paige [HP55, Theorem 5], Drake [Dra79, Theorem 1.10])**.** *Let G be a group containing a nontrivial cyclic Sylow 2-subgroup, and let λ be odd. Then there does not exist a $(G, 3, \lambda)$ difference matrix.*

3 Constructions for difference matrices

In this section we describe some of the principal constructive results for difference matrices, especially as they relate to the case $\lambda = 1$. We sometimes omit proofs, or else describe constructions without proving they satisfy the required poperties.

3.1 Finite field construction (Drake)

The following construction, based on properties of a finite field, is a foundational example that shows the upper bound of Theorem 2.1 can be attained for every elementary abelian group.

4

Proposition 3.1 (Drake [Dra79, Proposition 1.5]). *Let p be prime and let n be a positive integer. Then the additive form of a multiplication table for $\mathrm{GF}(p^n)$ is a $(\mathbb{Z}_p^n, p^n, 1)$ difference matrix.*

Example 3.2. *We use Proposition 3.1 to construct a $(\mathbb{Z}_2^2, 4, 1)$ difference matrix. Let α be a root of the primitive polynomial $f(x) = x^2 + x + 1$ in $\mathbb{Z}_2[x]$, and construct $\mathrm{GF}(2^2)$ as $\mathbb{Z}_2[x]/\langle f(x)\rangle$. The additive group of $\mathrm{GF}(2^2)$ is $\mathbb{Z}_2^2$, and the multiplication table of $\mathrm{GF}(2^2)$ written in additive notation gives the $(\mathbb{Z}_2^2, 4, 1)$ difference matrix*

$$
\begin{array}{c|cccc}
\cdot & 0 & 1 & \alpha & \alpha^2 \\
\hline
0 & 00 & 00 & 00 & 00 \\
1 & 00 & 01 & 10 & 11 \\
\alpha & 00 & 10 & 11 & 01 \\
\alpha^2 & 00 & 11 & 01 & 10
\end{array}.
$$

Example 3.3. *We use Proposition 3.1 to construct a $(\mathbb{Z}_2^3, 8, 1)$ difference matrix. Let α be a root of the primitive polynomial $f(x) = x^3 + x + 1$ in $\mathbb{Z}_2[x]$, and construct $\mathrm{GF}(2^3)$ as $\mathbb{Z}_2[x]/\langle f(x)\rangle$. The additive group of $\mathrm{GF}(2^3)$ is $\mathbb{Z}_2^3$, and the multiplication table of $\mathrm{GF}(2^3)$ written in additive notation gives the $(\mathbb{Z}_2^3, 8, 1)$ difference matrix*

$$
\begin{array}{c|cccccccc}
\cdot & 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\
\hline
0 & 000 & 000 & 000 & 000 & 000 & 000 & 000 & 000 \\
1 & 000 & 001 & 010 & 100 & 011 & 110 & 111 & 101 \\
\alpha & 000 & 010 & 100 & 011 & 110 & 111 & 101 & 001 \\
\alpha^2 & 000 & 100 & 011 & 110 & 111 & 101 & 001 & 010 \\
\alpha^3 & 000 & 011 & 110 & 111 & 101 & 001 & 010 & 100 \\
\alpha^4 & 000 & 110 & 111 & 101 & 001 & 010 & 100 & 011 \\
\alpha^5 & 000 & 111 & 101 & 001 & 010 & 100 & 011 & 110 \\
\alpha^6 & 000 & 101 & 001 & 010 & 100 & 011 & 110 & 111
\end{array}.
$$

(We shall refer to the shaded entries of this multiplication table in Example 5.7.)

The next result extends the construction of Proposition 3.1 to give examples with $\lambda > 1$.

Lemma 3.4 ([Dra79, Proposition 1.8], [Jun79, Proposition 4.4]). *Let G and H be groups. Suppose that $\phi\colon G \to H$ is a surjective homomorphism and that $A = (a_{ij})$ is a (G, m, λ) difference matrix. Then $\phi(A) = (\phi(a_{ij}))$ is an $(H, m, \lambda|\operatorname{Ker}\phi|)$ difference matrix.*

Proof. The difference of two distinct rows of A contains each element of G exactly λ times, so by the First Isomorphism Theorem the difference of two distinct rows of $\phi(A)$ contains each element of H exactly $\lambda|\operatorname{Ker}\phi|$ times. □

Corollary 3.5 ([Dra79, Corollary 1.9]). *Let p be prime, and let $m, n \geq 1$ and $s \geq 0$ be integers. Then there exists a $(\mathbb{Z}_p^n, m, p^s)$ difference matrix if and only if $m \leq p^{n+s}$.*

Proof. The condition $m \leq p^{n+s}$ is necessary, by Theorem 2.1. To show existence for $m < p^{n+s}$, delete $p^{n+s} - m$ of the rows of the difference matrix for $m = p^{n+s}$. It remains to construct a $(\mathbb{Z}_p^n, p^{n+s}, p^s)$ difference matrix. By Proposition 3.1, there exists a $(\mathbb{Z}_p^{n+s}, p^{n+s}, 1)$ difference matrix. Apply Lemma 3.4 using a surjective homomorphism $\phi : \mathbb{Z}_p^{n+s} \to \mathbb{Z}_p^n$. □

Example 3.6. *We use Lemma 3.4 to construct a $(\mathbb{Z}_2^2, 8, 2)$ difference matrix from the $(\mathbb{Z}_2^3, 8, 1)$ difference matrix of Example 3.3. Apply the canonical homomorphism $\mathbb{Z}_2^3 \to \mathbb{Z}_2^2$ to remove the third component of each element of $\mathbb{Z}_2^3$, giving the $(\mathbb{Z}_2^2, 8, 2)$ difference matrix*

$$
\begin{bmatrix}
00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\
00 & 00 & 01 & 10 & 01 & 11 & 11 & 10 \\
00 & 01 & 10 & 01 & 11 & 11 & 10 & 00 \\
00 & 10 & 01 & 11 & 11 & 10 & 00 & 01 \\
00 & 01 & 11 & 11 & 10 & 00 & 01 & 10 \\
00 & 11 & 11 & 10 & 00 & 01 & 10 & 01 \\
00 & 11 & 10 & 00 & 01 & 10 & 01 & 11 \\
00 & 10 & 00 & 01 & 10 & 01 & 11 & 11
\end{bmatrix} .
$$

3.2   Composition construction (Buratti)

The following composition construction combines difference matrices in groups H and K to produce a difference matrix in $H \times K$. We can use this composition to combine difference matrices in groups of prime power order, including those of Section 3.3, giving a rich existence pattern.

Theorem 3.7 (Jungnickel [Jun79, Proposition 4.5]). *Let H and K be groups. Suppose there exists an (H, m, λ) difference matrix and a (K, m, μ) difference matrix. Then there exists a $(H \times K, m, \lambda\mu)$ difference matrix.*

Theorem 3.7 occurs as the case $G = H \times K$ of the following more general composition construction, which combines difference matrices in groups H and G/H to produce a difference matrix in G.

Theorem 3.8 (Buratti [Bur98, Theorem 2.5 and Corollary 2.6]). *Let G be a group containing a normal subgroup H. Suppose that A is an (H, m, λ) difference matrix and that $(b_{ij}H)$ is a $(G/H, m, \mu)$ difference matrix, and let $B = (b_{ij})$. Then the matrix each of whose rows is the Kronecker product of the corresponding rows in A and B is a $(G, m, \lambda\mu)$ difference matrix.*

Example 3.9. *We use Theorem 3.8 to construct a $(G, 4, 1)$ difference matrix for $G = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, using additive notation. Let $H = \langle 010, 200 \rangle$, so that $G/H = \langle 001 + H, 100 + H \rangle$ and both H and G/H are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. The $(\mathbb{Z}_2^2, 2, 1)$ difference matrix of Example 3.2 gives the $(H, 4, 1)$ difference matrix*

$$
A =
\begin{bmatrix}
000 & 000 & 000 & 000 \\
000 & 010 & 200 & 210 \\
000 & 200 & 210 & 010 \\
000 & 210 & 010 & 200
\end{bmatrix}
$$

and the $(G/H, 4, 1)$ difference matrix $(b_{ij} + H)$, where

$$
B = (b_{ij}) =
\begin{bmatrix}
000 & 000 & 000 & 000 \\
000 & 001 & 100 & 101 \\
000 & 100 & 101 & 001 \\
000 & 101 & 001 & 100
\end{bmatrix} .
$$

By Theorem 3.8, the Kronecker product of corresponding rows in A and B then gives the rows of the $(G, 4, 1)$ difference matrix

$$\begin{bmatrix} (000+000) & (000+000) & (000+000) & (000+000) & (000+000) & (000+000) & \cdots \\ (000+000) & (000+001) & (000+100) & (000+101) & (010+000) & (010+001) & \cdots \\ (000+000) & (000+100) & (000+101) & (000+001) & (200+000) & (200+100) & \cdots \\ (000+000) & (000+101) & (000+001) & (000+100) & (210+000) & (210+101) & \cdots \end{bmatrix}$$

$$= \begin{bmatrix} 000 & 000 & 000 & 000 & 000 & 000 & 000 & 000 & 000 & 000 & 000 & 000 & 000 & 000 & 000 & 000 \\ 000 & 001 & 100 & 101 & 010 & 011 & 110 & 111 & 200 & 201 & 300 & 301 & 210 & 211 & 310 & 311 \\ 000 & 100 & 101 & 001 & 200 & 300 & 301 & 201 & 210 & 310 & 311 & 211 & 010 & 110 & 111 & 011 \\ 000 & 101 & 001 & 100 & 210 & 311 & 211 & 310 & 010 & 111 & 011 & 110 & 200 & 301 & 201 & 300 \end{bmatrix}.$$

Repeated application of the composition construction of Theorem 3.8 to difference matrices over elementary abelian groups, as given by Proposition 3.1, produces examples over a larger set of groups.

Example 3.10. *We use Theorem 3.8 to construct $(G, 4, 1)$ difference matrix for $G = \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2$. Form a chain of subgroups*

$$G \supset G_1 \supset G_2,$$

where $G_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ and $G_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ such that $G/G_1 \cong \mathbb{Z}_2^4$ and $G_1/G_2 \cong \mathbb{Z}_2^3$. By Proposition 3.1, there is a $(G/G_1, 2^4, 1)$ and a $(G_1/G_2, 2^3, 1)$ and a $(G_2, 2^2, 1)$ difference matrix. Use Theorem 3.8 to combine the first 2^2 rows of the $(G_2, 2^2, 1)$ and $(G_1/G_2, 2^3, 1)$ difference matrices to give a $(G_1, 2^2, 1)$ difference matrix; then combine this with the first 2^2 rows of the $(G/G_1, 2^4, 1)$ difference matrix to give a $(G, 2^2, 1)$ difference matrix. The number of rows in this difference matrix is $\min(2^4, 2^3, 2^2) = 2^2$.

However, by using a different chain of subgroups we can instead obtain a $(G, 8, 1)$ difference matrix: choose $G_1' \cong \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $G_2' \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ such that $G/G_1' \cong \mathbb{Z}_2^3$ and $G_1'/G_2' \cong \mathbb{Z}_2^3$. Since each of G_2', G_1'/G_2', and G/G_1' is isomorphic to $\mathbb{Z}_2^3$, combination under Theorem 3.8 produces a $(G, 2^3, 1)$ difference matrix. The number of rows in this difference matrix is $\min(2^3, 2^3, 2^3) = 2^3$.

Example 3.10 shows that when Proposition 3.1 and Theorem 3.8 are used to produce a difference matrix by choosing a chain of subgroups, some choices can result in a larger number of rows for the final difference matrix than others. Proposition 3.11 shows how to choose a chain of subgroups that will produce the largest number of rows in the final difference matrix, and Theorem 3.12 gives the result of making this choice.

Proposition 3.11 (Buratti [Bur98, Lemma 2.10])**.** *Let p be prime, and let G be an abelian group of order p^n and exponent p^e. Then $\lfloor n/e \rfloor$ is the largest integer s for which there is a chain of subgroups G_i of G satisfying*

$$G = G_0 \supset G_1 \supset \cdots \supset G_r$$

for some integer $r \geq 0$, such that G_r and each of the quotient groups G_{i-1}/G_i is elementary abelian and of order at least p^s. The upper bound $\lfloor n/e \rfloor$ is attained when each of the $\lfloor n/e \rfloor$ largest direct factors of G_{i-1} is reduced by a factor of p in G_i and when G_r is the first resulting subgroup that is elementary abelian, and in this case we have

$$G_{i-1}/G_i \cong \mathbb{Z}_p^{\lfloor n/e \rfloor} \text{ for each } i \text{ satisfying } 1 \leq i \leq r, \text{ and } G_r \cong \mathbb{Z}_p^{\ell} \text{ for some integer } \ell \geq \lfloor n/e \rfloor.$$

Theorem 3.12 (Buratti [Bur98, Theorem 2.11]). *Let p be prime, and let G be an abelian group of order p^n and exponent p^e. Then there exists a $(G, p^{\lfloor n/e \rfloor}, 1)$ difference matrix.*

Proof. By Proposition 3.11, there is an integer $r \geq 0$ and a chain of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_r$$

such that $G_{i-1}/G_i \cong \mathbb{Z}_p^{\lfloor n/e \rfloor}$ for each i satisfying $1 \leq i \leq r$, and $G_r \cong \mathbb{Z}_p^\ell$ for some integer $\ell \geq \lfloor n/e \rfloor$. By Proposition 3.1 there is therefore a $(G_{i-1}/G_i, p^{\lfloor n/e \rfloor}, 1)$ difference matrix for each i, and by Corollary 3.5 there is a $(G_r, p^{\lfloor n/e \rfloor}, 1)$ difference matrix. Apply Theorem 3.8 to successive pairs $(G, H) = (G_{r-1}, G_r), (G_{r-2}, G_{r-1}), \ldots, (G_0, G_1)$ to obtain a $(G_i, p^{\lfloor n/e \rfloor}, 1)$ difference matrix for $i = r - 1, r - 2, \ldots, 0$. The case $i = 0$ gives the result. $\square$

Theorem 3.8 can also be used to obtain the following result.

Theorem 3.13 ([Bur98, Theorem 2.13]). *Let G be a group and let p be the smallest prime divisor of $|G|$. Then there exists a $(G, p, 1)$ difference matrix.*

3.3   Abelian noncyclic construction (Pan and Chang)

By Proposition 3.11, no chain of subgroups will produce a larger number of rows than $p^{\lfloor n/e \rfloor}$ in Theorem 3.12 under combination of Proposition 3.1 and Theorem 3.8. However, we now show that larger values are sometimes possible, using the following construction in 2-groups with large exponent.

Theorem 3.14 (Pan and Chang [PC16, Lemma 3.3]). *Let e be a positive integer. Then there exists a $(\mathbb{Z}_{2^e} \times \mathbb{Z}_2, 4, 1)$ difference matrix.*

Construction for Theorem 3.14. Define sets

$$
\begin{aligned}
I_1 &= \{0, 1, \ldots, 2^{e-2} - 1\}, \\
I_2 &= \{2^{e-2}, 2^{e-2} + 1, \ldots, 2^{e-1} - 1\}, \\
I_1^* &= I_1 \setminus \{2^{e-2} - 1\} \cup \{2^{e-1} - 1\}, \\
I_2^* &= I_2 \setminus \{2^{e-1} - 1\} \cup \{2^{e-2} - 1\}.
\end{aligned}
$$

For $0 \leq i \leq 2^{e-1} - 1$, define length 4 column vectors over $\mathbb{Z}_{2^e} \times \mathbb{Z}_2$

$$
c_i^{(0)} = \begin{cases} \left[(0,0) \quad (2i,0) \quad (4i,0) \quad (-2i,0) \right]^\mathsf{T} & \text{for } i \in I_1, \\ \left[(0,0) \quad (2i,0) \quad (4i,1) \quad (-2i,1) \right]^\mathsf{T} & \text{for } i \in I_2, \end{cases}
$$

$$
c_i^{(1)} = \begin{cases} \left[(0,0) \quad (2i,1) \quad (4i+1,0) \quad (-2i-1,1) \right]^\mathsf{T} & \text{for } i \in I_1, \\ \left[(0,0) \quad (2i,1) \quad (4i+1,1) \quad (-2i-1,0) \right]^\mathsf{T} & \text{for } i \in I_2, \end{cases}
$$

$$
c_i^{(2)} = \begin{cases} \left[(0,0) \quad (2i+1,0) \quad (4i+2,0) \quad (-2i-1,0) \right]^\mathsf{T} & \text{for } i \in I_1, \\ \left[(0,0) \quad (2i+1,0) \quad (4i+2,1) \quad (-2i-1,1) \right]^\mathsf{T} & \text{for } i \in I_2, \end{cases}
$$

$$c_i^{(3)} = \begin{cases} \begin{bmatrix} (0,0) & (2i+1,1) & (4i+3,0) & (-2i-2,1) \end{bmatrix}^\mathsf{T} & \text{for } i \in I_1^*, \\ \begin{bmatrix} (0,0) & (2i+1,1) & (4i+3,1) & (-2i-2,0) \end{bmatrix}^\mathsf{T} & \text{for } i \in I_2^*. \end{cases}$$

Define a $4 \times 2^{e-1}$ matrix

$$D_r = \begin{bmatrix} c_0^{(r)} & c_1^{(r)} & \dots & c_{2^{e-1}-1}^{(r)} \end{bmatrix} \quad \text{for } r = 0, 1, 2, 3.$$

Then a $(\mathbb{Z}_{2^e} \times \mathbb{Z}_2, 4, 1)$ difference matrix is

$$D = \begin{bmatrix} D_0 \mid D_1 \mid D_2 \mid D_3 \end{bmatrix}. \qquad \square$$

Example 3.15. *We use the construction for Theorem 3.14 to produce a $(\mathbb{Z}_8 \times \mathbb{Z}_2, 4, 1)$ difference matrix. Set $I_1 = \{0, 1\}$, $I_2 = \{2, 3\}$, $I_1^* = \{0, 3\}$ $I_2^* = \{1, 2\}$. Each D_r is a 4×4 matrix whose columns are $c_0^{(r)}, c_1^{(r)}, c_2^{(r)}, c_3^{(r)}$, and the constructed matrix is*

$$D = \begin{bmatrix} 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 20 & 40 & 60 & 01 & 21 & 41 & 61 & 10 & 30 & 50 & 70 & 11 & 31 & 51 & 71 \\ 00 & 40 & 01 & 41 & 10 & 50 & 11 & 51 & 20 & 60 & 21 & 61 & 30 & 71 & 31 & 70 \\ 00 & 60 & 41 & 21 & 71 & 51 & 30 & 10 & 70 & 50 & 31 & 11 & 61 & 40 & 20 & 01 \end{bmatrix}.$$

By combining the result of Theorem 3.14 with a suitable chain of subgroups, we can construct a $(G, 4, 1)$ difference matrix in all abelian noncyclic 2-groups.

Theorem 3.16 (Pan and Chang [PC16, Lemma 3.4]). *Let G be an abelian noncyclic 2-group. Then there exists a $(G, 4, 1)$ difference matrix.*

Proof. Let G have order 2^n. The proof is by induction on $n \geq 2$. The base case $n = 2$ requires a $(\mathbb{Z}_2^2, 4, 1)$ difference matrix, which is provided by Proposition 3.1. Now assume all cases up to $n - 1 \geq 2$ are true. If $G = \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_2$, then case n is true by Theorem 3.14, and if $G = \mathbb{Z}_2^3$ then case n is true by Corollary 3.5. Otherwise we can choose a noncyclic subgroup H of G such that $G/H \cong \mathbb{Z}_2^2$. There exists a $(G/H, 4, 1)$ difference matrix by Proposition 3.1, and an $(H, 4, 1)$ difference matrix by the inductive hypothesis. Apply Theorem 3.8 to produce a $(G, 4, 1)$ difference matrix, proving case n and completing the induction. $\square$

Pan and Chang provide a generalization of Theorem 3.16 to non-2-groups, and a corresponding result for the case $\lambda > 1$.

Theorem 3.17 ([PC16, Theorem 1.2]). *Let G be an abelian noncyclic group whose Sylow 2-subgroup of G is trivial or noncyclic. Then there exists a $(G, 4, 1)$ difference matrix.*

Theorem 3.18 ([PC16, Theorem 1.3]). *Let G be an abelian group and let $\lambda > 1$ be an integer. If λ is even, or if λ is odd and the Sylow 2-subgroup of G is trivial or noncyclic, then there exists a $(G, 4, \lambda)$ difference matrix.*

3.4 Other constructions

Theorems 2.2 and 3.17 settle the existence question for a $(G, 4, 1)$ difference matrix over all abelian groups G, except those that are cyclic of odd order. The following result concerns these groups.

Theorem 3.19 (Ge [Ge05, Theorem 3.12]). *Let $v \geq 5$ be an odd integer for which $\gcd(v, 27) \neq 9$. Then there exists a $(\mathbb{Z}_v, 4, 1)$ difference matrix.*

The existence pattern for the cases not handled by Theorem 3.19 (namely those for which $\gcd(v, 27) = 9$) is not yet clear; it is known [PC16, Lemma 2.2] that there does not exist a $(\mathbb{Z}_9, 4, 1)$ difference matrix.

The following construction, like that of Proposition 3.1, is based on properties of a finite field and provides examples of generalized Hadamard matrices.

Theorem 3.20 (Jungnickel [Jun79, Theorem 2.4]). *Let p be an odd prime and let n be a positive integer. Then there exists a $(\mathbb{Z}_p^n, 2p^n, 2)$ difference matrix.*

The construction of Theorem 3.8 composes difference matrices over groups H and G/H. In contrast, the construction of Theorem 3.21 (based on a Kronecker product) and of Theorem 3.22 (based on concatenation) both compose two difference matrices over the same group.

Theorem 3.21 (Shrikhande [Shr64, Theorem 3]). *Let G be a group. Suppose there exists a (G, m, λ) difference matrix and a (G, m', μ) difference matrix. Then there exists a $(G, mm', \lambda\mu|G|)$ difference matrix.*

Theorem 3.22 (Jungnickel [Jun79, Proposition 4.2]). *Let G be a group. Suppose there exists a (G, m, λ) difference matrix and a (G, m, μ) difference matrix. Then there exists a $(G, m, \lambda + \mu)$ difference matrix.*

There are several constructions of difference matrices based on the existence of other types of combinatorial design such as pairwise balanced designs, orthogonal arrays, transversal designs, affine resolvable block designs, rings, difference families, and group complementary pairs [CK96], [Jun79], [Lau86], [Lau87].

3.5   Computer search results

After submitting the original version of this paper, we became aware of the following computer search results for difference matrices in groups of order 16. These results, which were found using the viewpoint of orthogonal orthomorphisms, improve on the constructions of Sections 3.1–3.3.

Proposition 3.23 (Lazebnik and Thomason [LT04, p.1556]). *The largest number of rows m for which a $(G, m, 1)$ difference matrix exists is*

(i) *5 for $G = \mathbb{Z}_8 \times \mathbb{Z}_2$,*

(ii) *8 for $G = \mathbb{Z}_4 \times \mathbb{Z}_4$,*

(iii) *8 for $G = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.*

4   Reduced linking systems of difference sets

We use multiplicative notation for groups throughout this section.

Definition 4.1. *Let G be a group of order v 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 $\{d_1 d_2^{-1} : d_1, d_2 \in D$ and $d_1 \neq d_2\}$ contains every non-identity element of G exactly λ times and, by convention, $n = k - \lambda$.*

A difference set in a group G is equivalent to a symmetric design with a regular automorphism group [Lan83] (see [Jun92] and its updates [JS97], [JS98], for example, for background).

Definition 4.2. *Let G be a group of order v 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*

$$\sum_{d_i \in D_i} d_i \sum_{d_j \in D_j} d_j^{-1} = (\mu - \nu) \sum_{d \in D(i,j)} d + \nu \sum_{g \in G} g \quad \text{in } \mathbb{Z}[G]. \tag{3}$$

A reduced linking system of difference sets is equivalent to a linking system of difference sets [JLS18, Proposition 1.7], as 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 [Dam99].

Jedwab, Li, and Simon [JLS18] recently showed how to construct a reduced linking system of difference sets, based on a difference matrix over a 2-group having $\lambda = 1$.

Theorem 4.3 ([JLS18, Theorems 1.2 and 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 there exists a reduced linking system of (v, k, λ, n)-difference sets in G of size $m - 1$, where*

$$(v, k, \lambda, n) = (2^{2d+2}, 2^d(2^{d+1} - 1), 2^d(2^d - 1), 2^{2d}). \tag{4}$$

Construction for Theorem 4.3. Let $s = 2^{d+1} - 1$ and let $H_1, H_2, \ldots, H_s$ be the subgroups of G corresponding to the hyperplanes (d-dimensional subspaces) of E when E is regarded as a vector space of dimension $d + 1$ over GF(2). Let the normalized form (see Section 2) of the $(G/E, m, 1)$-difference matrix be $B = (b_{ij}E)$ for $0 \leq i \leq m - 1$ and $0 \leq j \leq s$. Choose $e_{ij} \in E$ for each $1 \leq i \leq m - 1$ and $1 \leq j \leq s$ arbitrarily and let

$$D_i = \bigcup_{j=1}^{s} b_{ij}e_{ij}H_j \quad \text{for } 1 \leq i \leq m - 1.$$

Then $\{D_1, D_2, \ldots, D_{m-1}\}$ is a reduced linking system of (v, k, λ, n)-difference sets in G of size $m-1$, with (v, k, λ, n) as given in (4). $\qquad\square$

Example 4.4 ([JLS18, Example 5.7]). *We use the construction for Theorem 4.3 to produce a reduced linking system of $(16, 6, 2, 4)$-difference sets in $G = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \langle x, y, z \rangle$ of size 3. Let $E = \langle x^2, z \rangle$, which is isomorphic to $\mathbb{Z}_2^2$. 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 $H_1 = \langle x^2 \rangle, H_2 = \langle z \rangle, H_3 = \langle x^2z \rangle$. Using the $(\mathbb{Z}_2^2, 4, 1)$ difference matrix of Example 3.2, the matrix $(b_{ij}E)$ is a $(G/E, 4, 1)$-difference matrix where*

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

Take, for example,

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

Then $\{D_1, D_2, D_3\}$ is a reduced linking system of $(16, 6, 2, 4)$-difference sets in G of size 3, where where

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

The application of Theorem 4.3 to the difference matrices specified in Theorems 3.16 and 3.12 gives the infinite families of linking systems of difference sets of Theorem 4.5 (i) and (ii), respectively.

Theorem 4.5 ([JLS18, Corollaries 5.8 and 5.9])**.** *Let G be an abelian group of order 2^{2d+2}, rank at least $d + 1$, and exponent 2^e.*

(i) *If $e \le d + 1$, then there exists a reduced linking system of (v, k, λ, n)-difference sets in G of size 3, with (v, k, λ, n) as given in (4).*

(ii) *If $2 \le e \le \frac{d+3}{2}$, then there exists a reduced linking system of (v, k, λ, n)-difference sets in G of size $2^{\lfloor \frac{d+1}{e-1} \rfloor} - 1$, with (v, k, λ, n) as given in (4).*

5 Contracted difference matrices

We observe that some difference matrices over an abelian p-group have a particularly rich structure, in that their rows can be written as a $\mathbb{Z}_p$-linear combination of a small set of rows, and their columns can likewise be written as a $\mathbb{Z}_p$-linear combination of a small set of columns. In this section we capture this structure by introducing the concept of a contracted difference matrix, and present a series of constructions for contracted difference matrices related to those for difference matrices given in Section 3.

Definition 5.1. *Let p be prime and let M be a $k \times \ell$ matrix over an abelian p-group $(G, +)$. The p-expansion of M, written $f_p(M)$, is a $p^k \times p^\ell$ matrix over G whose rows are indexed by $\mathbf{r} \in \mathbb{Z}_p^k$ and whose columns are indexed by $\mathbf{c} \in \mathbb{Z}_p^\ell$. The $(\mathbf{r}, \mathbf{c})$ entry of $f_p(M)$ is the vector-matrix-vector product $\mathbf{r}M\mathbf{c}^\mathsf{T}$ (in which $\mathbf{r}$ and $\mathbf{c}$ are regarded as row vectors).*

The p-expansion of a matrix can be represented as the product of matrices, as demonstrated in Example 5.3.

Definition 5.2. *Let p be prime and let G be an abelian group of order p^n. A $k \times (n + s)$ matrix M over G is a (G, k, s) contracted difference matrix if the $p^k \times p^{n+s}$ matrix $f_p(M)$ is a (G, p^k, p^s) difference matrix.*

Example 5.3. *The matrix* $M = \begin{bmatrix} 01 & 10 & 20 \\ 21 & 01 & 10 \end{bmatrix}$ *over* $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ *is a* $(G, 2, 0)$ *contracted difference matrix because its* 2*-expansion*

$$f_2(M) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 01 & 10 & 20 \\ 21 & 01 & 10 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$= \begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{cccccccc} 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ \begin{bmatrix} 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 10 & 01 & 11 & 21 & 31 & 20 & 30 \\ 00 & 20 & 10 & 30 & 01 & 21 & 11 & 31 \\ 00 & 30 & 11 & 01 & 20 & 10 & 31 & 21 \end{bmatrix} \end{array}$$

(in which the row and column indexing is shown explicitly) is a $(G, 4, 1)$ *difference matrix.*

Example 5.4. *The matrix* $M = \begin{bmatrix} 01 & 10 \\ 10 & 11 \end{bmatrix}$ *over* $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ *is a* $(G, 2, 0)$ *contracted difference matrix, because its* 3*-expansion*

$$f_3(M) = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}^\mathsf{T} \begin{bmatrix} 01 & 10 \\ 10 & 11 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$$

$$= \begin{array}{c} \\ 00 \\ 01 \\ 02 \\ 10 \\ 11 \\ 12 \\ 20 \\ 21 \\ 22 \end{array} \begin{array}{ccccccccc} 00 & 01 & 02 & 10 & 11 & 12 & 20 & 21 & 22 \\ \begin{bmatrix} 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 11 & 22 & 10 & 21 & 02 & 20 & 01 & 12 \\ 00 & 22 & 11 & 20 & 12 & 01 & 10 & 02 & 21 \\ 00 & 10 & 20 & 01 & 11 & 21 & 02 & 12 & 22 \\ 00 & 21 & 12 & 11 & 02 & 20 & 22 & 10 & 01 \\ 00 & 02 & 01 & 21 & 20 & 22 & 12 & 11 & 10 \\ 00 & 20 & 10 & 02 & 22 & 12 & 01 & 21 & 11 \\ 00 & 01 & 02 & 12 & 10 & 11 & 21 & 22 & 20 \\ 00 & 12 & 21 & 22 & 01 & 10 & 11 & 20 & 02 \end{bmatrix} \end{array}$$

is a $(G, 9, 1)$ *difference matrix.*

If a (G, k, s) contracted difference matrix with $k \geq 2$ exists, then deleting one row gives a $(G, k-1, s)$ contracted difference matrix.

A trivial $(G, 1, s)$ contracted difference matrix exists for every abelian p-group $G = \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_r}}$ and every integer $s \geq 0$, for example comprising a single row containing the elements $\bigcup_{i=1}^{r} \{\mathbf{e}_i, p\mathbf{e}_i, p^2\mathbf{e}_i, \ldots, p^{a_i - 1}\mathbf{e}_i\}$ together with s copies of the identity 0_G, where $\mathbf{e}_i$ is the vector of length r taking the value 1 in position i and 0 in all other positions. For p a prime and G an abelian group of order p^n, the number of rows in a nontrivial (G, k, s) contracted difference matrix therefore satisfies $k \geq 2$, and by Theorem 2.1 and Definition 5.2 it also satisfies $k \leq n + s$.

We now give a method for testing whether a given matrix is a (G, k, s) contracted difference matrix without calculating the p-expansion of the matrix in full. The method simplifies further in the case $s = 0$, which is of particular interest because a $(G, k, 0)$ contracted difference matrix produces a difference matrix with $\lambda = 1$ (having special significance, as discussed in Section 2).

13

Lemma 5.5. *Let p be prime and let G be an abelian group of order p^n.*

(i) *Let M be a $k \times (n + s)$ matrix over G. Then M is a (G, k, s) contracted difference matrix if and only if the set*

$$\left\{ \mathbf{a} M \mathbf{c}^\mathsf{T} : \mathbf{c} \in \mathbb{Z}_p^{n+s} \right\} \text{ contains each element of } G \text{ exactly } p^s \text{ times}$$

for all nonzero row vectors $\mathbf{a} = (a_i)$ of length k, where each a_i is an integer satisfying $-p < a_i < p$.

(ii) *Let M be a $k \times n$ matrix over G. Then M is a $(G, k, 0)$ contracted difference matrix if and only if*

$$\mathbf{a} M \mathbf{b}^\mathsf{T} = 0_G \quad \text{implies} \quad \mathbf{a} = \mathbf{0} \text{ or } \mathbf{b} = \mathbf{0}$$

for all row vectors $\mathbf{a} = (a_i)$ and $\mathbf{b} = (b_j)$ of length k and n respectively, where each a_i and b_j is an integer satisfying $-p < a_i, b_j < p$.

Proof.

(i) By definition, M is a (G, k, s) contracted difference matrix if and only if $f_p(M)$ is a (G, p^k, p^s) difference matrix. Since the row of $f_p(M)$ indexed by $\mathbf{r} \in \mathbb{Z}_p^k$ comprises the elements of the set $\left\{ \mathbf{r} M \mathbf{c}^\mathsf{T} : \mathbf{c} \in \mathbb{Z}_p^{n+s} \right\}$, this condition holds if and only if the set $\left\{ (\mathbf{r}_1 - \mathbf{r}_2) M \mathbf{c}^\mathsf{T} : \mathbf{c} \in \mathbb{Z}_p^{n+s} \right\}$ contains each element of G exactly p^s times, for all distinct $\mathbf{r}_1, \mathbf{r}_2 \in \mathbb{Z}_p^k$. Set $\mathbf{a} = \mathbf{r}_1 - \mathbf{r}_2$ to obtain the result.

(ii) Using the case $s = 0$ in the proof of part (i), we have that M is a $(G, k, 0)$ contracted difference matrix if and only if the set $\left\{ (\mathbf{r}_1 - \mathbf{r}_2) M \mathbf{c}^\mathsf{T} : \mathbf{c} \in \mathbb{Z}_p^n \right\}$ contains each element of G exactly once, for all distinct $\mathbf{r}_1, \mathbf{r}_2 \in \mathbb{Z}_p^k$. Since G has order p^n, this condition holds if and only if $(\mathbf{r}_1 - \mathbf{r}_2) M (\mathbf{c}_1 - \mathbf{c}_2)^\mathsf{T} \neq 0_G$ for all distinct $\mathbf{r}_1, \mathbf{r}_2 \in \mathbb{Z}_p^k$ and all distinct $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{Z}_p^n$. Set $\mathbf{a} = \mathbf{r}_1 - \mathbf{r}_2$ and $\mathbf{b} = \mathbf{c}_1 - \mathbf{c}_2$ to obtain the result. $\square$

We now present several constructions of contracted difference matrices over abelian p-groups, which are related to the constructions for difference matrices given in Section 3 as set out in Table 1. Each of the contracted difference matrix constructions is more compact and simple than the corresponding difference matrix construction, as can be seen by comparing the examples of this section with those of Section 3. The proofs of some of the corresponding pairs of results are similar (particularly Corollary 3.5/5.9, Corollary 3.12/5.13, and Corollary 3.16/5.16); however, the construction proving Theorem 5.15 is considerably more straightforward than that proving Theorem 3.14. By Definition 5.2, the major results Theorems 3.12 and 3.16 are direct consequences of Corollaries 5.13 and 5.16, respectively.

5.1 Finite field construction

The constructions in this section are related to those in Section 3.1.

Proposition 5.6. *Let p be prime, let n be a positive integer, and let α be a primitive element of $\mathrm{GF}(p^n)$. Then the additive form of the multiplication table for $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a $(\mathbb{Z}_p^n, n, 0)$ contracted difference matrix.*

Table 1: Related constructions in Sections 3 and 5.

	construction of difference matrix	construction of contracted difference matrix
Finite field	Proposition 3.1 Corollary 3.5	Proposition 5.6 Corollary 5.9
Homomorphism	Lemma 3.4	Lemma 5.8
Composition	Theorem 3.8 Theorem 3.12	Theorem 5.11 Corollary 5.13
Abelian noncyclic 2-group	Theorem 3.14 Theorem 3.16	Theorem 5.15 Corollary 5.16

Proof. The matrix corresponding to the multiplication table for $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ has (i,j) entry α^{i+j} for $0 \leq i, j \leq n-1$. We shall use Lemma 5.5 (ii) to show that the additive form of this matrix is a $(\mathbb{Z}_p^n, n, 0)$ contracted difference matrix, where we regard $\mathbb{Z}_p^n$ as the additive group of $\mathrm{GF}(p^n)$. Suppose that $0 = \sum_{i,j=0}^{n-1} a_i \alpha^{i+j} b_j$ for integers a_i, b_j satisfying $-p < a_i, b_j < p$. Then $\sum_{i=0}^{n-1} a_i \alpha^i = 0$ or $\sum_{j=0}^{n-1} b_j \alpha^j = 0$, and since $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is an integral basis for $\mathbb{Z}_p^n$ we conclude that either $a_i = 0$ for all i or else $b_j = 0$ for all j. $\square$

Example 5.7. *We use Proposition 5.6 to construct a $(\mathbb{Z}_2^3, 3, 0)$ contracted difference matrix. The shaded entries of Example 3.3, constructed using a primitive element α of $\mathrm{GF}(2^3)$ satisfying $\alpha^3 + \alpha + 1 = 0$, comprise the additive form of the multiplication table for $\{1, \alpha, \alpha^2\}$ and so are a $(\mathbb{Z}_2^3, 3, 0)$ contracted difference matrix.*

The next result extends the construction of Proposition 5.6 to give examples with $s > 0$.

Lemma 5.8. *Let p be prime, and let G and H be abelian groups of orders p^{n+u} and p^n, respectively. Suppose that $\phi : G \to H$ is a surjective homomorphism and that $M = (m_{ij})$ is a (G, k, s) contracted difference matrix. Then $\phi(M) = (\phi(m_{ij}))$ is an $(H, k, u+s)$ contracted difference matrix.*

Proof. Let $\mathbf{a} = (a_i)$ be a nonzero row vector of length k, where each a_i is an integer satisfying $-p < a_i < p$. By Lemma 5.5 (i), we are given that $\{\mathbf{a} M \mathbf{c}^\intercal : \mathbf{c} \in \mathbb{Z}_p^{n+u+s}\}$ contains each element of G exactly p^s times and are required to prove that $\{\mathbf{a} \phi(M) \mathbf{c}^\intercal : \mathbf{c} \in \mathbb{Z}_p^{n+u+s}\}$ contains each element of H exactly $p^u p^s$ times. This follows from the First Isomorphism Theorem, because $|\mathrm{Ker}(\phi)| = |G|/|H| = p^u$. $\square$

Corollary 5.9. *Let p be prime, and let $k, n \geq 1$ and $s \geq 0$ be integers. Then there exists a $(\mathbb{Z}_p^n, k, s)$ contracted difference matrix if and only if $k \leq n + s$.*

Proof. The condition $k \leq n + s$ is necessary, by Theorem 2.1 and Definition 5.2. To show existence for $k < n + s$, delete $n + s - k$ of the rows of the contracted difference matrix for $k = n + s$. It remains to construct a $(\mathbb{Z}_p^n, n+s, s)$ contracted difference matrix. By Proposition 5.6, there exists a $(\mathbb{Z}_p^{n+s}, n+s, 0)$ contracted difference matrix. Apply Lemma 5.8 using a surjective homomorphism $\phi : \mathbb{Z}_p^{n+s} \to \mathbb{Z}_p^n$. $\square$

Example 5.10. *We use Lemma 5.8 to construct a $(\mathbb{Z}_2^2, 4, 2)$ contracted difference matrix. Firstly construct a $(\mathbb{Z}_2^4, 4, 0)$ contracted difference matrix according to Proposition 5.6, using a primitive element α of $\mathrm{GF}(2^4)$ satisfying $\alpha^4 + \alpha + 1 = 0$:*

$$
\begin{array}{c|cccc}
\cdot & 1 & \alpha & \alpha^2 & \alpha^3 \\
\hline
1 & 0001 & 0010 & 0100 & 1000 \\
\alpha & 0010 & 0100 & 1000 & 0011 \\
\alpha^2 & 0100 & 1000 & 0011 & 0110 \\
\alpha^3 & 1000 & 0011 & 0110 & 1100
\end{array}.
$$

Now apply the canonical homomorphism from $\mathbb{Z}_2^4$ to $\mathbb{Z}_2^2$ that removes the last two components of each element of $\mathbb{Z}_2^4$, giving the $(\mathbb{Z}_2^2, 4, 2)$ contracted difference matrix

$$
\begin{bmatrix}
00 & 00 & 01 & 10 \\
00 & 01 & 10 & 00 \\
01 & 10 & 00 & 01 \\
10 & 00 & 01 & 11
\end{bmatrix}.
$$

5.2 Composition construction

The constructions in this section are related to those in Section 3.2.

Theorem 5.11. *Let G be an abelian p-group and let H be a subgroup of G. Suppose that L is an (H, k, s) contracted difference matrix and that $(m_{ij} + H)$ is a $(G/H, k, t)$ contracted difference matrix, and let $M = (m_{ij})$. Then the matrix $\left[L \mid M \right]$ is a $(G, k, s+t)$ contracted difference matrix.*

Proof. Let $|H| = p^n$ and $|G| = p^{n+u}$. Let $\mathbf{a} = (a_i)$ be a nonzero row vector of length k, where each a_i is an integer satisfying $-p < a_i < p$. By Lemma 5.5 (i), we are given that $\left\{ \mathbf{a}L\mathbf{c}^{\intercal} : \mathbf{c} \in \mathbb{Z}_p^{n+s} \right\}$ contains each element of H exactly p^s times and that $\left\{ \mathbf{a}(m_{ij} + H)\mathbf{d}^{\intercal} : \mathbf{d} \in \mathbb{Z}_p^{u+t} \right\}$ contains each element of G/H exactly p^t times. Since each element of G can be written uniquely as the sum of an element of H and a coset representative of H in G, it follows that $\left\{ \mathbf{a}[L \mid M](\mathbf{c}, \mathbf{d})^{\intercal} : (\mathbf{c}, \mathbf{d}) \in \mathbb{Z}_p^{n+s+u+t} \right\}$ contains each element of G exactly $p^s p^t$ times. The result follows by Lemma 5.5 (i). $\square$

Example 5.12. *We use Theorem 5.11 to construct a $(G, 2, 0)$ contracted difference matrix for $G = \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Let $H = \langle 300, 010 \rangle$, so that both H and G/H are isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$. Apply Proposition 5.6, using a primitive element α of $\mathrm{GF}(3^2)$ satisfying $\alpha^2 + \alpha + 2 = 0$, to construct the $(H, 2, 0)$ and $(G/H, 2, 0)$ contracted difference matrices*

$$
\begin{bmatrix}
010 & 300 \\
300 & 610
\end{bmatrix}
\quad \text{and} \quad
\begin{bmatrix}
001 + H & 100 + H \\
100 + H & 201 + H
\end{bmatrix}.
$$

By Theorem 5.11, a $(G, 2, 0)$ contracted difference matrix is

$$
\begin{bmatrix}
010 & 300 & 001 & 100 \\
300 & 610 & 100 & 201
\end{bmatrix}.
$$

The proof of the next result follows that of Theorem 3.12, by replacing each quoted result for a difference matrix by the corresponding result for a contracted difference matrix according to Table 1.

Corollary 5.13. *Let p be prime, and let G be an abelian group of order p^n and exponent p^e. Then there exists a $(G, \lfloor n/e \rfloor, 0)$ contracted difference matrix.*

Example 5.14. *We illustrate the proof of Corollary 5.13 with $p = 2$, $n = 11$, $e = 3$ to construct a $(G, 3, 0)$ contracted difference matrix for $G = \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$. Following Proposition 3.11, we set $G = G_0$ and choose successive subgroups G_1, G_2, ... so that each of the $\lfloor n/e \rfloor = 3$ largest direct factors of G_{i-1} is reduced by a factor of 2 in G_i, and determine G_r to be the first resulting subgroup that is elementary abelian:*

$$G_0 = \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2,$$
$$\langle 20000, 02000, 00200, 00010, 00001 \rangle = G_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_2,$$
$$\langle 40000, 04000, 00200, 00020, 00001 \rangle = G_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

This gives $r = 2$ and $G_0/G_1 \cong \mathbb{Z}_2^3$ and $G_1/G_2 \cong \mathbb{Z}_2^3$ and $G_2 \cong \mathbb{Z}_2^5$.

Use Example 5.7 to construct the $(G_0/G_1, 3, 0)$ and $(G_1/G_2, 3, 0)$ contracted difference matrices

$$\begin{bmatrix} 00100 + G_1 & 01000 + G_1 & 10000 + G_1 \\ 01000 + G_1 & 10000 + G_1 & 01100 + G_1 \\ 10000 + G_1 & 01100 + G_1 & 11000 + G_1 \end{bmatrix} \quad and \quad \begin{bmatrix} 00010 + G_2 & 02000 + G_2 & 20000 + G_2 \\ 02000 + G_2 & 20000 + G_2 & 02010 + G_2 \\ 20000 + G_2 & 02010 + G_2 & 22000 + G_2 \end{bmatrix}.$$

Apply Proposition 5.6, using a primitive element α of $\mathrm{GF}(2^5)$ satisfying $\alpha^5 + \alpha^2 + 1 = 0$, to construct a $(G_2, 5, 0)$ contracted difference matrix and then delete the last two rows to leave a $(G_2, 3, 0)$ contracted difference matrix

$$\begin{bmatrix} 00001 & 00020 & 00200 & 04000 & 40000 \\ 00020 & 00200 & 04000 & 40000 & 00201 \\ 00200 & 04000 & 40000 & 00201 & 04020 \end{bmatrix}.$$

Now use Theorem 5.11 to combine the $(G_2, 3, 0)$ and $(G_1/G_2, 3, 0)$ contracted difference matrices to give a $(G_1, 3, 0)$ contracted difference matrix; then combine this with the $(G_0/G_1, 3, 0)$ contracted difference matrix to give a $(G_0, 3, 0)$ contracted difference matrix

$$\begin{bmatrix} 00001 & 00020 & 00200 & 04000 & 40000 & 00010 & 02000 & 20000 & 00100 & 01000 & 10000 \\ 00020 & 00200 & 04000 & 40000 & 00201 & 02000 & 20000 & 02010 & 01000 & 10000 & 01100 \\ 00200 & 04000 & 40000 & 00201 & 04020 & 20000 & 02010 & 22000 & 10000 & 01100 & 11000 \end{bmatrix}.$$

5.3 Abelian noncyclic 2-group construction

The constructions in this section are related to those in Section 3.3.

Theorem 5.15. *Let e be a positive integer. Then there exists a $(\mathbb{Z}_{2^e} \times \mathbb{Z}_2, 2, 0)$ contracted difference matrix.*

Proof. We use Lemma 5.5 (ii) to show that $2 \times (e + 1)$ matrix

$$M = \begin{bmatrix} (0,1) & (1,0) & (2,0) & (4,0) & (8,0) & \cdots & (2^{e-1}, 0) \\ (2^{e-1}, 1) & (0,1) & (1,0) & (2,0) & (4,0) & \cdots & (2^{e-2}, 0) \end{bmatrix}$$

is a $(\mathbb{Z}_{2^e} \times \mathbb{Z}_2, 2, 0)$ contracted difference matrix. Suppose that $\mathbf{a}M\mathbf{b}^{\mathsf{T}} = (0, 0)$, where $\mathbf{a} = \begin{bmatrix} a_1 & a_2 \end{bmatrix}$ and $\mathbf{b} = \begin{bmatrix} b_e & b_0 & b_1 & b_2 & \dots & b_{e-1} \end{bmatrix}$, and that each $a_i, b_j \in \{-1, 0, 1\}$ and $(a_1, a_2) \neq (0, 0)$. It is sufficient to show that each b_j is 0.

Expand the equation $\mathbf{a}M\mathbf{b}^{\mathsf{T}} = (0,0)$ to give

$$2^{e-1}a_2b_e + a_1b_0 + (2a_1 + a_2)(b_1 + 2b_2 + 4b_3 + \cdots + 2^{e-2}b_{e-1}) \equiv 0 \pmod{2^e} \qquad (5)$$

$$(a_1 + a_2)b_e + a_2b_0 \equiv 0 \pmod{2}. \qquad (6)$$

Case 1: $a_2 = 0$. By (5),

$$a_1(b_0 + 2b_1 + 4b_2 + \cdots + 2^{e-1}b_{e-1}) \equiv 0 \pmod{2^e}.$$

Since $(a_1, a_2) \neq (0,0)$ we have $a_1 \neq 0$, and therefore $b_0 = b_1 = \cdots = b_{e-1} = 0$. Then (6) gives $a_1b_e \equiv 0 \pmod{2}$, so that $b_e = 0$.

Case 2: $a_2 \in \{-1, 1\}$. We firstly note that $a_1b_0 = 0$: if $a_1 = 0$ this is immediate, otherwise we have $a_1 + a_2 \equiv 0 \pmod{2}$ and then from (6) we conclude that $b_0 = 0$. Now substitute $a_1b_0 = 0$ in (5) to give

$$(2a_1 + a_2)(b_1 + 2b_2 + 4b_3 + \cdots + 2^{e-2}b_{e-1} + 2^{e-1}b_e) \equiv 0 \pmod{2^e}.$$

Since $2a_1 + a_2 \in \{-3, -1, 1, 3\}$, this implies that

$$b_1 + 2b_2 + 4b_3 + \cdots + 2^{e-2}b_{e-1} + 2^{e-1}b_e \equiv 0 \pmod{2^e}$$

and so $b_1 = b_2 = \cdots = b_e = 0$. Then from (6) we have $b_0 = 0$. $\qquad\square$

We remark that Theorem 5.15 implies Theorem 3.14, and yet relies on a considerably simpler construction.

The proof of the next result follows that of Theorem 3.16, by replacing each quoted result for a difference matrix by the corresponding result for a contracted difference matrix according to Table 1.

Corollary 5.16. *Let G be an abelian noncyclic 2-group. Then there exists a $(G, 2, 0)$ contracted difference matrix.*

6 Further examples of contracted difference matrices

In this section we present a $(G, 3, 0)$ contracted difference matrix in each of four abelian 2-groups G, and derive several consequences. These examples cannot be obtained from the constructions given in Section 5, but were instead found by computer search.

A principal advantage of searching for a contracted difference matrix is that an exhaustive search can be feasible even though an exhaustive search for the corresponding size of difference matrix is not, because only an exponentially smaller number of matrices need be considered: in the present case, when G is an abelian group of order 2^n, a $(G, 3, 0)$ contracted difference matrix has $3n$ entries in G whereas a $(G, 2^3, 1)$ difference matrix has 2^{n+3} entries in G. Even when neither exhaustive search is feasible, a random search for a $(G, 3, 0)$ contracted difference matrix appears experimentally to be successful far more often than a random search for a $(G, 2^3, 1)$ difference matrix. A further advantage of searching for a contracted difference matrix is that Lemma 5.5 allows us to check a candidate contracted difference matrix efficiently, without the need to expand the matrix and check the differences between all row pairs explicitly.

Example 6.1. *The following $(G, 3, 0)$ contracted difference matrices were found by computer search:*

$$\begin{bmatrix} 001 & 010 & 100 & 200 \\ 010 & 201 & 001 & 100 \\ 211 & 100 & 201 & 210 \end{bmatrix} \ \textit{over } G = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2,$$

$$\begin{bmatrix} 001 & 010 & 020 & 100 & 200 \\ 021 & 001 & 211 & 010 & 100 \\ 220 & 101 & 200 & 210 & 320 \end{bmatrix} \ \textit{over } G = \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2,$$

$$\begin{bmatrix} 0001 & 0010 & 0100 & 1000 & 2000 \\ 0010 & 0100 & 2001 & 0001 & 1000 \\ 1001 & 2110 & 0001 & 0010 & 0101 \end{bmatrix} \ \textit{over } G = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,$$

$$\begin{bmatrix} 4101 & 2000 & 1100 & 0010 & 7111 & 0101 \\ 4010 & 0111 & 2011 & 4001 & 7001 & 0001 \\ 4000 & 7110 & 5100 & 0011 & 5010 & 2011 \end{bmatrix} \ \textit{over } G = \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Table 2 combines the contracted difference matrices of Example 6.1 with the constructive results of Corollaries 5.13 and 5.16 to show the largest number of rows k for which a $(G, k, 0)$ contracted difference matrix is known to exist, for all abelian 2-groups of order at most 64. The nonexistence results of Theorems 2.1 and 2.2, together with exhaustive search results, are used to indicate when the displayed value of k is known to be the maximum possible.

6.1 A new infinite family of $(G, 3, 0)$ contracted difference matrices

We can use the four examples given in Example 6.1 to construct a $(G, 3, 0)$ contracted difference matrix for infinitely many abelian 2-groups G that are not handled by the methods of Section 5. By Theorem 5.11 it is sufficient to find a chain of subgroups G_i of G satisfying

$$G = G_0 \supset G_1 \supset \cdots \supset G_r \supset G_{r+1} = \{0_G\}$$

such that there exists a $(G_{i-1}/G_i, 3, 0)$ contracted difference matrix for each i satisfying $1 \leq i \leq r + 1$. By Proposition 5.6 and Example 6.1, this is possible in particular if the quotient group G_{i-1}/G_i is isomorphic to $\mathbb{Z}_2^r$ for some $r \geq 3$ or to one of the groups in the set

$$\{\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \ \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2, \ \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \ \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2\},$$

for each i. For example, to construct a $(G, 3, 0)$ contracted difference matrix for $G = \mathbb{Z}_{256} \times \mathbb{Z}_{32} \times \mathbb{Z}_{16} \times \mathbb{Z}_4 \times \mathbb{Z}_2$, we can use the subgroup chain $G = G_0$, $G_1 \cong \mathbb{Z}_{32} \times \mathbb{Z}_{16} \times \mathbb{Z}_{16} \times \mathbb{Z}_2$, $G_2 \cong \mathbb{Z}_{16} \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$, $G_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $G_4 = \{0_G\}$. It does not seem straightforward to determine the set of all such groups G explicitly, but we can show the existence of a large set of such groups by a straightforward induction.

Theorem 6.2. *Let $n \geq 3$ and $e \leq n/2$ be positive integers. Then for at least one abelian group G of order 2^n and exponent 2^e there exists a $(G, 3, 0)$ contracted difference matrix.*

Proof. The proof is by induction on $n \geq 3$, using base cases $n = 3, 4, 5, 6$. The base cases are provided by entries of Table 2. Now assume all cases up to $n - 4 \geq 3$ are true. If $e = 1$ or 2, then case n is true by Corollary 5.13 because $\lfloor n/e \rfloor \geq 3$. Otherwise $e \geq 3$, and then by the inductive hypothesis there is a group H of order 2^{n-4} and exponent 2^{e-2} for which there exists a

Table 2: The largest number of rows k for which a $(G, k, 0)$ contracted difference matrix is known to exist, for each abelian 2-group G of order at most 64. An example matrix for each of these groups is given in Appendix A.

Group G	# rows k	Source	Maximum possible k?
$\mathbb{Z}_2$	1	trivial	yes (Theorem 2.2)
$\mathbb{Z}_2 \times \mathbb{Z}_2$	2	Corollary 5.13	yes (Theorem 2.1)
$\mathbb{Z}_4$	1	trivial	yes (Theorem 2.2)
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	3	Corollary 5.13	yes (Theorem 2.1)
$\mathbb{Z}_4 \times \mathbb{Z}_2$	2	Corollary 5.16	yes (computer search)
$\mathbb{Z}_8$	1	trivial	yes (Theorem 2.2)
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	4	Corollary 5.13	yes (Theorem 2.1)
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	3	computer search	yes (computer search)
$\mathbb{Z}_4 \times \mathbb{Z}_4$	2	Corollary 5.16	yes (computer search)
$\mathbb{Z}_8 \times \mathbb{Z}_2$	2	Corollary 5.16	yes (computer search)
$\mathbb{Z}_{16}$	1	trivial	yes (Theorem 2.2)
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	5	Corollary 5.13	yes (Theorem 2.1)
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	3	computer search	unknown
$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	3	computer search	unknown*
$\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	2	Corollary 5.16	unknown*
$\mathbb{Z}_8 \times \mathbb{Z}_4$	2	Corollary 5.16	unknown*
$\mathbb{Z}_{16} \times \mathbb{Z}_2$	2	Corollary 5.16	unknown*
$\mathbb{Z}_{32}$	1	trivial	yes (Theorem 2.2)
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	6	Corollary 5.13	yes (Theorem 2.1)
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$3^\dagger$	Corollary 5.13	unknown
$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$3^\dagger$	Corollary 5.13	unknown
$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$	3	Corollary 5.13	unknown
$\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	3	computer search	unknown
$\mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	$2^\dagger$	Corollary 5.16	unknown
$\mathbb{Z}_8 \times \mathbb{Z}_8$	2	Corollary 5.16	unknown
$\mathbb{Z}_{16} \times \mathbb{Z}_2 \times \mathbb{Z}_2$	2	Corollary 5.16	unknown
$\mathbb{Z}_{16} \times \mathbb{Z}_4$	2	Corollary 5.16	unknown
$\mathbb{Z}_{32} \times \mathbb{Z}_2$	2	Corollary 5.16	unknown
$\mathbb{Z}_{64}$	1	trivial	yes (Theorem 2.2)

* Known by exhaustive search to be the maximum possible k when one of the rows of the contracted difference matrix takes its lexicographically first feasible value (the 2-expansion of this row consisting of a row of only 0_G and a row containing every element of G), for example $\begin{bmatrix} 001 & 010 & 020 & 100 & 200 \end{bmatrix}$ when $G = \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$.

$\dagger$ Question 7.3 asks: can this number be increased by one?

Corollary 5.16

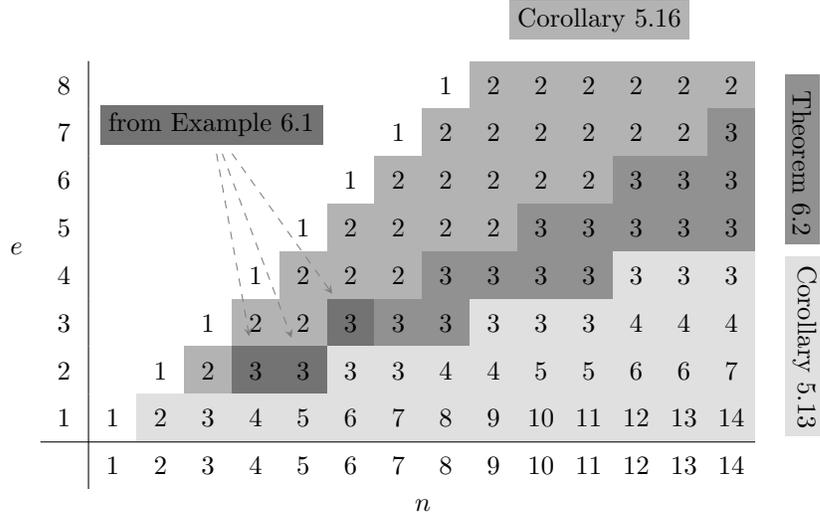| e \ n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
8								1	2	2	2	2	2	2
7							1	2	2	2	2	2	2	3
6						1	2	2	2	2	2	3	3	3
5					1	2	2	2	2	3	3	3	3	3
4				1	2	2	2	3	3	3	3	3	3	3
3			1	2	2	3	3	3	3	3	3	4	4	4
2		1	2	3	3	3	3	4	4	5	5	6	6	7
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14

from Example 6.1 — Theorem 6.2 — Corollary 5.13

Figure 1: The largest number of rows k for which a $(G, k, 0)$ contracted difference matrix is known to exist for at least one abelian group G of order 2^n and exponent 2^e.

$(H, 3, 0)$ contracted difference matrix. Take G to be an abelian group of order 2^n and exponent 2^e such that $G/H \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. By Example 6.1, there exists a $(G/H, 3, 0)$ contracted difference matrix. Apply Theorem 5.11 to produce a $(G, 3, 0)$ contracted difference matrix, proving case n and completing the induction. □

Example 6.3. *We construct a $(G, 3, 0)$ contracted difference matrix for $G = \mathbb{Z}_{16} \times \mathbb{Z}_8 \times \mathbb{Z}_4$ (whereas Corollary 5.13 gives only a $(G, 2, 0)$ contracted difference matrix). Choose $G_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ to be a subgroup of G such that $G/G_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Using the $(Z_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2, 3, 0)$ and $(Z_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, 3, 0)$ contracted difference matrices of Example 6.1 in Theorem 5.11 we then obtain the following $(G, 3, 0)$ contracted difference matrix:*

$$\begin{bmatrix} 002 & 020 & 040 & 400 & 800 & 001 & 010 & 100 & 200 \\ 042 & 002 & 822 & 020 & 400 & 010 & 201 & 001 & 100 \\ 840 & 402 & 800 & 820 & (12)40 & 211 & 100 & 201 & 210 \end{bmatrix}$$

Fig. 1 shows how the results of Theorem 6.2 improve those of Corollaries 5.13 and 5.16.

6.2 New linking systems of difference sets of size 7

Question 1 of [JLS18, Section 6] asks whether there are examples of difference matrices over 2-groups having more rows than those specified in Theorems 3.12 and 3.16. The difference matrices described in Proposition 3.23 provide such examples. By Definition 5.2, the four new $(G, 3, 0)$ contracted difference matrices described in Section 6.1 immediately give $(G, 8, 1)$ difference matrices that likewise cannot be obtained from those two theorems (giving, in particular, a second source for a $(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, 8, 1)$ difference matrix).

Moreover, we now describe how the four new contracted difference matrices of Section 6.1 can be used to construct reduced linking systems of difference sets of size 7 in certain abelian 2-groups

G of order 2^{2d+2} for which the largest previously known size was 3. To construct such a reduced linking system, it is sufficient by Theorem 4.3 for G to contain a subgroup E isomorphic to $\mathbb{Z}_2^{d+1}$ such that there is a $(G/E, 3, 0)$ contracted difference matrix. We may therefore choose H to be any group satisfying the quotient chain condition described in Section 6.1, and then choose G to be any abelian group containing a subgroup E isomorphic to $\mathbb{Z}_2^{d+1}$ such that $G/E \cong H$. It again does not seem straightforward to determine the set of all such groups G explicitly (in the absence of an explicit condition for all suitable groups H), but we can show the existence of a large set of such groups G.

Corollary 6.4. *Let $d \geq 2$ and let e be an integer satisfying $2 \leq e \leq \frac{d+3}{2}$. Then there is at least one abelian group G of order 2^{2d+2}, rank $d+1$, and exponent 2^e, such that there is a reduced linking system of (v, k, λ, n)-difference sets in G of size 7, with (v, k, λ, n) as given in (4).*

Proof. Applying Theorem 6.2 with $n = d+1$ and e replaced by $e-1$, there is at least one abelian group H of order 2^{d+1} and exponent 2^{e-1} for which there exists an $(H, 3, 0)$ contracted difference matrix and therefore an $(H, 8, 1)$ difference matrix. Since H has rank at most $d+1$, there is therefore a group G of order 2^{2d+2}, rank $d+1$, and exponent 2^e, containing a subgroup $E \cong \mathbb{Z}_2^{d+1}$ such that $G/E \cong H$. The result then follows from Theorem 4.3. $\qquad\square$

The reduced linking systems of difference sets given by Theorem 4.5 (i) all have size 3, and those given by Theorem 4.5 (ii) (under the stated condition $2 \leq e \leq \frac{d+3}{2}$) have size 3 when $\frac{d+1}{e-1} < 3$. Corollary 6.4 therefore provides reduced linking systems of difference sets, that are larger than those previously known, for all $d \geq 2$ and all e satisfying $\frac{d+4}{3} < e \leq \frac{d+3}{2}$.

Example 6.5. *The largest known size of a reduced linking system of $(256, 120, 56, 64)$-difference sets in an abelian group of order 256 and exponent 8 was given as 3 in [JLS18, Table 3]. Using the above procedure, we can increase this size to 7 for each of the groups*

$$\mathbb{Z}_8 \times \mathbb{Z}_2^5, \quad \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2^3, \quad \mathbb{Z}_8 \times \mathbb{Z}_4^2 \times \mathbb{Z}_2$$

(but not for the group $\mathbb{Z}_8^2 \times \mathbb{Z}_2^2$) by choosing a subgroup E isomorphic to $\mathbb{Z}_2^4$ such that $G/E \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, and using the $(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, 3, 0)$ contracted difference matrix of Example 6.1 to provide a $(\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, 8, 1)$ difference matrix for use in Theorem 4.3.

We remark that additional reduced linking systems of difference sets of size 7 can be obtained by applying the composition construction of Theorem 3.8 to the $(Z_4 \times \mathbb{Z}_4, 8, 1)$ difference matrix of Proposition 3.23 (ii) to produce a further infinite family of difference matrices with 8 rows in abelian 2-groups. This infinite family does not arise from the analogous construction for contracted difference matrices, because there is no $(\mathbb{Z}_4 \times \mathbb{Z}_4, 3, 0)$ contracted difference matrix (see Table 2).

7 Open Questions

We conclude with three open questions.

The first question concerns how effective the concept of a contracted difference matrix is in explaining the existence pattern of difference matrices in abelian p-groups. It is motivated by comparing the results of Proposition 3.1, Theorem 3.12, Theorem 3.16 for difference matrices with those of Proposition 5.6, Corollary 5.13, Corollary 5.16, respectively, for contracted difference matrices.

Question 7.1. *For which primes p, abelian p-groups G, and integers $k \geq 1$ does there exist a $(G, p^k, 1)$ difference matrix but not a $(G, k, 0)$ contracted difference matrix?*

The only example currently known that satisfies the conditions of Question 7.1 is given by $p = 2$ and $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ and $k = 3$, from Proposition 3.23 (ii) and the exhaustive search result for $\mathbb{Z}_4 \times \mathbb{Z}_4$ in Table 2.

The second question concerns the largest number of rows of a difference matrix over an abelian p-group.

Question 7.2. *For which primes p and abelian p-groups G is the largest integer m for which a $(G, m, 1)$ difference matrix exists not a power of p?*

The only example currently known that satisfies the conditions of Question 7.2 is given by $p = 2$ and $G = \mathbb{Z}_8 \times \mathbb{Z}_2$ and $m = 5$, from Proposition 3.23 (i). We also know that $p = 3$ and $G = \mathbb{Z}_9 \times \mathbb{Z}_3$ and $k = 2$ satisfy the conditions of at least one of Questions 7.1 and 7.2: by Theorem 3.17 there exists a $(\mathbb{Z}_9 \times \mathbb{Z}_3, 4, 1)$ difference matrix, but exhaustive search shows there is no $(\mathbb{Z}_9 \times \mathbb{Z}_3, 2, 0)$ contracted difference matrix.

The third question follows from the observation that the currently known existence pattern for contracted difference matrices over 2-groups of fixed order, as illustrated in Table 2, appears to favor groups of smaller exponent and larger rank.

Question 7.3. *Let G be an abelian group of order 2^n, exponent at most $2^{\frac{n}{r-1}}$, and rank at least r. Does there exist a $(G, r, 0)$ contracted difference matrix?*

A positive answer to Question 7.3 for the case $r = 2$ is given by Corollary 5.16; and a positive answer for the case $r = 3$ would allow the words "for at least one abelian group" in Theorem 6.2 to be replaced by "for all abelian groups", provided that a minimum rank of 3 is specified.

Acknowledgements

References

[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.

[CK96]   C.J. Colbourn and D.L. Kreher. Concerning difference matrices. *Des. Codes Cryptogr.*, 9:61–70, 1996.

[CK07]   R. Craigen and H. Kharaghani. Hadamard matrices and Hadamard designs. In C.J. Colbourn and J.H. Dinitz, editors, *Handbook of Combinatorial Designs*, pages 273–280. Chapman & Hall/CRC, Boca Raton, 2nd edition, 2007.

[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.

[Dam99]   E.R. van Dam. Three-class association schemes. *J. Algebraic Combin.*, 10:69–107, 1999.

[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.

[Dra79]   D.A. Drake. Partial λ-geometries and generalized Hadamard matrices over groups. *Canad. J. Math.*, 31:617–627, 1979.

[Eva07]   A.B. Evans. On orthogonal orthomorphisms of cyclic and nonabelian groups. II. *J. Combin. Des.*, 15:195–209, 2007.

[Ge05]   G. Ge. On $(g, 4; 1)$-difference matrices. *Discrete Math.*, 301:164–174, 2005.

[Hor06]   K.J. Horadam. *Hadamard matrices and their applications*. Princeton University Press, Princeton and Oxford, 2006.

[HP55]   M. Hall and L.J. Paige. Complete mappings of finite groups. *Pacific J. Math.*, 5:541–549, 1955.

[JLS18]   J. Jedwab, S. Li, and S. Simon. Linking systems of difference sets. `arXiv:1708.04405v2 [math.CO]`, April 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.

[Jun79]   D. Jungnickel. On difference matrices, resolvable transversal designs and generalized Hadamard matrices. *Math. Z.*, 167:49–60, 1979.

[Jun80]   D. Jungnickel. On difference matrices and regular Latin squares. *Abh. Math. Sem. Hamburg*, 50:219–231, 1980.

[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.

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

[Lau86]   W. de Launey. A survey of generalized Hadamard matrices and difference matrices $d(k, \lambda; g)$ with large k. *Utilitas Math.*, 30:5–29, 1986.

[Lau87]   W. de Launey. On difference matrices, transversal designs, resolvable transveral designs and large sets of mutually orthogonal f-squares. *J. Stat. Plann. Infer.*, 16:107–125, 1987.

[Lau07]   W. de Launey. Generalized Hadamard matrices. In C.J. Colbourn and J.H. Dinitz, editors, *Handbook of Combinatorial Designs*, pages 301–306. Chapman & Hall/CRC, Boca Raton, 2nd edition, 2007.

[LT04]   F. Lazebnik and A. Thomason. Orthomorphisms and the construction of projective planes. *Math. Comp.*, 73:1547–1557, 2004.

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

[Shr64]   S.S. Shrikhande. Generalized Hadamard matrices and orthogonal arrays of strength two. *Canad. J, Math*, 16:736–740, 1964.

Appendix A   Contracted difference matrix examples

This appendix gives an example $(G, k, 0)$ contracted difference matrix containing the largest known number of rows k (as stated in Table 2), for each abelian 2-group G of order at most 64.

Group	Matrix
$\mathbb{Z}_2$	$\begin{bmatrix} 1 \end{bmatrix}$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\begin{bmatrix} 01 & 10 \\ 10 & 11 \end{bmatrix}$
$\mathbb{Z}_4$	$\begin{bmatrix} 1 & 2 \end{bmatrix}$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\begin{bmatrix} 001 & 010 & 100 \\ 010 & 100 & 011 \\ 100 & 011 & 110 \end{bmatrix}$
$\mathbb{Z}_4 \times \mathbb{Z}_2$	$\begin{bmatrix} 01 & 10 & 20 \\ 21 & 01 & 10 \end{bmatrix}$
$\mathbb{Z}_8$	$\begin{bmatrix} 1 & 2 & 4 \end{bmatrix}$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\begin{bmatrix} 0001 & 0010 & 0100 & 1000 \\ 0010 & 0100 & 1000 & 0011 \\ 0100 & 1000 & 0011 & 0110 \\ 1000 & 0011 & 0110 & 1100 \end{bmatrix}$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\begin{bmatrix} 001 & 010 & 100 & 200 \\ 010 & 201 & 001 & 100 \\ 211 & 100 & 201 & 210 \end{bmatrix}$
$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\begin{bmatrix} 01 & 10 & 02 & 20 \\ 10 & 11 & 20 & 22 \end{bmatrix}$
$\mathbb{Z}_8 \times \mathbb{Z}_2$	$\begin{bmatrix} 01 & 10 & 20 & 40 \\ 41 & 01 & 10 & 20 \end{bmatrix}$
$\mathbb{Z}_{16}$	$\begin{bmatrix} 1 & 2 & 4 & 8 \end{bmatrix}$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\begin{bmatrix} 00001 & 00010 & 00100 & 01000 & 10000 \\ 00010 & 00100 & 01000 & 10000 & 00101 \\ 00100 & 01000 & 10000 & 00101 & 01010 \\ 01000 & 10000 & 00101 & 01010 & 10100 \\ 10000 & 00101 & 01010 & 10100 & 01101 \end{bmatrix}$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\begin{bmatrix} 0001 & 0010 & 0100 & 1000 & 2000 \\ 0010 & 0100 & 2001 & 0001 & 1000 \\ 1001 & 2110 & 0001 & 0010 & 0101 \end{bmatrix}$

$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	$\begin{bmatrix} 001 & 010 & 020 & 100 & 200 \\ 021 & 001 & 211 & 010 & 100 \\ 220 & 101 & 200 & 210 & 320 \end{bmatrix}$
$\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\begin{bmatrix} 010 & 100 & 200 & 001 & 400 \\ 210 & 010 & 100 & 400 & 401 \end{bmatrix}$
$\mathbb{Z}_8 \times \mathbb{Z}_4$	$\begin{bmatrix} 01 & 10 & 20 & 02 & 40 \\ 21 & 01 & 10 & 40 & 42 \end{bmatrix}$
$\mathbb{Z}_{16} \times \mathbb{Z}_2$	$\begin{bmatrix} 01 & 10 & 20 & 40 & 80 \\ 81 & 01 & 10 & 20 & 40 \end{bmatrix}$
$\mathbb{Z}_{32}$	$\begin{bmatrix} 1 & 2 & 4 & 8 & (16) \end{bmatrix}$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\begin{bmatrix} 000001 & 000010 & 000100 & 001000 & 010000 & 100000 \\ 000010 & 000100 & 001000 & 010000 & 100000 & 000011 \\ 000100 & 001000 & 010000 & 100000 & 000011 & 000110 \\ 001000 & 010000 & 100000 & 000011 & 000110 & 001100 \\ 010000 & 100000 & 000011 & 000110 & 001100 & 011000 \\ 100000 & 000011 & 000110 & 001100 & 011000 & 110000 \end{bmatrix}$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\begin{bmatrix} 00100 & 01000 & 20000 & 00001 & 00010 & 10000 \\ 01000 & 20000 & 01100 & 00010 & 10000 & 00011 \\ 20000 & 01100 & 21000 & 10000 & 00011 & 10010 \end{bmatrix}$
$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\begin{bmatrix} 0010 & 0200 & 2000 & 0001 & 0100 & 1000 \\ 0200 & 2000 & 0210 & 0100 & 1000 & 0101 \\ 2000 & 0210 & 2200 & 1000 & 0101 & 1100 \end{bmatrix}$
$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$	$\begin{bmatrix} 002 & 020 & 200 & 001 & 010 & 100 \\ 020 & 200 & 022 & 010 & 100 & 011 \\ 200 & 022 & 220 & 100 & 011 & 110 \end{bmatrix}$
$\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\begin{bmatrix} 4101 & 2000 & 1100 & 0010 & 7111 & 0101 \\ 4010 & 0111 & 2011 & 4001 & 7001 & 0001 \\ 4000 & 7110 & 5100 & 0011 & 5010 & 2011 \end{bmatrix}$
$\mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	$\begin{bmatrix} 020 & 400 & 010 & 200 & 001 & 100 \\ 400 & 420 & 200 & 210 & 100 & 101 \end{bmatrix}$
$\mathbb{Z}_8 \times \mathbb{Z}_8$	$\begin{bmatrix} 04 & 40 & 02 & 20 & 01 & 10 \\ 40 & 44 & 20 & 22 & 10 & 11 \end{bmatrix}$
$\mathbb{Z}_{16} \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\begin{bmatrix} 010 & 800 & 001 & 100 & 200 & 400 \\ 800 & 810 & 401 & 001 & 100 & 200 \end{bmatrix}$
$\mathbb{Z}_{16} \times \mathbb{Z}_4$	$\begin{bmatrix} 02 & 80 & 01 & 10 & 20 & 40 \\ 80 & 82 & 41 & 01 & 10 & 20 \end{bmatrix}$
$\mathbb{Z}_{32} \times \mathbb{Z}_2$	$\begin{bmatrix} 01 & 10 & 20 & 40 & 80 & (16)0 \\ (16)1 & 01 & 10 & 20 & 40 & 80 \end{bmatrix}$
$\mathbb{Z}_{64}$	$\begin{bmatrix} 1 & 2 & 4 & 8 & (16) & (32) \end{bmatrix}$