Sets of Mutually Quasi-Orthogonal Latin Squares

David Bedford, Roger M. Whitaker

Department of Mathematics
Keele University
Keele, Staffordshire, ST5 5BG, U.K.

Abstract

In this paper we are concerned with the existence of sets of mutually quasi-orthogonal latin squares (MQOLS). We establish a correspondence between equidistant permutation arrays and MQOLS which has facilitated a computer search to identify all sets of MQOLS of order ≤ 6. In particular we report that the maximum number of latin squares of order 6 in a mutually quasi-orthogonal set is 3, and give an example of such a set. We also report on a non-exhaustive computer search for sets of 3 MQOLS of order 10, which whilst not identifying such a set, has led to the identification of all the resolutions of each $(10, 3, 2)$-balanced incomplete block design. Improvements are given on the existence results for MQOLS based on groups, and a new construction is given for sets of MQOLS based on groups from sets of mutually orthogonal latin squares based on groups. We show that this construction yields sets of $2^n - 1$ MQOLS of order 2^n, based on two infinite classes of group. Finally we give a new construction for difference matrices from mutually quasi-orthogonal quasi-orthomorphisms, and use this to construct a $(2^n, 2^n; 2)$-difference matrix over $C_2^{n-2} \times C_4$.

1 Introduction

A latin square of order n is an $n \times n$ array defined on a symbol set S with every element of S occuring precisely once in each row and precisely once in each column. Two latin squares of order n are said to be orthogonal if, when superimposed so as to form an array of ordered pairs Λ, each of the n^2 possible ordered pairs occurs precisely once in Λ. In [1], Bedford

JCMCC 33 (2000), pp. 299-310

generalised this well known concept (also see [11]). Two latin squares are said to be *quasi-orthogonal* if, when superimposed so as to form an array of unordered pairs Λ^*, each unordered pair of the form $\{x, x\}$ occurs precisely once whilst unordered pairs of distinct symbols occur precisely twice in Λ^*. Although first explicitly introduced in [1], quasi-orthogonal latin squares are related to many well established designs including Room squares, r-orthogonal latin squares, Steiner triple systems, and starters and adders. For a detailed discussion of these relationships, see [15].

In [1] emphasis was given to the problem of constructing pairs of quasi-orthogonal latin squares based on groups, that is where each latin square in a given quasi-orthogonal pair can be bordered so as to form the Cayley table of some finite group. In this paper we concern ourselves with the more general question of the existence of sets of mutually quasi-orthogonal latin squares (MQOLS). We present a method of exhaustive computer search to identify all sets of MQOLS of order n by establishing a correspondence between MQOLS and equidistant permutation arrays. This search is carried out for $n \leq 6$. Given the non-existence of a pair of orthogonal latin squares of order 6, we observe with interest the existence of sets of 3 MQOLS of order 6. We also present details of a computer search for a resolvable $(10, 3, 2)$-balanced incomplete block design with certain properties (defined in section 3) sufficent for the existence of 3 MQOLS of order 10. In fact this search was originally started in [10] by Keedwell, and although we find that there is no such design, we report the classification of all resolutions of each $(10, 3, 2)$-balanced incomplete block design.

For larger n, we restrict our attention to sets of MQOLS of order n based on groups. We extend existence results for mutually quasi-orthogonal quasi-orthomorphisms due to Jungnickel [9], Bedford [1] and Quinn [13]. We also give a construction for sets of MQOLS from sets of mutually orthogonal latin squares (MOLS), and show that it is successful in establishing sets of $2^n - 1$ mutually quasi-orthogonal latin squares of order 2^n based on the groups $C_2^{n-2} \times C_4$ and $C_2^{n-3} \times Q_4$ (no known sets of MOLS of this size are based on these groups). Finally we give a related construction for maximal $(2^n, 2^n; 2)$-difference matrices over the group $C_2^{n-2} \times C_4$.

We know that there are at most $n-1$ MOLS of order n and that this bound is achieved when n is a prime or prime power. It is natural to ask the same question for MQOLS, but unfortunately, no simple answer has been found. Currently, the best known bound is given by the maximal size of an EPA (defined below), and is of the form $n^2 - 4n - \sqrt{2n} + O(1)$, for $n \geq 6$: see [12].

2 A search for MQOLS of order ≤ 6

An exhaustive computer search for maximal sets of MQOLS of order ≤ 6 has been performed. Central to this search was the idea of an equidistant permutation array.

Definition 1 *An equidistant permutation array (EPA) of index 1 is a $k \times n$ array such that each row is a permutation of a symbol set S, of size n, and any two rows agree in precisely 1 place.*

Consider a set $\{A_1, \ldots, A_n\}$ of $k \times n$ EPAs and let R_{ij} denote the i^{th} row of A_j. We define $M(R_{\alpha\beta}, R_{\gamma\delta})$ to be the number of places in which $R_{\alpha\beta}$ and $R_{\gamma\delta}$ match. If for all $s \neq t$, the set $\{A_1, \ldots, A_n\}$ satisfies $M(R_{is}, R_{it}) = 0$ for all i, then they are equivalent to the existence of a set $\{L_1, \ldots, L_k\}$ of latin squares of order n with the property that when two squares from the set are superimposed so as to form an array of ordered pairs, each ordered pair of the form (x, x) occurs exactly once. This correspondence is established by the relation $(i, c, r) \in A_s \Leftrightarrow (r, c, s) \in L_i$, where $(x, y, z) \in \Gamma$ denotes the fact that the element z occurs as the $(x, y)^{th}$ entry of the array Γ.

The latin squares are mutually orthogonal if and only if the EPAs have the further property that for $\alpha \neq \beta$ and $\gamma \neq \delta$ $M(R_{\alpha\gamma}, R_{\beta\delta}) = 1$. Similarly the latin squares are mutually quasi-orthogonal if and only if for $\alpha \neq \beta$ and $\gamma \neq \delta$, $M(R_{\alpha\gamma}, R_{\beta\delta}) + M(R_{\alpha\delta}, R_{\beta\gamma}) = 2$.

The above equivalence provides an efficient way of constructing MQOLS by first finding EPAs of the desired type. Consider constructing a set of k MQOLS of order n. We need to identify kn^2 suitable entries for the cells of k, $n \times n$ arrays. If we search for EPAs corresponding to MQOLS, acceptance of a permutation as a row of an EPA is equivalent to locating the n cells of a latin square which will contain a given element. For small n, permutations which form candidates for rows of the EPAs are easily generated. Using this approach, an exhaustive computer search was carried out for maximal sets of MQOLS up to order 6. Restricting attention to maximal sets of MQOLS which are not MOLS we found 3 MQOLS based on Z_4 as reported in [1], 2 MQOLS using the non-cyclic square of order 5, pairs of MQOLS of order 6 and also several triples, a representative of which is reproduced below along with the corresponding EPAs. The search established that for these orders, no larger sets of MQOLS exist.

A_0						A_1						A_2					
0	1	2	3	5	4	1	0	5	4	2	3	2	3	0	5	4	1
1	2	5	0	3	4	3	0	1	5	4	2	5	4	2	3	0	1
1	3	0	4	5	2	2	0	4	1	3	5	5	2	1	0	4	3

A_3						A_4						A_5					
3	2	4	0	1	5	4	5	3	1	0	2	5	4	1	2	3	0
4	3	0	1	2	5	2	1	3	4	5	0	0	5	4	2	1	3
4	5	2	3	1	0	0	4	3	5	2	1	3	1	5	2	0	4

0	1	2	3	4	5
1	0	5	4	3	2
2	3	0	5	1	4
3	2	4	0	5	1
4	5	3	1	2	0
5	4	1	2	0	3

5	1	3	0	2	4
0	4	1	3	5	2
4	0	2	5	3	1
1	3	4	2	0	5
3	2	5	4	1	0
2	5	0	1	4	3

4	1	0	2	5	3
0	5	2	1	3	4
1	2	3	5	4	0
5	0	4	3	1	2
3	4	1	0	2	5
2	3	5	4	0	1

3 Triples of MQOLS of order 10

Although pairs of orthogonal latin squares of order 10 are known to exist no triple has yet been found. In [10], Keedwell performed a non-exhaustive search for 3 MOLS of order 10 using balanced incomplete block designs (BIBDs). In particular, a (10, 3, 2)-BIBD is *resolvable* if its 30 blocks can be partitioned into 10 sets each containing 3 pairwise disjoint blocks. Such a partition of blocks is called a resolution with each set of blocks called a *parallel class*. Keedwell called a resolution of a (10, 3, 2)-BIBD of *latin square type* if there exists a 10×10 latin square $L = (l_{ij})$ such that $\{\{l_{i1}, l_{i2}, l_{i3}\}, \{l_{i4}, l_{i5}, l_{i6}\}, \{l_{i7}, l_{i8}, l_{i9}\}\}$, $i = 0, \ldots, 9$ are the parallel classes of the design. Keedwell required additional properties for his search, we however have the following theorem.

Theorem 1 *If there exists a latin square type resolution of a* (10, 3, 2)*-BIBD then there exists 3 MQOLS of order 10.*

Proof: Let L_0 be the latin square from which the latin square type resolution is obtained, and label the columns of L_0: $c_0, c_1, \ldots, c_9$. We cycle the columns of L_0, in the following fashion to obtain L_1, L_2 such that L_0, L_1, L_2

are MQOLS.

$$\begin{array}{ll} L_0: & c_0,\ c_1, c_2, c_3,\ c_4, c_5, c_6,\ c_7, c_8, c_9 \\ L_1: & c_0,\ c_3, c_1, c_2,\ c_6, c_4, c_5,\ c_9, c_7, c_8 \\ L_2: & c_0,\ c_2, c_3, c_1,\ c_5, c_6, c_4,\ c_8, c_9, c_7. \end{array}$$

Consider the superimposition of L_i and L_j into an array of unordered pairs Λ. Then all pairs of the form $\{x, x\}$ occur in the 0^{th} column of Λ and nowhere else. Now consider pairs $\{x, y\}$, $x \neq y$. Such a pair will occur in Λ if and only if x, y occur together in a block of the BIBD. As x, y occur together in precisely 2 blocks of the BIBD, $\{x, y\}$ occurs twice in Λ. □

In [3, 4, 5, 6] a complete census of the 960 $(10,3,2)$-BIBDs was given, as was partial information on the number of resolutions of these designs. As part of our search we have compiled a full catalogue of these resolutions [14], and found, surprisingly, that not one of these resolutions was of latin square type. This implies that neither 3 MQOLS nor 3 MOLS of order 10 can be constructed in this way.

4 Existence results for MQOLS based on groups

By generalising the concept of a complete mapping as defined in [8], Bedford [1] showed that a *quasi-complete mapping* defined on the elements of a finite group G is sufficient for the existence of a pair of MQOLS based on G. We reiterate the main ideas used in [1], and given in [11]. A useful concept is that of a *quasi-ordering* of a group G of order n, being a list of n elements of G with the following properties:

- every element in G of period 2 occurs precisely once in the list, as does the identity;
- for every non-identity element $x \in G$ not of period 2, both x and x^{-1} occur precisely once in the list, or x occurs precisely twice with x^{-1} absent, or x^{-1} occurs precisely twice whilst x is absent.

Definition 2 *Let the mapping $\theta : G \to G$ be such that $\theta(g_1), \theta(g_2), \ldots, \theta(g_n)$ is a quasi-ordering of G. Define $\phi : g_i \mapsto g_i\theta(g_i)$. If ϕ is a permutation on G then θ is quasi-complete.*

In the preceding definition, ϕ is referred to as the *quasi-orthomorphism* associated with θ. Note that if θ is a permutation on G then θ is a complete mapping and ϕ is an orthomorphism. By letting L denote the Cayley table of G and L_ϕ denote the resultant latin square after the columns of L have been permuted according to ϕ, then L and L_ϕ are quasi-orthogonal.

Definition 3 *Two permutations ϕ_1, ϕ_2 of G are quasi-orthogonal if*

$$\phi_1(g_1)^{-1}\phi_2(g_1), \ldots, \phi_1(g_n)^{-1}\phi_2(g_n)$$

is a quasi-ordering of G.

The above definition allows for sets of MQOLS to be obtained from the Cayley tables of a finite group, as was shown by the following theorem.

Theorem 2 *Let ϕ_1, ϕ_2 be quasi-orthogonal quasi-orthomorphisms of G, let L be the Cayley table of G with L_{ϕ_1}, L_{ϕ_2} denoting the latin squares obtained from permuting the columns of L according to ϕ_1 and ϕ_2 respectively. Then L_{ϕ_1} and L_{ϕ_2} are quasi-orthogonal.*

Proof: see [1].

Jungnickel [9] gave a weak lower bound on the number of MOLS of a given order. Letting G and H be finite groups, Jungnickel showed that if G admits r mutually orthogonal complete mappings, and H possesses s mutually orthogonal complete mappings, then $G \times H$ possesses at least $\min\{r, s\}$ mutually orthogonal complete mappings. This result provides the best known lower bound on the number of MOLS of order n for many large values of n. Similarly, Jungnickel's result generalises to MQOLS to give a weak lower bound on the size of a maximal set of MQOLS possessed by a group.

We may construct a mapping of $G \times H$, say θ^*, from a quasi-complete mapping θ of G and a complete mapping θ' of H by defining $\theta^* : G \times H \rightarrow G \times H$ by:

$$\theta^*(g, h) = (\theta(g), \theta'(h)), \forall (g, h) \in G \times H.$$

The elements of $\{\theta^*(g, h) : g \in G, h \in H\}$ form a quasi-ordering of $G \times H$ and $\phi^* : (g, h) \mapsto (g, h) \times \theta^*(g, h)$ is a permutation on $G \times H$ since $\phi : g \mapsto g\theta(g)$ is a permutation on G and $\phi' : h \mapsto h\theta'(h)$ is a permutation on H, so ϕ^* is a quasi-orthomorphism of $G \times H$.

Theorem 3 *Let $\{\phi_1, \ldots, \phi_r\}$ be a set of mutually quasi-orthogonal quasi-orthomorphisms of G and let $\{\phi'_1, \ldots, \phi'_s\}$ be a set of mutually orthogonal orthomorphisms of H. Then $G \times H$ possesses a set X, of mutually quasi-orthogonal quasi-orthomorphisms, where $|X| = min\{r, s\}$.*

Proof: Let $X = \{\phi_1^*, \ldots, \phi_{min\{r,s\}}^*\}$ where $\phi_i^*(g,h) = (\phi_i(g), \phi_i'(h)), 1 \leq i \leq min\{r,s\}$. Then X is a set of quasi-orthomorphisms of $G \times H$. It remains to be checked that for $i \neq j$, $\phi_i^*, \phi_j^* \in X$ are quasi-orthogonal. This is so since;

$$\begin{aligned} \{\theta_i^*(x)^{-1}\theta_j^*(x) : x \in G \times H\} &= \{(\theta_i(g)^{-1}\theta_j(g), \theta_i'(h)^{-1}\theta_j'(h)) : g \in G, h \in H\} \\ &= \{(g,h) : g \in Q, h \in H\} \end{aligned}$$

where Q forms a quasi-ordering of G. Such a set forms a quasi-ordering of $G \times H$. □

Hall and Paige [7] showed that for finite groups K and H, where H is a normal subgroup of K, if there exists a complete mapping of H and a complete mapping of K/H, then there exists a complete mapping of K. In [1], Bedford extended this result to quasi-complete mappings whilst in [13] Quinn extended this result to sets of orthogonal complete mappings. In the following theorem, we state, without proof, the analogous extension to sets of mutually quasi-orthogonal, quasi-complete mappings.

Theorem 4 *If there exist r mutually orthogonal complete mappings of H and there exist r mutually quasi-orthogonal quasi-complete mappings of K/H, then there exist at least r mutually quasi-orthogonal, quasi-complete mappings of K.*

We note that although theorem 3 follows from theorem 4 on setting $K = G \times H$, the proof of theorem 3 provides a more useful direct construction.

5 MQOLS from MOLS

In this section we present a construction for MQOLS based on groups from MOLS based on groups. Our approach is to take mutually orthogonal orthomorphisms of a group G and from these, construct mutually quasi-orthogonal quasi-orthomorphisms of a group G'. First we need the following result, in which we denote the inverse of an element g in the group G_i by $INV_{G_i}[g]$.

Lemma 1 *Let $G_1 = (G, \cdot)$ and $G_2 = (G, \circ)$ be finite groups with identity element e. If $\forall g \in G$, $g \cdot g \neq e \Rightarrow INV_{G_1}[g] = INV_{G_2}[g]$ then a quasi-ordering of G_1 is a quasi-ordering of G_2.*

Proof: Let Q be a quasi-ordering of G_1 and let g be an element of Q not of period 2 in G_1. Since $INV_{G_1}[g] = INV_{G_2}[g]$, g is not of period

2 in G_2 and so the occurrences of such elements do not prohibit Q from being a quasi-ordering of G_2. Now let g be an element in Q which is of period 2 in G_1. We need to show that if g does not have period 2 in G_2, then $INV_{G_2}[g]$ occurs only once in Q. This is necessarily the case since $INV_{G_2}[g]$ has period 2 in G_1. To see this assume to the contrary that $INV_{G_2}[g]$ is not of period 2 in G_1, i.e. $INV_{G_2}[g] \cdot INV_{G_2}[g] \neq e$, and so $INV_{G_1}[INV_{G_2}[g]] = INV_{G_2}[INV_{G_2}[g]] = g$ (†). Then:

$$\begin{aligned} INV_{G_2}[g] \cdot INV_{G_2}[g] &\neq e \\ \Rightarrow INV_{G_1}[INV_{G_2}[g] \cdot INV_{G_2}[g]] &\neq e \\ \Rightarrow INV_{G_1}[INV_{G_2}[g]] \cdot INV_{G_1}[INV_{G_2}[g]] &\neq e \\ \Rightarrow g \cdot g &\neq e \text{ (by (†))} \end{aligned}$$

- a contradiction since g has period 2 in G_1. □

Definition 4 *(Compliancy) Let $G_1 = (G, \cdot), G_2 = (G, \circ)$ be finite groups. If the following conditions are satisfied then G_1 is said to be compliant to G_2.*

1. $\forall g \in G,\ g \cdot g \neq e \Rightarrow INV_{G_1}[g] = INV_{G_2}[g]$
2. *All $x, y \in G$ satisfy at least one of the following identities:*

$$\begin{aligned} INV_{G_1}[x] \cdot y &= INV_{G_2}[x] \circ y \\ INV_{G_1}[INV_{G_1}[x] \cdot y] &= INV_{G_2}[x] \circ y \\ INV_{G_2}[INV_{G_1}[x] \cdot y] &= INV_{G_2}[x] \circ y \\ INV_{G_2}[INV_{G_1}[INV_{G_1}[x] \cdot y]] &= INV_{G_2}[x] \circ y. \end{aligned}$$

The motivation for the above definition is that if G_1 is compliant to G_2, then a quasi-orthomorphism of G_1 is a quasi-orthomorphism of G_2. To see this, let ϕ be a quasi-orthomorphism of G_1 so that the list $INV_{G_1}[g_1] \cdot \phi(g_1), \ldots, INV_{G_1}[g_n] \cdot \phi(g_n)$ is a quasi-ordering of G_1 and hence by lemma 1, is also a quasi-ordering of G_2. We are required to show that $INV_{G_2}[g_1] \circ \phi(g_1), \ldots, INV_{G_2}[g_n] \circ \phi(g_n)$ is a quasi-ordering of G_2. This follows by virtue of the second condition of compliancy and the fact that if we replace an element of a quasi-ordering by its inverse in that group then the resultant list is still a quasi-ordering of the group. Furthermore, this result extends in a natural way to give the following.

Theorem 5 *Let G_1 and G_2 be groups with G_1 compliant to G_2. If G_1 admits a set M of mutually quasi-orthogonal quasi-orthomorphisms, then M is also such a set for G_2.*

Before giving some examples of compliant groups we present a recursive construction which allows us to construct infinite classes of compliant groups from particular examples.

Theorem 6 *Let $G_1 = (G, \cdot)$ and $G_2 = (G, \circ)$ be groups with G_1 compliant to G_2. Then $C_2 \times G_1 = (C_2 \times G, \cdot)$ is compliant to $C_2 \times G_2 = (C_2 \times G, \circ)$.*

Proof: Firstly note that if $(x, g)^2 \neq e$ in $C_2 \times G_1$ then we have $g \cdot g \neq e$ and hence $INV_{G_1}[g] = INV_{G_2}[g]$. It follows that $INV_{C_2 \times G_1}[(x, g)] = (x, INV_{G_1}[g]) = (x, INV_{G_2}[g]) = INV_{C_2 \times G_2}[(x, g)]$.

Now suppose $INV_{G_1}[g_1] \cdot g_2 = INV_{G_2}[g_1] \circ g_2$ then

$$\begin{aligned} INV_{C_2 \times G_1}[(x_1, g_1)] \cdot (x_2, g_2) &= (x_1, INV_{G_1}[g_1]) \cdot (x_2, g_2) \\ &= (x_1 x_2, INV_{G_1}[g_1] \cdot g_2) \\ &= (x_1 x_2, INV_{G_2}[g_1] \circ g_2) \\ &= (x_1, INV_{G_2}[g_1]) \circ (x_2, g_2) \\ &= INV_{C_2 \times G_2}[(x_1, g_1)] \circ (x_2, g_2). \end{aligned}$$

Similarly

$$\begin{aligned} INV_{G_1}[INV_{G_1}[g_1] \cdot g_2] &= INV_{G_2}[g_1] \circ g_2 \\ \Rightarrow INV_{C_2 \times G_1}[INV_{C_2 \times G_1}[(x_1, g_1)] \cdot (x_2, g_2)] &= INV_{C_2 \times G_2}[(x_1, g_1)] \circ (x_2, g_2) \end{aligned}$$

and:

$$\begin{aligned} INV_{G_2}[INV_{G_1}[g_1] \cdot g_2] &= INV_{G_2}[g_1] \circ g_2 \\ \Rightarrow INV_{C_2 \times G_2}[INV_{C_2 \times G_1}[(x_1, g_1)] \cdot (x_2, g_2)] &= INV_{C_2 \times G_2}[(x_1, g_1)] \circ (x_2, g_2) \end{aligned}$$

and:

$$\begin{aligned} INV_{G_2}[INV_{G_1}[INV_{G_1}[g_1] \cdot g_2]] &= INV_{G_2}[g_1] \circ g_2 \\ \Rightarrow INV_{C_2 \times G_2}[INV_{C_2 \times G_1}[INV_{C_2 \times G_1}[(x_1, g_1)] \cdot (x_2, g_2)]] & \\ &= INV_{C_2 \times G_2}[(x_1, g_1)] \circ (x_2, g_2). \square \end{aligned}$$

We now give some examples of compliant groups. In Figure 1 we document all pairs of compliant groups of order n, for each $n \leq 14$. H_1 and H_2 occur in the columns headed G_1 and G_2 respectively if and only if H_1 is compliant to H_2. Many of the entries in Figure 1 are special cases of more general results. D_{2n} is compliant to Q_{2n} and D_n is compliant to $C_2 \times C_n$, where:

$$\begin{aligned} D_n &= \langle a, b : a^n = e, b^2 = e, ab = ba^{-1} \rangle \\ C_2 \times C_n &= \langle a, b : a^n = e, b^2 = e, ab = ba \rangle \\ Q_{2n} &= \langle a, b : a^{2n} = e, b^2 = a^n, ab = ba^{-1} \rangle. \end{aligned}$$

n	G_1	G_2
4	$C_2 \times C_2$	C_4
6	D_3	$C_2 \times C_3$
8	$C_2 \times C_2 \times C_2$	$C_2 \times C_4$
	$C_2 \times C_2 \times C_2$	Q_4
	$C_2 \times C_4$	Q_4
	D_4	$C_2 \times C_4$
	D_4	Q_4
10	D_5	C_{10}
12	D_6	Q_6
14	D_7	C_{14}

Figure 1:

Also, it follows from theorem 6 that C_2^n is compliant to $C_2^{n-2} \times C_4$ and that $C_2^{n-2} \times C_4$ is compliant to $C_2^{n-3} \times Q_4$ (where C_2^n denotes the group $C_2 \times \cdots \times C_2$ of order 2^n). It is well known that there exists $2^n - 2$ mutually orthogonal orthomorphisms of C_2^n, and therefore $2^n - 1$ MQOLS based on $C_2^{n-2} \times C_4$ and similarly $2^n - 1$ MQOLS based on $C_2^{n-3} \times Q_4$. We note that no sets of MOLS of this size are known to be based on these groups for any n.

6 Difference Matrices from Quasi-Orthomorphisms

Let G be a finite group of order n. A $(n, k; \lambda)$-*difference matrix* $D = (d_{ij})$ is a $k \times n\lambda$ matrix with entries from G such that for each $1 \leq i < j \leq k$, the list $d_{i1}d_{j1}^{-1}, \ldots, d_{i,n\lambda}d_{j,n\lambda}^{-1}$ contains each element of G precisely λ times. We refer to such a list as the difference between rows i and j of D. For further details regarding difference matrices, see [2].

The next theorem shows how quasi-orthomorphisms of groups can be used to construct difference matrices with even λ. The following proof uses the fact that if $x_1, \ldots, x_n$ is a quasi-ordering of G then the list $x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}$ contains every element of G twice.

Theorem 7 *Let $S = \{\phi_1, \ldots, \phi_t\}$ be a set of mutually quasi-orthogonal quasi-orthomorphisms of an abelian group G. Then there exists a $(n, t+2; 2)$ difference matrix over G.*

Proof: We construct the $(t+2) \times 2n$ matrix $D = [A|A^{-1}]$ as follows, where A^{-1} is the array A with every entry replaced by its inverse, and A is the

$(t+2) \times n$ matrix below.

$$A = \begin{pmatrix} \phi_1(g_1) & \phi_1(g_2) & \cdots & \phi_1(g_n) \\ \vdots & \vdots & & \vdots \\ \phi_t(g_1) & \phi_t(g_2) & \cdots & \phi_t(g_n) \\ g_1 & g_2 & \cdots & g_n \\ e & e & \cdots & e \end{pmatrix}$$

Let θ_i, θ_j denote the quasi-complete mappings associated with $\phi_i, \phi_j \in S$. Indexing rows as $1, \ldots, t, t+1, t+2$ the difference between rows $t+1$ and i is the list $\theta_i(g_1), \ldots, \theta_i(g_n), \theta_i(g_1)^{-1}, \ldots, \theta_i(g_n)^{-1}$, which contains every element of G twice. Now consider the difference between rows i, j. This is the list

$$\phi_i^{-1}(g_1)\phi_j(g_1), \ldots, \phi_i^{-1}(g_n)\phi_j(g_n), [\phi_i^{-1}(g_1)\phi_j(g_1)]^{-1}, \ldots, [\phi_i^{-1}(g_n)\phi_j(g_n)]^{-1}$$

which contains every element of G twice. □

Corollary 1 *There exists a* $(2^\alpha, 2^\alpha, 2)$*-difference matrix over* $C_2^{\alpha-2} \times C_4$.

Proof: Follows from theorem 7 since there exist $2^n - 2$ mutually quasi-orthogonal quasi-orthomorphisms based on $C_2^{\alpha-2} \times C_4$. □

Although the existence of $(2^\alpha, 2^\alpha; 2)$-difference matrices is well known, as far as the authors are aware, this is the first construction of such matrices over the group $C_2 \times C_2 \times \cdots \times C_4$.

References

[1] D. Bedford, Quasi-orthogonal latin squares and related designs, Journal of Comb. Math. and Comb. Computing 26, (1998) 213-224.

[2] Th. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, 1985.

[3] C.J. Colbourn, M.J. Colbourn, J.J. Harms, A. Rosa, A complete census of (10, 3, 2)-block designs and of Mendelsohn triple systems of order ten. III. (10, 3, 2)-block designs without repeated blocks, Congressus Numerantium, 37 (1983), 211-234.

[4] B. Ganter, A. Gulzow, R. Mathon, A. Rosa, A complete census of (10, 3, 2)-block designs and of Mendelsohn triple systems of order ten. IV. (10, 3, 2)-block designs with repeated blocks, Technical Report 5/78, Gesamthochschule Kassel, 1978.

[5] B. Ganter, R. Mathon, A. Rosa, A complete census of $(10, 3, 2)$-block designs and of Mendelsohn triple systems of order ten. I. Mendelsohn triple systems without repeated blocks. Proc. Seventh Manitoba Conf. on Numerical Math. and Computing, (1977), 383-398. Congressus Numerantium XX, Univ. of Mantoba, Winnipeg.

[6] B. Ganter, R. Mathon, A. Rosa, A complete census of $(10, 3, 2)$-block designs and of Mendelsohn triple systems of order ten. II. Mendelsohn triple systems with repeated blocks. Proc. Eighth Manitoba Conf. on Numerical Math. and Computing, (1978), 181-204. Congressus Numerantium XXII, Univ. of Mantoba, Winnipeg.

[7] M.Hall and L.J Paige, Complete mappings of finite groups, Pacific J. Math. 5 (1955), 541-549.

[8] D. M. Johnson, A. L. Dulmage, N. S. Mendelsohn, Orthomorphisms of groups and orthogonal latin squares, I, Canad. J. Math. 13 (1961), 356-372.

[9] D. Jungnickel, On regular sets of latin squares, Problemes combinatoires et theorie des graphes (colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976) Colloq. Internat. CNRS 260, 255-256.

[10] A. D. Keedwell, Concerning the existence of triples of pairwise almost orthogonal 10×10 latin squares, Ars Comb. 9 (1980), 3-10.

[11] A. D. Keedwell, Complete mappings and sequencings of finite groups, in: C.J. Colbourn, J.H. Dinitz eds., The CRC Handbook of Combinatorial Designs, CRC Press, 1996, 246-253.

[12] R. Mathon, Bounds for equidistant permutation arrays of index one, in: Combinatorial Mathematics: Proc. of the Third International Conf. New York Academy of Sciences, New York, 1989, 303-309.

[13] K.A.S. Quinn, Difference matrices and orthomorphisms over non-abelian groups, Ars Comb. to appear.

[14] R. M. Whitaker, A complete census of the resolutions of $(10, 3, 2)$-balanced incomplete block designs, Research Report 98-1, Department of Mathematics, Keele University, 1998.

[15] R. M. Whitaker, Mutually Quasi-Orthogonal Latin Squares, Ph.D. thesis, Keele University, in preparation.