Noname manuscript No.
(will be inserted by the editor)

Difference Covering Arrays and Pseudo-Orthogonal Latin Squares

Fatih Demirkale · Diane Donovan · Joanne Hall · Abdollah Khodkar · Asha Rao

Received: date / Accepted: date

Abstract A pair of Latin squares, A and B, of order n, is said to be pseudo-orthogonal if each symbol in A is paired with every symbol in B precisely once, except for one symbol with which it is paired twice and one symbol with which it is not paired at all. A set of t Latin squares, of order n, are said to be mutually pseudo-orthogonal if they are pairwise pseudo-orthogonal. A special class of pseudo-orthogonal Latin squares are the mutually nearly orthogonal Latin squares (MNOLS) first discussed in 2002, with general constructions

F. Demirkale
Department of Mathematics,
Yıldız Technical University
Esenler, İstanbul 34220, Turkey.
E-mail: fatihd@yildiz.edu.tr

D. Donovan
School of Mathematics and Physics
University of Queensland
Brisbane, QLD 4072, Australia
E-mail: dmd@maths.uq.edu.au

J. Hall
Mathematical Sciences School
Queensland University of Technology
Brisbane, QLD 4000, Australia
Tel.: + 61 7 31380458
E-mail: j42.hall@qut.edu.au

A. Khodkar
Department of Mathematics
University of West Georgia
Carrollton, GA 30118, USA
E-mail: akhodkar@westga.edu

A. Rao
School of Mathematical and Geospatial Sciences
RMIT University
Melbourne, VIC 3000, Australia
E-mail: asha@rmit.edu.au

given in 2007. In this paper we develop row complete MNOLS from difference covering arrays. We will use this connection to settle the spectrum question for sets of 3 mutually pseudo-orthogonal Latin squares of even order, for all but the order 146.

Keywords Difference covering array · Latin squares · pseudo-orthogonal Latin squares · mutually nearly orthogonal Latin squares

Mathematics Subject Classification (2000) 05B15

1 Introduction

Difference matrices are a fundamental tool used in the construction of combinatorial objects, generating a significant body of research that has identified a number of existence constraints. These difference matrices have been used for diverse applications, for instance, in the construction of authentication codes without secrecy [13], software testing [3,4] and data compression [9]. This diversity of applications, coupled with existence constraints, has motivated authors to generalise the definition to holey difference matrices, difference covering arrays and difference packing arrays, to mention just a few.

Some orthogonal Latin squares are combinatorialy equivalent to difference matrices [8] with specific properties, hence many of the applications for difference matrices apply to orthogonal Latin squares. However in the design of certain experiments, designs that are close to being mutually orthogonal are preferred [1,2]. Thus constructing sets of pseudo-orthogonal Latin squares, (and their combinatorially equivalent difference matrices) are of interest to experimental scientists, in addition to satisfying mathematical curiosity.

In the current paper we are interested in constructing subclasses of cyclic difference covering arrays and exploiting these structures to emphasize new connections with other combinatorial objects, such as pseudo-orthogonal Latin squares. We use this connection to settle the existence spectrum for sets of 3 mutually pseudo-orthogonal Latin squares of even order, in all but one case. We begin with the formal definitions.

A *difference matrix* (DM) over an abelian group $(G,+)$ of order n is defined to be an $\lambda n \times k$ matrix $Q = [q(i,j)]$ with entries from G such that, for all pairs of columns $0 \le j, j' \le k-1$, $j \ne j'$, the difference multi-set

$$\Delta_{j,j'} = \{q(i,j) - q(i,j') \mid 0 \le i \le \lambda n - 1\}$$

contains every element of G equally often, say λ times. E.g. [5,7,8]. Note that we label the rows from 0 to $\lambda n - 1$ and the columns 0 to $k-1$. Also to be consistent with later sections involving Latin squares and covering arrays our definition uses the transpose of the matrix given in [5] and [7]. Since the addition of a constant, over G, to any row and a constant to columns does not alter the set $\Delta_{j,j'}$, we may assume that one row and one column contain only 0, the identity element of G. More precisely, to simplify later calculations, we will assume that all entries in the last row and last column of Q are 0. A difference matrix will be denoted $\mathrm{DM}(n, k; \lambda)$. If $(G, +)$ is a cyclic group we refer to a *cyclic difference matrix.*

Theorem 1 *[5, Thm 17.5, p 411] A $DM(n, k; \lambda)$ does not exist if $k > \lambda n$.*

In the main, we will use difference matrices with $k = 4$, $\lambda = 1$ and where possible we will work with cyclic difference matrices. In Section 4 we list a number of existence results.

A *holey difference matrix* (HDM) [16] over an abelian group $(G, +)$ of order n with a subgroup H of order h is defined to be an $\lambda(n-h) \times k$ matrix $Q = [q(i, j)]$ with entries from G such that, for all pairs of columns $0 \le j, j' \le k-1$, $j \neq j'$, the difference multi-set

$$\Delta_{j,j'} = \{q(i, j) - q(i, j') \mid 0 \le i \le \lambda(n-h) - 1\}$$

contains every element of $G \setminus H$ equally often, say λ times. A holey difference matrix will be denoted $\mathrm{HDM}(k, n; h)$, where $|G| = n$ and $|H| = h$. If G is a cyclic group then we refer to a *cyclic holey difference matrix.*

As before, a constant may be added to any column without affecting $\Delta_{j,j'}$ so we may assume that all entries in the last column of Q are equal to 0. However since H is a subgroup, 0 belongs to the hole. Consequently, 0 does not occur in $\Delta_{j,j'}$, and thus there will be no row containing two or more 0's. Further since $\Delta_{j,k-1} = \lambda(G \setminus H)$, $0 \le j \le k-2$, the entries of H do not occur in the first $k-1$ columns of Q.

A *difference covering (packing) array* over an abelian group $(G, +)$ of order n is defined to be an $\eta \times k$ matrix $Q = [q(i, j)]$ with entries from G such that, for all pairs of distinct columns $0 \le j, j' \le k-1$, the difference multi-set

$$\Delta_{j,j'} = \{q(i, j) - q(i, j') \mid 0 \le i \le \eta - 1\}$$

contains every element of G at least (at most) once, see for example [16, 17]. A difference covering array will be denoted $\mathrm{DCA}(k, \eta; n)$ and a difference packing array will be denoted $\mathrm{DPA}(k, \eta; n)$. If $(G, +)$ is the cyclic group, then the difference covering (packing) array is said to be *cyclic.* As before we may assume that the last row and last column of a $\mathrm{DCA}(k, \eta; n)$ contain only 0.

In the papers [16] and [17], Yin constructs cyclic $\mathrm{DCA}(4, n+1; n)$ for all even integers n, with similar results for cyclic difference packing arrays. Yin documents a number of product constructions for difference covering arrays, some of which will be reviewed in Section 4 and then adapted to construct difference covering arrays with specific properties; properties that build connections with pseudo-orthogonal Latin squares.

The additional properties that we seek are that 0 (the identity element of G) occurs at least twice in each column of the $\mathrm{DCA}(k, n+1; n)$ and for pairs of columns, not including the last column, the repeated difference is not the element 0. Formally, we are interested in $\mathrm{DCA}(k, n+1; n)$, $Q = [q(i, j)]$, $(0 \le i \le n,\ 0 \le j \le k-1)$ satisfying the properties:

P1. the entry $0 \in G$ occurs at least twice in each column of Q, and

P2. for all pairs of distinct columns j and j', $j \neq k-1 \neq j'$, $\Delta_{j,j'} = \{q(i,j) - q(i,j') \mid 0 \leq i \leq n-1\} = G \setminus \{0\}$,

Note that **P2** implies that $\Delta_{j,j'}$ contains a repeated difference that is not 0.

The following example is a cyclic DCA$(4,7;6)$ satisfying **P1** and **P2** [12].

$$B^T = \begin{bmatrix} 0\,1\,2\,3\,4\,5\,0 \\ 1\,3\,5\,0\,2\,4\,0 \\ 3\,0\,4\,1\,5\,2\,0 \\ 0\,0\,0\,0\,0\,0\,0 \end{bmatrix}$$

In the next lemma we show that if G is the cyclic group $\mathbb{Z}_n$, then these conditions imply that for all distinct columns j and j', $j \neq k-1 \neq j'$,

$$\Delta_{j,j'} = \{0, 1, 2, \ldots, n/2, n/2, \ldots, n-1\}$$

with repetition retained.

Lemma 1 *If there exists a cyclic DCA$(k, n+1; n)$, $Q = [q(i,j)]$, $(0 \leq i \leq n$, $0 \leq j \leq k-1)$ satisfying properties* **P1** *and* **P2**, *then n is even. Further, given d_0 such that $d_0 = q(i,j) - q(i,j') = q(i',j) - q(i',j')$, for $i \neq i'$ and $k-1 \neq j \neq j' \neq k-1$, then $d_0 = n/2$.*

Proof Let $Q = [q(i,j)]$ $(0 \leq i \leq n,\ 0 \leq j \leq k-1)$ represent the difference covering array. The definition requires that $\mathbb{Z}_n \subseteq \Delta_{j,j'}$ and since column $k-1$ of Q contains all zeros, property **P1** implies that the remaining columns are permutations of the multi-set $\{0, 0, 1, 2, \ldots, n-1\}$.

Let $d_0 \in \mathbb{Z}_n \setminus \{0\}$ represent the repeated difference in $\Delta_{j,j'}$. Suppose n is odd and, without loss of generality, that column 0 is in standard form. Then, for all $0 < j \leq k-2$, $\sum_{i=0}^{n-1} q(i,j) = \frac{(n-1)n}{2}$ and

$$\sum_{i=0}^{n-1} (i - q(i,j)) \equiv \frac{(n-1)n}{2} + d_0 \mod n.$$

Consequently, $2d_0 = n(2\ell - n + 1)$, for some integer ℓ, or equivalently $n|2d_0$. But since n is odd, this leads to the contradiction, $d_0 \in \mathbb{Z}_n$ and $n|d_0$. Thus n is $2p$ for some integer p, where p divides d_0, implying $d_0 = p$.

The remainder of this paper is organised as follows. In Section 2 we will draw the connection between DCA$(k, n+1; n)$ and sets of mutually pseudo-orthogonal Latin squares. In Section 3 we give three new constructions for DCA$(4, n+1; n)$'s and consequently new families of mutually pseudo-orthogonal Latin squares. In Section 4 we review some of the general constructions for difference covering arrays and show that these constructions can be used to construct DCA$(k, n+1; n)$ that satisfy Properties **P1** and **P2**, and hence mutually pseudo-orthogonal Latin squares. This leads to showing that 3 mutually pseudo-orthogonal Latin squares exist for every order except possibly 146.

The notation $[a, b] = \{a, a+1, \ldots, b-1, b\}$ refers to the closed interval of integers from a to b.

2 Pseudo-orthogonal Latin squares and difference covering arrays

In this section we verify that cyclic difference covering arrays can be used to construct pseudo-orthogonal Latin squares.

A *Latin square* of order n is an $n \times n$ array in which each of the symbols of $\mathbb{Z}_n$ occurs once in every row and once in every column. Two Latin squares $A = [a(i,j)]$ and $B = [b(i,j)]$, of order n, are said to be *orthogonal* if

$$O = \{(a(i,j), b(i,j)) \mid 0 \le i, j \le n-1\} = \mathbb{Z}_n \times \mathbb{Z}_n.$$

A set of t Latin squares is said to be *mutually orthogonal*, t-MOLS(n), if they are pairwise orthogonal. A set of t *idempotent* MOLS(n), denoted t-IMOLS(n), is a set of t-MOLS(n) each of which is idempotent; that is, the cell (i,i) contains the entry i, for all $0 \le i \le n-1$. It is well known that difference matrices can be used to construct sets of mutually orthogonal Latin squares, see for instance [8, Lemma 6.12].

Raghavarao, Shrikhande and Shrikhande [12] and Bate and Boxall [1] slightly vary the orthogonality condition to that of pseudo-orthogonal. A pair of Latin squares, $A = [a(i,j)]$ and $B = [b(i,j)]$, of order n, is said to be *pseudo-orthogonal* if given $O = \{(a(i,j), b(i,j)) \mid 0 \le i, j \le n-1\}$, for all $c \in \mathbb{Z}_n$

$$|\{(c, b(i,j)) \mid (c, b(i,j)) \in O\}| = n-1.$$

That is, each symbol in A is paired with every symbol in B precisely once, except for one symbol with which it is paired twice and one symbol with which it is not paired at all. A set of t Latin squares, of order n, are said to be mutually pseudo-orthogonal if they are pairwise pseudo-orthogonal.

Mutually nearly orthogonal Latin squares (MNOLS) are a special class of pseudo-orthogonal Latin squares, in that the set O does not contain the pair (c,c), for any $c \in \mathbb{Z}_n$ and the pair $(i, i+n/2 \bmod n)$ appears twice in O, where $0 \le i \le n-1$. Mutually nearly orthogonal Latin squares (MNOLS) were first discussed in a paper by Raghavarao, Shrikhande and Shirkhande in 2002 [12].

A natural question to ask is: Can we use difference techniques to construct mutually pseudo-orthogonal Latin squares? Raghavarao, Shrikhande and Shirkhande did precisely this and constructed mutually pseudo-orthogonal Latin squares from cyclic DCA$(k, n+1; n)$ termed (k,n)-difference sets in [12].

Theorem 2 *[12] If there exists a cyclic DCA$(t+1, 2p+1; 2p)$, $Q' = [q'(i,j)]$, that satisfies* **P1** *and* **P2***, then there exists a set of t mutually nearly orthogonal Latin squares of order $2p$.*

Proof Recall that without loss of generality we may assume that the last row and column of Q' contain all zeros. Construct a new matrix $Q = [q(i,j)]$ by removing the last row and last column from Q' and define a set of t arrays, $L_s = [l_s(i,j)]$, $0 \le s \le t-1$, of order $2p$, by

$$l_s(i,j) = q(i,s) + j (\bmod 2p), \; 0 \le i, j \le 2p-1. \tag{1}$$

It is easy to see that each column of L_s is a permutation of $\mathbb{Z}_{2p}$ and so L_s is a Latin square. By Lemma 1

$$\Delta_{j,j'} = \{q'(i,j) - q'(i,j') \mid 1 \le i \le 2p\} = (\mathbb{Z}_{2p} \setminus \{0\}) \cup \{p\}$$

implying that when any two Latin squares are superimposed we obtain the set of ordered pairs $(\{\mathbb{Z}_{2p} \times \mathbb{Z}_{2p}\} \setminus \{(x,x) \mid 0 \le x \le 2p-1\}) \cup \{(x, x+p) \mid 0 \le x \le 2p-1\}$ with repetition retained.

If there exists a pair of pseudo-orthogonal Latin squares generated from cyclic difference covering arrays satisfying **P1** and **P2**, then there exists a pair of nearly orthogonal Latin squares. Conversely, a pair of nearly orthogonal Latin squares are necessarily pseudo-orthogonal Latin squares. Given this and the connection with [10] and [12] we will state all results in terms of MNOLS.

Raghavarao, Shrikhande and Shirkhande established bounds on the maximum number of Latin squares in a set of MNOLS [12]. This result provides bounds on t for DCA$(t, n+1; n)$ that satisfy **P1** and **P2**.

Lemma 2 *Let $p \ge 2$ be a positive integer. If there exists a DCA$(t+1, 2p+1; 2p)$ that satisfies* **P1** *and* **P2***, then $t \le p+1$. Further if p is even and there exists a DCA$(t, 2p+1; 2p)$, then $t < p+1$.*

Proof Theorem 5.2 of [12] gives bounds on NMOLS(2p). Theorem 2 shows that this can be applied to DCA$(t+1, 2p+1; 2p)$ and DCA$(t, 2p+1; 2p)$.

An $n \times n$ Latin square $L = [\ell(i,j)]$ with entries from $\mathbb{Z}_n$ is *row complete* if the ordered pairs $(\ell_{i,j}, \ell_{i,j+1})$ are all distinct for all $1 \le i \le n$ and $1 \le j \le n-1$. Williams showed that the Latin square corresponding to the cyclic group of even order is row complete, [15]. Since the MNOLS$(2p)$ constructed from cyclic difference covering arrays are essentially copies of the cyclic group, they are row complete. In addition, they are *bachelor squares*, in that they have no orthogonal mate.

3 Construction of difference covering arrays DCA$(4, 2m+1; 2m)$

This section is devoted to giving new constructions for families of cyclic DCA$(4, 2m+1; 2m)$ when $m = 2k+1$, $m = 8k+4$ and $m = 3k+2$, respectively. In each of these cases the difference covering arrays satisfy **P1** and **P2** and so they can be used to construct MNOLS$(2m)$.

When using a cyclic DCA$(4, 2m+1; 2m)$ to construct nearly orthogonal Latin squares we strip off the last row and last column of zeros. Thus to reduce the complexity of the notation and to avoid confusion, we will assume that we are constructing a $2m \times 3$ array $Q = [q(i,j)]$ that satisfies:

- each column is a permutation of $\mathbb{Z}_{2m}$ and
- $\Delta_{j,j'} = \{q(i,j) - q(i,j')| \mid 0 \le i \le 2m-1\} = \{1, 2, \ldots, m, m, \ldots, 2m-1\}$, with repetition retained.

Also we will use the following notation: $q(a,0) = a$ (or $q(\alpha,0) = a(\alpha)$), $q(a,1) = b(a)$ (or $q(\alpha,1) = b(\alpha)$), and $q(a,2) = c(a)$ (or $q(\alpha,2) = c(\alpha)$).

The following lemmas document some well known results, stated without proof, which will be used extensively in the proof of subsequent results.

Lemma 3 *For all integers x, y, z,* $\gcd(x + yz, z) = gcd(x, z)$.

Lemma 4 *Let g and p be positive integers and h a non-negative integer. Working modulo $2p$, if $gcd(g, 2p) = 1$ then*

$$\{gx + h \mid 0 \leq x \leq 2p - 1\} = \mathbb{Z}_{2p},$$

or if $gcd(g, 2p) = r$ and $h \equiv s \bmod r$ then

$$\{gx + h \mid 0 \leq x \leq 2p/r - 1\} = \{rx + s \mid 0 \leq x \leq 2p/r - 1\}.$$

3.1 Construction for general families DCA$(4, 2m + 1; 2m)$ for some odd m

In this subsection we give a general construction for a difference covering array DCA$(4, 2m + 1; 2m)$, for m odd. The proof that such a difference covering array exists uses the results presented in the following lemma. Note that in this section unless otherwise stated all arithmetic is modulo $2m$. In particular, for $i \not\equiv 2 \bmod 3$ a non-negative integer, and $k = 2i^2 + 7i + 6$, we present an infinite family of DCA$(4, 2m + 1; 2m)$ for $m = 2k + 1$.

Lemma 5 *Let f and m be integers such that $gcd(f, 2m) = 2$, $gcd(f+2, 2m) = 2$, and $f^2 + f + 1 \equiv m \bmod 2m$. Then*

$$\gcd(f, m) = 1, \quad (2)$$
$$\gcd(f + 1, m) = 1, \quad (3)$$
$$\gcd(f - 1, m) = 1, \quad (4)$$
$$\gcd(2f + 1, m) = 1 \quad (5)$$
$$mf \equiv 0 \bmod 2m. \quad (6)$$

Proof Eq 2: Since f is even, $f^2 + f + 1$ is odd, implying m is odd and hence $\gcd(f, m) = 1$.

Eq 3: Since $f + 1 \equiv -f^2 \bmod m$ and $\gcd(f, m) = 1$, we have $1 = \gcd(f, m) = \gcd(f^2, m) = \gcd(f + 1, m)$.

Eq 4: Since $f - 1 \equiv f(f+2) \bmod m$, $\gcd(f, m) = 1$ and $\gcd(f+2, m) = 1$, we have $1 = \gcd(f(f + 2), m) = \gcd(f - 1, m)$.

Eq 5: Since $2f+1 \equiv -f(f-1) \bmod m$, $\gcd(f, m) = 1$ and $\gcd(f-1, m) = 1$, we have $1 = \gcd(f(f - 1), m) = \gcd(2f + 1, m)$.

Eq 6: This follows from the fact that f is even.

For a suitable choice of f, we partition the domain of a into the subintervals $[0, m + f]$, $[m + f + 1, m - 1]$, $[m, m - f - 1]$ and $[m - f, 2m - 1]$ where all endpoints are included. (Additions are all modulo $2m$.)

Intervals	I_1	I_2	I_3	I_4
$q(a,0) = a$	$[0, m+f]$	$[m+f+1, m-1]$	$[m, m-f-1]$	$[m-f, 2m-1]$
$q(a,1) = b(a)$	$af + m$	$af + m$	$(a+1)f$ $+m-1$	$(a+1)f$ $+m-1$
$q(a,2) = c(a)$	$-(a-1)(f+1)$ -2	$-(a-1)(f+1)$ $+m-2$	$-a(f+1)$ $+m$	$-a(f+1)$
$b(a) - a$	$a(f-1)$ $+m$	$a(f-1)$ $+m$	$(a+1)(f-1)$ $+m$	$(a+1)(f-1)$ $+m$
$c(a) - a$	$-(a-1)(f+2)$ -3	$-(a-1)(f+2)$ $+m-3$	$-a(f+2)$ $+m$	$-a(f+2)$
$c(a) - b(a)$	$-a(2f+1)$ $+f-1+m$	$-a(2f+1)$ $+f-1$	$-a(2f+1)$ $-(f-1)$	$-a(2f+1)$ $-(f-1)+m$

Fig. 1 Entries are elements of $\mathbb{Z}_{2m}$, where $q(a,0) = a$, $q(a,1) = b(a)$ and $q(a,2) = c(a)$ in the array $Q = [q(i,j)]$. Rows 5 to 7 give the differences.

Example 1 To aid understanding we begin with an example constructing a *DCA* according to Figure 1 with $m = 13$ and $f = 16$. We give the transpose of the difference covering array DCA$(4, 27; 26)$. The key to understanding the proof is to recognise that within the subintervals $I_1 = [0,3], I_2 = [4,12], I_3 = [13,22]$ and $I_4 = [23,25]$, the value of a, $b(a)$ and $c(a)$ increases by a constant "jump", respectively 1, $f = 16$ and $-(f+1) = 9$. This implies that the differences will also increase by a constant. By carefully choosing the start value on each subinterval it is possible to obtain the required values in $\mathbb{Z}_{2m}$. The value $m = 13$ is boldfaced in the differences.

	I_1				I_2									I_3										I_4		
a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$b(a)$	13	3	19	9	25	15	5	21	11	1	17	7	23	2	18	8	24	14	4	20	10	0	16	6	22	12
$c(a)$	15	24	7	16	12	21	4	13	22	5	14	23	6	0	9	18	1	10	19	2	11	20	3	25	8	17
$b(a) - a$	**13**	2	17	6	21	10	25	14	3	18	7	22	11	15	4	19	8	23	12	1	16	5	20	9	24	**13**
$c(a) - a$	15	23	5	**13**	8	16	24	6	14	22	4	12	20	**13**	21	3	11	19	1	9	17	25	7	2	10	18
$c(a) - b(a)$	2	21	14	7	**13**	6	25	18	11	4	23	16	9	24	17	10	3	22	15	8	1	20	**13**	19	12	5

Theorem 3 *Let f and m be natural numbers such that* $\gcd(f, 2m) = 2$, $\gcd(f+2, 2m) = 2$, $f^2 + f + 1 \equiv m \bmod 2m$, *and* $m + 3 \le f \le 2m - 4$. *Then a cyclic DCA*$(4, 2m+1; 2m)$ *satisfying* **P1** *and* **P2** *exists.*

Proof The proof is by construction with the values of DCA$(4, 2m+1; 2m)$ as given in Figure 1, with the 3 columns of $Q = [q(i,j)]$ given by $q(a,0) = a$, $q(a,1) = b(a)$, $q(a,2) = c(a)$. We will show that Q has the required properties.

If $m + 3 \le f \le 2m - 4$ and f is even then, working in the least residue system modulo $2m$, we have $3 \le m + f \le m - 4$ and so the intervals $[0, m+f]$ and $[m+f+1, m-1]$ are non-empty. Further, $m + 4 \le m - f \le 2m - 3$ and so the intervals $[m, m-f-1]$ and $[m-f, 2m-1]$ are non-empty.

Given that f is even and m is odd, then by Lemma 4

$$af + m \equiv 1 \bmod 2 \Longrightarrow \{b(a) \mid a \in I_1 \cup I_2\} = \{2g + 1 \mid 0 \le g \le m - 1\},$$

$$(a+1)f + m - 1 \equiv 0 \bmod 2 \Longrightarrow \{b(a) \mid a \in I_3 \cup I_4\} = \{2g \mid 0 \le g \le m - 1\},$$

and so $\{b(a) \mid 0 \le a \le 2m - 1\} = [2m]$.

On each of the subintervals $c(a)$ takes the form $ag+h$, where $g=-(f+1)$, so the "jump" size is $-(f+1)$ and

$$\begin{aligned}
c(m) &= 0,\\
c(m+f+1)-c(m-f-1) &= -m-f(f+1)+m-2+m\\
&\quad -f(f+1)-(f+1)-m\\
&= -2f^2-2f-2-(f+1) = -(f+1),\\
c(0)-c(m-1) &= -(f+1),\\
c(m-f)-c(m+f) &= -(f+1),\\
c(m)-c(2m-1) &= -(f+1).
\end{aligned}$$

Thus by reordering the subintervals as I_3, I_2, I_1, I_4, and noting that $c(m-f-1)-(f+1)=c(m+f+1)$, we get $\{c(a) \mid 0 \le a \le 2m-1\} = [2m]$.

For $b(a)-a$, $c(a)-a$ and $c(a)-b(a)$ we are required to show that for $a \in [2m]$ the differences cover the multi-set $\{1,2,\ldots,m-1,m,m,m+1,\ldots,2m-1\} = ([2m]\setminus\{0\})\cup\{m\}$.

For $b(a)-a$, the subintervals are taken in natural order I_1, I_2, I_3, I_4. Starting at $a=0$ and finishing at $a=2m-1$, we have $b(0)-0=m=(2m-1+1)(f-1)+m=b(2m-1)-(2m-1)$, so the difference m occurs twice. Further, the $\gcd(f-1,2m)=1$ implies that $a(f-1)+m$, $0\le a\le m-1$, are all distinct, as are $(a+1)(f-1)+m$, $m\le a\le 2m-1$ and

$$\begin{aligned}
b(m)-m &= (m+1)(f-1)+m = f-1,\\
b(m-1)-(m-1) &= (m-1)(f-1)+m = -(f-1).
\end{aligned}$$

Thus there is a "jump" of $-2(f-1)$ between $a=m-1$ and $a=m$ and the difference 0 is omitted, implying $\{b(a)-a \mid 0\le a\le 2m-1\} = ([2m]\setminus\{0\})\cup\{m\}$.

For $c(a)-a$, since $f+2$ is even and $\gcd(f+2,m)=1$, these values are all distinct on each of the subintervals, $|I_3\cup I_1| = m+1$, $|I_4\cup I_2| = m-1$, and

$$\begin{aligned}
c(m)-m &= -m(f+2)+m = m,\\
c(m+f)-(m+f) &= -(m+f-1)(f+2)-3 = m,\\
(c(0)-0)-(c(m-f-1)-(m-f-1)) &= m-f(f+2)-3 = -(f+2),\\
c(2m-1)-(2m-1) &= -(2m-1)(f+2) = f+2,\\
c(m+f+1)-(m+f+1) &= -f^2-2f+m-3 = -(f+2).
\end{aligned}$$

Thus $-(a-1)(f+2)-3, -a(f+2)+m \equiv 1 \bmod 2$, hence,

$$\{c(a)-a \mid a\in I_3\cup I_1\} = \{2g+1 \mid 0\le g\le m-1\}\cup\{m\}.$$

In addition, $-a(f+2)+m-1, -a(f+2) \equiv 0 \bmod 2$ implies that

$$\{c(a)-a \mid a\in I_4\cup I_2\} = \{2g \mid 1\le g\le m-1\},$$

giving $\{c(a)-a \mid 0\le a\le 2m-1\} = ([2m]\setminus\{0\})\cup\{m\}$.

For $c(a) - b(a)$, since $\gcd(2f + 1, 2m) = 1$, these values are all distinct on the subintervals, $c(m + f + 1) - b(m + f + 1) = -2f^2 - 2f - 2 + m = m = m + 2f^2 + 2f + 2 = c(m - f - 1) - b(m - f - 1)$, and

$$\begin{aligned} c(0) - b(0) - (c(m-1) - b(m-1)) &= -(2f+1), \\ c(m+f) - b(m+f) &= 2f+1, \\ c(m-f) - b(m-f) &= -(2f+1). \end{aligned}$$

Thus when the subintervals are reordered to I_2, I_1, I_4, I_3 we may verify that $\{c(a) - b(a) \mid 0 \leq a \leq 2m - 1\} = ([2m] \setminus \{0\}) \cup \{m\}$. Note that the values of $c(a)-b(a)$ start and finish on m and the value 0 is omitted between $a = m+f$ and $a = m - f$.

Corollary 1 *For every non-negative integer* $i \not\equiv 2 \bmod 3$ *there exists a cyclic* $DCA(4, 2m + 1; 2m)$ *satisfying* **P1** *and* **P2**, *where* $m = 2(2i^2 + 7i + 6) + 1$.

Proof Taking $f = m+3+2i$, then f is even. In addition $m+3 \leq f \leq 2m-4$, since $i \geq 0$ and $2m - 4 = (m + 3) + (m - 7) = (m + 3) + (4i^2 + 14i + 6) \geq m + 3 + 2i = f$. Now

$$\begin{aligned} f^2 + f + 1 &\equiv 4i^2 + 14i + 13 \bmod 2m \\ &= 2(2i^2 + 7i + 6) + 1 = m \bmod 2m. \end{aligned}$$

Further, applying Lemma 3 repeatedly,

$$\begin{aligned} \gcd(f, 2m) &= 2(\gcd(2i^2 + 8i + 8, (2i^2 + 8i + 8) + 2i^2 + 6i + 5)), \\ &= 2(\gcd(2i + 3, 2i^2 + 4i + 2 + (2i + 3))), \\ &= 2(\gcd(2i + 3, 2(i + 1)^2)) = 2(\gcd(2i + 3, i + 1)) = 2. \end{aligned}$$

Also,

$$\begin{aligned} \gcd(f + 2, 2m) &= 2(\gcd(2i^2 + 8i + 9, (2i^2 + 8i + 9) + 2i^2 + 6i + 4)), \\ &= 2(\gcd(2i + 5, 2(i + 2)(i + 1))), \\ &= 2(\gcd(2i + 5, (i + 2)(i + 1))). \end{aligned}$$

Now $\gcd(2i + 5, i + 2) = \gcd(2(i + 2) + 1, i + 2) = 1$. Whereas

$$\begin{aligned} \gcd(2i + 5, i + 1) &= \gcd(2(i + 1) + 3, i + 1)) = \gcd(3, i + 1) \\ &\neq 1 \text{ when } i + 1 \equiv 0 \bmod 3 \text{ or equivalently i} \equiv 2 \bmod 3. \end{aligned}$$

Thus taking $i \not\equiv 2 \bmod 3$ we can construct a $\mathrm{DCA}(4, 2m + 1; 2m)$ as per Theorem 3.

Intervals	I_1	I_2	I_3	I_4
$q(a,0)=a$	$[0, m-1]$	$[m, 2m-1]$	$[2m, 3m-1]$	$[3m, 4m-1]$
$q(a,1)=b(a)$	$(a+1)f-1$	$(a+1)f-1$	af	af
$q(a,2)=c(a)$	$(a+1)(2m-f+2)$ -1	$a(2m-f+2)$ $-m$	$(a+1)(2m-f+2)$ $+m-1$	$a(2m-f+2)$
$b(a)-a$	$(a+1)(f-1)$	$(a+1)(f-1)$	$a(f-1)$	$a(f-1)$
$c(a)-a$	$(a+1)(2m-f+1)$	$a(2m-f+1)$ $-m$	$(a+1)(2m-f+1)$ $+m$	$a(2m-f+1)$
$c(a)-b(a)$	$(a+1)(2m-2f+2)$	$a(2m-2f+2)$ $-f-m+1$	$a(2m-2f+2)$ $+3m-f+1$	$a(2m-2f+2)$

Fig. 2 Entries are elements of $\mathbb{Z}_{4m}$, where $q(a,0)=a$, $q(a,1)=b(a)$ and $q(a,2)=c(a)$ in the array $Q=[q(i,j)]$.

3.2 Construction of difference covering arrays DCA$(4, 4m+1; 4m)$

In this subsection we give a general construction for a difference covering array DCA$(4, 4m+1; 4m)$. It will be shown that for all non-negative integers k, such that $3 \nmid (2k+1)$, this construction gives an infinite family of DCA$(4, 16k+9; 16k+8)$. The proof that such a difference covering array exists uses the results presented in the following lemma. Note that in this section unless otherwise stated all arithmetic is modulo $4m$.

Lemma 6 *Let f and m be natural numbers such that $m \equiv 2 \bmod 4$, $\gcd(f, 4m) = 2$, $\gcd(f-1, 4m) = 1$, and $f^2 + f - 2 \equiv 2m \bmod 4m$. Then*

$$\gcd(2m+2-f, 4m) = 4, \tag{7}$$
$$\gcd(2m-f+1, 4m) = 1, \tag{8}$$
$$\gcd(2m-2f+2, 4m) = 2, \tag{9}$$
$$mf \equiv 2m \bmod 4m. \tag{10}$$

Proof Eq 7: Rewriting $2m+2-f = f^2+f-2+2-f = f^2 \bmod 4m$ and assuming $\gcd(f, 4m) = 2$ gives $\gcd(f^2, 4m) = 4$.

Eq 8: Since $2m-f+1$ is odd, the $\gcd(2m-f+1, 4m)$ is odd. Assume there exists an odd x such that $x|4m$ and $x|(2m-f+1)$, then $x|m$ and so $x|(f-1)$. But the $\gcd(f-1, 4m) = 1$, so $x = 1$.

Eq 9: Assume that there exists x such that $x|(m-f+1)$ and $x|2m$. Since $m-f+1$ is odd, x is odd and so $x|m$. Consequently, $x|(f-1)$ and $x|4m$, implying $x = 1$.

Eq 10: $mf \equiv m(2m-f^2+2) = 2m^2 - mf^2 + 2m \equiv 2m \bmod 4m$.

Theorem 4 *Let f be a natural number and $m = 4k+2$, where k is a non-negative integer, such that $\gcd(f, 4m) = 2$, $\gcd(f-1, 4m) = 1$, and $f^2+f-2 \equiv 2m \bmod 4m$. Then a cyclic DCA$(4, 4m+1; 4m)$ satisfying* **P1** *and* **P2** *exists.*

Proof The proof is by construction with the values of DCA$(4, 4m+1; 4m)$ as given in Figure 2, with the 3 columns of $Q = [q(i,j)]$ given by $q(a,0) = a$, $q(a,1) = b(a)$, $q(a,2) = c(a)$. We will show that Q has the required properties.

For $b(a)$, since f is even, Lemma 4 implies that

$$\begin{aligned}(a+1)f-1 \equiv 1 \bmod 2 &\Longrightarrow \{b(a) \mid a \in I_1 \cup I_2\} = \{2g+1 \mid 0 \le g \le 2m-1\},\\ af \equiv 0 \bmod 2 &\Longrightarrow \{b(a) \mid a \in I_3 \cup I_4\} = \{2g \mid 0 \le g \le 2m-1\},\end{aligned}$$

and $\{b(a) \mid 0 \le a \le 4m-1\} = \mathbb{Z}_{4m}$.

For $c(a)$, since $\gcd(2m-f+2, 4m) = 4$, Lemma 4 implies that

$$\begin{aligned}(a+1)(2m-f+2)+m-1 \equiv 1 \bmod 4 &\Longrightarrow \{c(a) \mid a \in I_3\} = \{4g+1 \mid 0 \le g \le m-1\},\\ a(2m-f+2) \equiv 0 \bmod 4 &\Longrightarrow \{c(a) \mid a \in I_4\} = \{4g \mid 0 \le g \le m-1\},\\ (a+1)(2m-f+2)-1 \equiv 3 \bmod 4 &\Longrightarrow \{c(a) \mid a \in I_1\} = \{4g+3 \mid 0 \le g \le m-1\},\\ a(2m-f+2)-m \equiv 2 \bmod 4 &\Longrightarrow \{c(a) \mid a \in I_2\} = \{4g+2 \mid 0 \le g \le m-1\}.\end{aligned}$$

Thus the set of values $\{c(a) \mid a \in \mathbb{Z}_{4m}\} = \mathbb{Z}_{4m}$.

For $b(a)-a$, $c(a)-a$ and $c(a)-b(a)$ we are required to show that for $a \in \mathbb{Z}_{4m}$ the differences cover the multi-set $\{1, 2, \dots, 2m-1, 2m, 2m, 2m+1, \dots, 4m-1\} = (\mathbb{Z}_{4m} \setminus \{0\}) \cup \{2m\}$.

For $b(a)-a$, the $\gcd(f-1, 4m) = 1$, and

$$\begin{aligned}b(2m)-2m &= 2m(f-1) = 2m,\\ b(2m-1)-(2m-1) &= (2m-1+1)f-1-(2m-1) = (2m)(f-1) = 2m,\\ b(4m-1)-(4m-1) &= -(f-1),\\ b(0)-0 &= f-1.\end{aligned}$$

So using a "jump" of $f-1$ and ordering the subintervals as I_3, I_4, I_1, I_2 we obtain the difference $2m$ twice and the difference 0 is omitted between $a = 4m-1$ and $a = 0$ implying that $\{b(a)-a \mid 0 \le a \le 4m-1\} = (\mathbb{Z}_{4m} \setminus \{0\}) \cup \{2m\}$.

For $c(a)-a$, the $\gcd(2m-f-1, 4m) = 1$, and

$$\begin{aligned}c(m)-m &= m(2m-f+1)-m = 2m,\\ c(3m-1)-(3m-1) &= (3m-1+1)(2m-f+1)+m\\ &= 2m,\\ c(3m)-3m-(c(2m-1)-(2m-1)) &= (m+1)(2m-f+1)+m\\ &= 2m-f+1,\\ c(0)-0 &= 2m-f+1,\\ c(4m-1)-(4m-1) &= (4m-1)(2m+f-1)\\ &= -(2m-f+1),\\ c(2m)-2m-(c(m-1)-(m-1)) &= (m+1)(2m-f+1)+m\\ &= 2m-f+1.\end{aligned}$$

So using a "jump" of $2m-f+1$ and ordering the subintervals as I_2, I_4, I_1, I_3 we obtain the difference $2m$ twice and the difference 0 is omitted between $a = 4m-1$ and $a = 0$, implying $\{c(a)-a \mid 0 \le a \le 4m-1\} = (\mathbb{Z}_{4m} \setminus \{0\}) \cup \{2m\}$.

For $c(a) - b(a)$, and

$$\begin{aligned} c(3m) - b(3m) &= m(2m - 2f + 2) = 2m, \\ c(m-1) - b(m-1) &= (m - 1 + 1)(2m - 2 + 2) = 2m, \\ c(4m-1) - b(4m-1) &= -(2m - 2f + 2), \\ c(0) - b(0) &= 2m - 2f + 2, \\ c(2m) - b(2m) - (c(2m-1) - b(2m-1)) &= 2m - 2f + 2. \end{aligned}$$

Then since

$$\begin{aligned} 2m - 2f - 2 \equiv 0 \bmod 2 &\Longrightarrow \{c(a) - b(a) \mid a \in I_4 \cup I_1\} = \{2g \mid 1 \leq g \leq 2m-1\} \cup \{2m\}, \\ -f + 1 \equiv 1 \bmod 2 &\Longrightarrow \{c(a) - b(a) \mid a \in I_2 \cup I_3\} = \{2g + 1 \mid 0 \leq g \leq 2m-1\}, \end{aligned}$$

implying $\{c(a) - b(a) \mid 0 \leq a \leq 4m - 1\} = (\mathbb{Z}_{4m} \setminus \{0\}) \cup \{2m\}$.

Corollary 2 *For $k \geq 0$ such that $k \not\equiv 1 \bmod 3$ a cyclic DCA$(4, 4m+1; 4m)$, where $m = 4k + 2$, satisfying* **P1** *and* **P2** *can be constructed as described in Theorem 4.*

Proof Given $m = 4k + 2$, take $f = 2m - 2$. Then $f = 8k + 2$, and

$$\gcd(f, 4m) = 2(\gcd(4k + 1, 8k + 4)) = 2(\gcd(4k + 1, 2(4k + 1) + 2)) = 2.$$

In addition

$$\begin{aligned} \gcd(f - 1, 4m) &= \gcd(2m - 3, 4m) = \gcd(8k + 1, 16k + 8) \\ &= \gcd(8k + 1, 2k + 1) \ \text{ since } \ 2 \nmid (8\text{k} + 1) \\ &= \gcd(6k, 2k + 1) = 1, \text{ if } 3 \nmid (2\text{k} + 1). \end{aligned}$$

Also

$$\begin{aligned} f^2 + f - 2 &= 64k^2 + 32k + 4 + 8k + 2 - 2 = 4k(16k + 8) + 8k + 4 \\ &\equiv 2m \bmod 4\text{m}. \end{aligned}$$

Hence, $f = 2m-2$ satisfies the assumptions of Theorem 4 and we can construct a DCA$(4, 16k + 9; 16k + 8)$ for k such that $3 \nmid (2k + 1)$.

3.3 Construction of difference covering arrays DCA$(4, 2m + 1; 2m)$, where $m = 3\mu + 2$

In this subsection we give a general construction for a difference covering array DCA$(4, 2m+1; 2m)$, where $m = 3\mu+2$. Note that in this section unless otherwise stated all arithmetic is modulo $12k + 10$, $k \geq 0$.

Theorem 5 *Let μ be an odd positive integer. Then there exists a cyclic DCA$(4, 6\mu+5; 6\mu + 4)$ satisfying* **P1** *and* **P2**.

Intervals for α	I_1 $[0, \mu-1]$	I_2 $[\mu, 2\mu]$	I_3 $[2\mu+1, 3\mu+1]$
$q(\alpha,0)=a(\alpha)$	$3\alpha+3\mu+4$	$3\alpha+2$	$3\alpha+3\mu+4$
$q(\alpha,1)=b(\alpha)$	$3\alpha(\mu+1)+2\mu+2$	$3\alpha(\mu+1)+2\mu+2$	$3\alpha(\mu+1)+2\mu+2$
$q(\alpha,2)=c(\alpha)$	$\alpha(3\mu+4)+5\mu+4$	$\alpha(3\mu+4)+5\mu+4$	$\alpha(3\mu+4)+5\mu+4$
$b(\alpha)-a(\alpha)$	$3\alpha\mu-\mu-2$	$3\alpha\mu+2\mu$	$3\alpha\mu-\mu-2$
$c(\alpha)-a(\alpha)$	$\alpha(3\mu+1)+2\mu$	$\alpha(3\mu+1)+5\mu+2$	$\alpha(3\mu+1)+2\mu$
$c(\alpha)-b(\alpha)$	$\alpha+3\mu+2$	$\alpha+3\mu+2$	$\alpha+3\mu+2$
Intervals for α	I_4 $[3\mu+2, 4\mu+2]$	I_5 $[4\mu+3, 5\mu+2]$	I_6 $[5\mu+3, 6\mu+3]$
$q(\alpha,0)=a(\alpha)$	$3\alpha+3\mu+3$	$3\alpha+1$	$3\alpha+3\mu+3$
$q(\alpha,1)=b(\alpha)$	$3\alpha(\mu+1)+2\mu+1$	$3\alpha(\mu+1)+2\mu+1$	$3\alpha(\mu+1)+2\mu+1$
$q(\alpha,2)=c(\alpha)$	$\alpha(3\mu+4)+5\mu+4$	$\alpha(3\mu+4)+5\mu+4$	$\alpha(3\mu+4)+5\mu+4$
$b(\alpha)-a(\alpha)$	$3\alpha\mu-\mu-2$	$3\alpha\mu+2\mu$	$3\alpha\mu-\mu-2$
$c(\alpha)-a(\alpha)$	$\alpha(3\mu+1)+2\mu+1$	$\alpha(3\mu+1)+5\mu+3$	$\alpha(3\mu+1)+2\mu+1$
$c(\alpha)-b(\alpha)$	$\alpha+3\mu+3$	$\alpha+3\mu+3$	$\alpha+3\mu+3$

Fig. 3 Entries are elements of $\mathbb{Z}_{6\mu+4}$, where $q(\alpha,0)=a(\alpha)$, $q(\alpha,1)=b(\alpha)$ and $q(\alpha,2)=c(\alpha)$ in the array $Q=[q(i,j)]$.

Proof First note that $n=6\mu+4\geq 10$ and $\gcd(3\mu+4,6\mu+4)=\gcd(3\mu,3\mu+4)=\gcd(3\mu,4)=1$ since μ is odd.

Let $\mu=2k+1$, $k\geq 0$, then

$$\begin{aligned}&\mu(3\mu+2)=(2k+1)(6k+5)=3\mu+2, \text{ and}\\&(3\mu+2)^2=3\mu+2.\end{aligned}$$

That is, $(n/2)^2\equiv n/2 \bmod n$.

The proof is by construction with the values for DCA$(4,6\mu+5;6\mu+4)$ as given in Figure 3, with the three columns of $Q=[q(i,j)]$ given by $q(\alpha,0)=a(\alpha)$, $q(\alpha,1)=b(\alpha)$ and $q(\alpha,2)=c(\alpha)$.

Since $\gcd(3,n)=1$, by Lemma 4, $\{3\alpha \mid 0\leq\alpha\leq n-1\}=\mathbb{Z}_n$. Further $a(3\mu+2)=3(3\mu+2)+3\mu+3=1$ and $a(2\mu)=6\mu+2$ and there is a "jump" of 3 between $a(4\mu+2)$ and $a(0)$; $a(\mu-1)$ and $a(5\mu+3)$; $a(6\mu+3)$ and $a(2\mu+1)$; $a(3\mu+1)$ and $a(4\mu+3)$; $a(5\mu+2)$ and $a(\mu)$.

Thus reordering the subintervals as I_4,I_1,I_6,I_3,I_5,I_2 gives $\{a(\alpha)\mid 0\leq\alpha\leq n-1\}=\mathbb{Z}_n$.

For $b(\alpha)$,

$$\begin{aligned}3\alpha(\mu+1)+2\mu+2\equiv 0 \bmod 2 \Longrightarrow &\{b(\alpha)\mid \alpha\in I_1\cup I_2\cup I_3\}\\&=\{2g\mid 0\leq g\leq 3\mu+2\},\\3\alpha(\mu+1)+2\mu+1\equiv 1 \bmod 2 \Longrightarrow &\{b(\alpha)\mid \alpha\in I_4\cup I_5\cup I_6\}\\&=\{2g+1\mid 0\leq g\leq 3\mu+1\}.\end{aligned}$$

For $c(\alpha)$, since $\gcd(3\mu+4,6\mu+4)=1$ Lemma 4 implies that $\{c(\alpha)\mid 0\leq\alpha\leq 6\mu+3\}=\mathbb{Z}_{6\mu+4}$.

For $b(\alpha) - a(\alpha)$, since $\gcd(3\mu, 6\mu + 4) = 1$,

$$\begin{aligned} b(\mu) - a(\mu) &= 3\mu + 2, \\ b(4\mu + 2) - a(4\mu + 2) &= 3\mu + 2, \\ b(5\mu + 3) - a(5\mu + 3) - (b(2\mu) - a(2\mu)) &= 3\mu, \\ b(4\mu + 3) - a(4\mu + 3) - (b(\mu - 1) - a(\mu - 1)) &= 6\mu, \\ b(2\mu + 1) - a(2\mu + 1) - (b(5\mu + 2) - a(5\mu + 2)) &= 3\mu, \\ b(0) - a(0) - (b(6\mu + 3) - a(6\mu + 3) &= 3\mu. \end{aligned}$$

So using a "jump" of 3μ and ordering the subintervals as $I_2, I_6, I_1, I_5, I_3, I_4$, we obtain the difference $3\mu+2$ twice and since there is 6μ between $b(\alpha)-a(\alpha)$ for $\alpha = \mu - 1$ and $\alpha = 4\mu + 3$ the difference 0 is omitted implying that $\{b(\alpha) - a(\alpha) \mid 0 \le \alpha \le 6\mu + 3\} = (\mathbb{Z}_n \setminus \{0\}) \cup \{n/2\}$.

For $c(\alpha) - b(\alpha)$, since $\gcd(3\mu + 1, 6\mu + 4) = 2$, we have

$$\begin{aligned} c(5\mu + 3) - a(5\mu + 3) &= 3\mu + 2, \\ c(2\mu) - a(2\mu) &= 3\mu + 2, \\ c(3\mu + 2) - a(3\mu + 2) - (c(6\mu + 3) - a(6\mu + 3)) &= -(3\mu + 3), \\ c(\mu) - a(\mu) - (c(4\mu + 2) - a(4\mu + 2)) &= -(3\mu + 3), \\ c(2\mu + 1) - a(2\mu + 1) &= 3\mu + 1, \\ c(5\mu + 2) - c(5\mu + 2) &= 3\mu + 3, \\ c(0) - a(0) - (c(3\mu + 1) - a(3\mu + 1)) &= -(3\mu + 3), \\ c(\mu - 1) - a(\mu - 1) - (c(4\mu + 3) - a(4\mu + 3)) &= -(3\mu + 3). \end{aligned}$$

Reordering the intervals as I_6, I_4, I_2 and I_3, I_1, I_5 and using a regular "jump" of $-(3\mu + 3)$, with the jump of $6\mu + 2$ between $\alpha = 2\mu + 1$ and $\alpha = 5\mu + 2$, being the exception, we have the difference $3\mu + 2$ twice and the difference 0 omitted, thus $\{c(\alpha) - a(\alpha) \mid 0 \le \alpha \le 6\mu + 3\} = (\mathbb{Z}_{6\mu+4} \setminus \{0\}) \cup \{3\mu + 2\}$ with repetition retained.

For $c(\alpha) - b(\alpha)$, we note that

$$\begin{aligned} c(0) - b(0) &= 3\mu + 2, \\ c(3\mu + 1) - b(3\mu + 1) &= -1, \end{aligned}$$

and so the values of $c(\alpha) - a(\alpha)$ on the subinterval $I_1 \cup I_2 \cup I_3$ cover the set $\{3\mu + 2, \ldots, -1\}$. Also

$$\begin{aligned} c(3\mu + 2) - b(3\mu + 2) &= 1, \\ c(6\mu + 3) - b(6\mu + 3) &= 3\mu + 2, \end{aligned}$$

and so the values of $b(\alpha) - c(\alpha)$ on the subinterval $I_4 \cup I_5 \cup I_6$ cover the set $\{3\mu + 2, \ldots, 6\mu - 1\}$. Consequently $\{b(\alpha) - c(\alpha) \mid 0 \le \alpha \le 6\mu + 3\} = ([6\mu + 4] \setminus \{0\}) \cup \{3\mu + 2\}$ with repetition retained.

3.4 Infinite families

The construction of Theorem 5 constructs sets of three MNOLS of orders $10, 22, 34, 46$ mod 48. The construction of Corollary 2 constructs sets of three MNOLS of orders $8, 40$ mod 48. Combined with the constructions of [6], there is a construction of three MNOLS for $8, 10, 14, 22, 34$, $38, 40, 46$ mod 48. There are infinite families constructed from Corollary 1 and from results of Li and van Rees [10], but these cannot be described mod 48.

4 The spectrum for sets of 3 mutually nearly orthogonal Latin squares

In 2007, Li and van Rees [10] continued the study of 3-MNOLS(n) conjecturing that they exist for all even $n \geq 6$. Here we make a slightly stronger conjecture.

Conjecture 1 There exists DCA$(4, 2p + 1; 2p)$ satisfying **P1** and **P2** for all positive integers $p \geq 3$.

In a partial solution, Li and van Rees proved the existence for orders less than 22 and orders greater than 356, (see also [11]).

Theorem 6 *[10, Thm 4.8] If* $2p \geq 358$*, then there exists a* 3*-MNOLS*$(2p)$*.*

This work was extended in 2014, when Demirkale, Donovan and Khodkar [6] developed further constructions for cyclic DCA$(4, 2p + 1; 2p)$ proving:

Theorem 7 *[6] There exist* 3*-MNOLS*$(2p)$*, where* $2p \equiv 14$, 22, 38, 46 mod 48*.*

The next result lists known values for cyclic DCA$(4, 2p + 1; 2p)$ satisfying **P1** and **P2**, with $2p \leq 356$.

Lemma 7 *There exists cyclic DCA*$(4, 2p+1; 2p)$ *for* $2p \in \{6, 8, \ldots, 20, 22, 38, 46, 62, 70, 86, 94, 110, 118, 134, 142, 158, 166, 182, 190, 206, 214, 230, 238, 254, 262, 278, 286, 302, 310, 326, 334, 350\}$*.*

Proof The existence of orders 6 and 8 was given in [12] and orders 10, 12, 14, 16, 18, 20 in [10]. All the remaining cases were shown to exist in [6].

van Rees recently summarised these results and indicated that 3-MNOLS($2p$) exist for all orders except possibly those given below.

Lemma 8 *[14] A set of* 3*-MNOLS*$(2p)$ *exists except possibly when* $2p \in \{24, 26, 28, 30, 34, 36, 42, 50, 52, 54, 58, 66, 74, 82, 92, 102, 106, 114, 116, 122, 124, 130, 138, 146, 148, 170, 172, 174, 178\}$*.*

In this section we show that 3-MNOLS($2p$) exist for all even orders except possibly $2p = 146$. For completeness we list all values less than $2p = 358$ and, given the connection with row complete Latin squares, where possible we will use cyclic difference covering arrays to construct the Latin squares. We begin this section by reviewing relevant results from [7], [16] and [17], and adapting these to construct cyclic DCA$(4, 2m + 1; 2m)$ that satisfy **P1** and **P2**.

We begin with the following straightforward result that is analogous to [7, Lem 2.3].

Lemma 9 *Suppose that there exists a HDM$(k, n; h)$ over the group $(G, +)$ with a hole over the subgroup H. Further suppose there exists a DCA$(k, h+1; h)$ over H satisfying* **P1** *and* **P2**. *Then there exists a DCA$(k, n + 1; n)$ over G satisfying* **P1** *and* **P2**. *Further suppose that the HDM$(k, n; h)$ and DCA$(k, h+1; h)$ are cyclic. Then there exists a cyclic DCA$(k, n+1; n)$ satisfying* **P1** *and* **P2**.

Proof In the cyclic case, let $A = [a(i, j)]$ $(0 \le i \le n - 1 - h,\ 0 \le j \le k - 1)$ represent the cyclic HDM$(k, n; h)$ and $B = [b(i, j)]$ $(0 \le i \le h,\ 0 \le j \le k - 1)$ represent the cyclic DCA$(k, h + 1; h)$. The definition of cyclic implies that $H = \{0, u, 2u, \ldots (h - 1)u\}$, where $n = uh$, and Lemma 1 implies that h is even and the repeated difference in $\Delta_{j,j'}$, $j \ne k - 1 \ne j'$, of B is $hu/2 = n/2$.

Set $Q = [q(i, j)]$ $(0 \le i \le n,\ 0 \le j \le k)$ to be the concatenation of A with an isomorphic copy of B and we obtain a cyclic DCA$(k, n+1; n)$ that satisfies **P1** and **P2**.

The non-cyclic case follows similarly.

Next we give a general product type construction taken from [7] and adapt it to construct cyclic difference covering arrays that satisfy **P1** and **P2**.

Lemma 10 *[7, Lem 2.6] If both a cyclic HDM$(k, n; h)$ and a cyclic DM$(n', k; 1)$ exist, then so does a cyclic HDM$(k, nn'; hn')$. In particular, if there exists a cyclic DM$(n, k; 1)$ and a cyclic DM$(n', k; 1)$ then there exists cyclic DM$(nn', k; 1)$.*

The first statement of Lemma 10 coupled with Lemma 9 leads to the following straightforward result.

Corollary 3 *Suppose that there exists a cyclic HDM$(k, n; h)$, a cyclic DM$(n', k; 1)$ and a cyclic DCA$(k, hn' + 1; hn')$ that satisfies* **P1** *and* **P2**. *Then there exists a cyclic DCA$(k, nn' + 1; nn')$ that satisfies* **P1** *and* **P2**.

The second statement of Lemma 10 can also be adapted.

Lemma 11 *Suppose a cyclic DM$(n, k; 1)$, a cyclic DM$(n', k; 1)$ and a cyclic DCA$(k, n' + 1; n')$ satisfying* **P1** *and* **P2** *exist. Then there exists a cyclic DCA$(k, nn' + 1; nn')$ that satisfies* **P1** *and* **P2**.

Proof This result can be obtained by taking a hole of size 1 in Corollary 3.

This result can be generalised to construct non-cyclic difference covering arrays as in [16].

We now combine these results with various results of [5], [7] and [17] to obtain results for cyclic DCA$(4, 2p + 1; 2p)$, satisfying **P1** and **P2**, implying new existence results for row complete 3-MNOLS$(2p)$, where $2p < 358$. In the lists below $*$ indicates that the existence of 3-MNOLS$(2p)$ was previously unknown.

In doing this we will settle the remaining cases in Lemma 8, with the exception of $2p = 146$. Here we believe that there exists a DCA$(4, 147; 146)$ satisfying **P1** and **P2** but have been unable to verify it.

Theorem 8 *[5, Thm 17.6, p 411] If n is a prime greater than or equal to k, then there exists a cyclic DM$(n, k; 1)$.*

Lemma 12 *[17, Lem 2.5] Let $n \geq 5$ be prime. Then there exists a cyclic HDM$(4, 2n; 2)$.*

Lemma 13 *There exists a cyclic DCA$(4, 2p + 1; 2p)$ for $2p = 50^*$, 98, 170^*, 242, 290, 338.*

Proof Corollary 3 together with Theorem 8 and Lemma 12 can be used first to construct a cyclic HDM$(4, 2p; h)$ with $2p(h) = 50(10), 98(14), 170(10), 242(22), 290(10), 338(26)$ and then the required DCA$(4, 2p + 1; 2p)$.

Lemmas 15, 16, 17 do not document any new existence results, however they do verify that for the given orders cyclic DCA$(4, 2p+1; 2p)$ satisfying **P1** and **P2** exist.

Lemma 14 *[17, Thm 2.1] Let n be an odd positive integer satisfying gcd$(n, 9) \neq 3$. Then there exists a cyclic HDM$(4, 2n; 2)$.*

Lemma 15 *There exists a cyclic DCA$(4, 2p + 1; 2p)$ for $2p = 90$, 126, 198, 234, 306, 342.*

Proof Corollary 3 together with Theorem 8 and Lemma 14 can be used first to construct a cyclic HDM$(4, 2p; h)$ with $2p(h) = 90(10)$, $126(14)$, $198(22)$, $234(26)$, $306(34)$, $342(38)$ and then the required DCA$(4, 2p + 1; 2p)$.

Theorem 9 *[17, Thm 2.3] Let $n \geq 4$ and $n = 2^\alpha 3^\beta p$, where p is coprime to 6 and $(\alpha, \beta) \neq (1, 0)$. Then there exists a cyclic HDM$(4, 2n; 2)$.*

Lemma 16 *There exists cyclic DCA$(4, 2p + 1; 2p)$ for $2p = 60$, 80, 84, 100, 112, 120, 132, 156, 160, 168, 176, 180, 204, 208, 224, 228, 240, 252, 264, 272, 276, 300, 304, 312, 320, 336, 352.*

Proof Corollary 3 together with Theorem 8 and Theorem 9 can be used first to construct a cyclic HDM$(4, 2p; h)$ with $2p(h) = 60(10)$, $80(10)$, $84(14)$, $100(10)$, $112(14)$, $120(10)$, $132(22)$, $156(26)$, $160(10)$, $168(14)$, $176(22)$, $180(10)$, $204(34)$, $208(26)$, $224(14)$, $228(38)$, $240(10)$, $252(14)$, $264(22)$, $272(34)$, $276(46)$, $300(10)$, $304(38)$, $312(26)$, $320(10)$, $336(14)$, $352(22)$ and then the required DCA$(4, 2p + 1; 2p)$.

Theorem 10 *[17, Thm 2.4] Let n be coprime to 6. Then there exists a cyclic $HDM(4, 4n; 4)$.*

Lemma 17 *There exists a cyclic $DCA(4, 2p+1; 2p)$ for $2p =$ 140, 196, 220, 260, 308, 340.*

Proof Corollary 3 together with Theorem 8 and Theorem 10 can be used first to construct a cyclic HDM$(4, 2p; h)$ with $2p(h) = 140(28)$, $196(28)$, $220(20)$, $260(20)$, $308(28)$, $340(20)$ and then the required DCA$(4, 2p+1; 2p)$.

Theorem 11 *[7, Thm 3.10] A cyclic $DM(3^i, 5; 1)$ exists for all $i \geq 3$.*

Lemma 18 *There exists a cyclic $DCA(4, 2p+1; 2p)$ for $2p =$ 216, 270, 324.*

Proof Corollary 3 together with Theorem 11 and Theorem 9 can be used to first construct a cyclic HDM$(4, 2p; h)$ with $2p(h) = 216(54)$, $270(54)$, $324(54)$ and then the required DCA$(4, 2p+1; 2p)$.

The next result from Yin's paper [17] is interesting in that it allows us to construct difference covering arrays and so mutually nearly orthogonal Latin squares of order $6n$, and gives many values that were previously unresolved (the obstruction was the non-existence of MOLS of order 6).

Theorem 12 *[17, Thm 2.2] Let n be coprime to 6. Then there exists a cyclic $HDM(4, 6n; 6)$.*

Corollary 4 *Let n be an integer of the form $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$, where $\alpha_i \geq 0$ and the prime factors $p_i \geq 5$ for $1 \leq i \leq t$. Then there exists a cyclic $DCA(4, 6n+1; 6n)$ satisfying* **P1** *and* **P2***. Consequently, there exists a cyclic $DCA(4, 2p+1; 2p)$ for $2p = 30^*, 42^*, 66^*, 78, 102^*, 114^*, 138^*, 150, 174^*, 186, 210, 222, 246, 258, 282, 294, 318, 330, 354$.*

The following result can be verified using direct constructions given in Section 3.

Lemma 19 *There exists a cyclic $DCA(4, 2p+1; 2p)$ for $2p = 26^*$, 266, $2p =$ 40, 56, 88, 104, 136, 152, 184, 200, 232, 248, 280, 296, 328, 344 and $2p = 34^*$, 58^*, 82^*, 106^*, 130^*, 154, 178^*, 202, 226, 250, 274, 298, 322, 346.*

Proof Corollary 1 verifies the existence of cyclic DCA$(4, 2p+1; 2p)$ with $2p = 26^*, 266$.

Corollary 2 verifies the existence of cyclic DCA$(4, 2p+1; 2p)$ with $2p =$ 40, 56, 88, 104, 136, 152, 184, 200, 232, 248, 280, 296, 328, 344.

Theorem 5 verifies the existence of cyclic DCA$(4, 2p+1; 2p)$ with $2p = 34^*, 58^*, 82^*, 106^*, 130^*$, 154, 178^*, 202, 226, 250, 274, 298, 322, 346.

Lemma 20 *There exists a cyclic $DCA(4, 2p+1; 2p)$ for $2p = 24^*, 28^*$, 32, 36^*, 44, 48, 52^*, 54^*.*

Proof These results have been verified by computer searches. The first column of the DCA$(4, 2p+1, 2p)$ is given by $[0, 1, 2, \ldots, 2p-1]$, the second column by $[1, 3, \ldots, 2p-1, 2, 4, \ldots, 2p-2]$ and the third column by
$2p = 24$: [2, 0, 3, 1, 14, 21, 20, 19, 23, 15, 6, 18, 16, 10, 17, 8, 11, 22, 5, 13, 4, 9, 7, 12]
$2p = 28$: [2, 0, 3, 1, 11, 16, 22, 25, 20, 23, 4, 8, 21, 5, 18, 10, 19, 13, 24, 27, 7, 26, 15, 9, 6, 14, 17, 12]
$2p = 32$: [2, 0, 3, 6, 1, 13, 22, 30, 21, 25, 28, 26, 7, 5, 23, 20, 12, 10, 24, 17, 31, 15, 29, 27, 11, 14, 4, 9, 8, 19, 18, 16]
$2p = 36$: [5, 35, 13, 20, 11, 9, 1, 31, 10, 2, 30, 33, 4, 34, 32, 25, 28, 16, 27, 22, 3, 29, 19, 24, 18, 15, 6, 23, 17, 7, 0, 8, 14, 12, 21, 26]
$2p = 44$: [39, 13, 26, 21, 35, 3, 17, 16, 40, 28, 38, 25, 6, 10, 34, 5, 18, 30, 43, 15, 19, 36, 7, 24, 32, 14, 4, 0, 31, 12, 2, 9, 23, 37, 11, 42, 41, 29, 20, 1, 33, 27, 8, 22]
$2p = 48$: [5, 41, 23, 40, 1, 39, 34, 25, 28, 8, 4, 9, 21, 30, 43, 18, 12, 2, 42, 45, 32, 37, 33, 0, 26, 15, 13, 22, 10, 35, 44, 7, 36, 16, 27, 19, 46, 38, 3, 47, 31, 29, 17, 14, 11, 24, 20, 6]
$2p = 52$: [18, 12, 50, 37, 16, 6, 45, 4, 31, 34, 47, 21, 29, 2, 5, 22, 38, 3, 39, 27, 0, 15, 51, 7, 28, 24, 42, 40, 48, 32, 9, 26, 20, 11, 1, 41, 19, 35, 43, 13, 49, 33, 14, 17, 46, 8, 36, 23, 10, 30, 25, 44]
$2p = 54$: [6, 5, 31, 27, 20, 38, 19, 4, 30, 51, 3, 52, 49, 14, 48, 23, 41, 12, 25, 0, 32, 40, 21, 50, 9, 45, 16, 1, 46, 11, 28, 42, 47, 35, 39, 2, 22, 13, 34, 33, 24, 44, 15, 53, 7, 17, 37, 36, 26, 18, 10, 43, 29, 8].

For the remaining values 64, 68, 72, 74, 76, 92, 96, 108, 116, 122, 124, 128, 144, 146, 148, 162, 164, 172, 188, 192, 194, 212, 218, 236, 244, 256, 268, 284, 288, 292, 314, 316, 332, 348, 356 we were unable to construct cyclic difference covering arrays however for completeness and to answer questions about the spectrum we give full details verifying existence. It should be noted that it is possible to construct DCA$(4, 2p+1; 2p)$ satisfying **P1** and **P2** for some of these orders however our construction does not give cyclic difference covering arrays and so the details have been omitted here.

To verify existence of certain sizes of DCA we require two more results. The second result uses group divisible designs: A $\mathcal{K}$-*group divisible design* of *type* $g_1^{a_1} g_2^{a_2} \ldots g_s^{a_s}$ is a partition $\mathcal{G}$ of a finite set $\mathcal{V}$, of cardinality $v = \sum_{i=1}^{s} a_i g_i$, into a_i *groups* of size g_i, $1 \leq i \leq s$, together with a family of subsets (*blocks*) $\mathcal{B}$ of $\mathcal{V}$ such that: 1) if $B \in \mathcal{B}$, then $|B| \in \mathcal{K}$, 2) every pair of distinct elements of $\mathcal{V}$ occurs in 1 block of $\mathcal{B}$ or 1 group of $\mathcal{G}$ but not both, and 3) $|\mathcal{G}| > 1$.

Theorem 13 *[10, Thm 4.1] Suppose there exists a k-MNOLS$(2p)$, a k-MOLS$(2p)$, and a k-MOLS(n). Then there exists a k-MNOLS$(2pn)$.*

Theorem 14 *[10, Thm 4.5] Suppose there exists a $\mathcal{K}$-GDD of type $g_1^{a_1} \ldots g_s^{a_s}$. Further suppose that for any group size g_i there exists a s-MNOLS(g_i) and for any block size $k \in \mathcal{K}$ there exists a s-IMOLS(k). Then there are s-MNOLS(t), where $t = \sum_{i=1}^{s} a_i g_i$.*

Lemma 21 *There exists a* 3-*NMOLS*$(2p)$ *for* $2p = 76$, 92^*, 96, 108, 116^*, 124^*, 128, 144, 148^*, 164, 172^*, 188, 192, 212, 236, 244, 256, 268, 284, 288, 292, 316, 332, 348 *and* 356*.*

Proof The 3-MNOLS$(2p)$, $2p = 76(12^5 16^1), 92(20^4 12), 96(16^5 16^1), 108(20^5 8^1), 116(20^5, 16), 124(20^5 24^1), 128(24^5 8^1), 144(24^5 24^1), 148(24^5 28), 164(28^5 24^1), 172(32^5 12), 188(32^5 28^1), 192(32^5 36^1), 212(36^5 32^1), 236(40^5 36^1), 244(40^5 44^1), 256(44^5 36^1), 268(44^5 48^1), 284(48^5 44^1), 288(48^5 48^1), 292(48^5 52^1), 316(52^5 56^1), 332(56^5 52^1), 348(56^5 68^1)$ and $356(60^5 56^1)$ can be constructed applying 5-GDD, that exist by [5, Thm 4.17, p 258], in Theorem 14. Here the bracketed information gives the type of the GDD.

Lemma 22 *There exists a* 3-*NMOLS*$(2p)$ *for* $2p = 64$, 68, 72, 74^*, 122, 162, 194, 218 *and* 314*.*

Proof 3-NMOLS$(2p)$ for $2p = 64$, 68, 72, 74^*, 122, 162, 194 and 218 can be constructed by applying, respectively, 8-GDD(8^8), $\{7, 8, 9\}$-GDD$(8^7 6^2)$, 9-GDD(8^9), $\{7, 8, 9\}$-GDD$(8^7 6^3)$, $\{7, 8\}$-GDD$(16^7 10^1)$, $\{11, 12, 13\}$-GDD$(12^{12} 10^1 8^1)$, $\{11, 12, 13\}$-GDD$(16^{11} 10^1 8^1)$, $\{13, 14\}$-GDD$(16^{13} 10^1)$ and $\{8, 9, 10, 11\}$-GDD$(32^8 14^2 10^1)$ in Theorem 14. All of the required group divisible designs exist by the standard finite field constructions for MOLS.

All the results of this paper combine to the following theorem.

Theorem 15 *There exists a* 3-*MNOLS*$(2p)$ *for each positive integers* $p \geq 3$*, except possibly* $p = 73$*.*

This leaves us tantalisingly close to Conjecture 1.

References

1. S.T. Bate, J. Boxall, The construction of multi-factor crossover designs in animal husbandry studies, Pharmaceutical Statistics **7** (2008) 179–194.
2. Bate, Simon T and Clark, Robin A, The Design and Statistical Analysis of Animal Experiments, Cambridge University Press, 2014.
3. D.M. Cohen, S.R. Dalal, M.L. Fredman, G.C. Patton, The AETG system: an approach to testing based on combinatorial designs, IEEE Trans Software Eng **23** (1997) 437–444.
4. D.M. Cohen, S.R. Dalal, J. Parelius, G.C. Patton, The combinatorial design approach to automatic test generation, IEEE Trans Software **13** (1996) 83–88.
5. C.J. Colbourn, J.H. Dinitz, (Eds.), Handbook of combinatorial designs, Second Edition. Chapman & Hall/CRC, Boca Raton, FL, 2006. press, 2010.
6. F. Demirkale, D. Donovan, A. Khodkar, Direct constructions for general families of cyclic mutually nearly orthogonal Latin squares, Journal of Combinatorial Designs, **23** (2015) 195-203.
7. G. Ge, On $(g, 4; 1)$-difference matrices, Discrete Mathematics **301** (2005) 164–174.
8. A.S. Hedayat, N.J.A. Sloane, J. Stufken, Orthogonal Arrays: Theory and Applications. Springer, New York, 1999.
9. J. Korner, M. Lucertini, Compressing inconsistent data, IEEE Trans. Inform. Theory **40** (1994) 706-715.
10. P.C. Li, G.H.J. van Rees, Nearly orthogonal Latin squares, Journal of Combinatorial Mathematics and Combinatorial Computing **62** (2007) 13–24.

11. E.B. Pasles, D. Raghavarao, Mutually nearly orthogonal Latin squares of order 6, Utilitas Mathematica **65** (2004) 65–72.
12. D. Raghavarao, S.S. Shrikhande, M.S. Shirkhande, Incidence matrices and inequalities for combinatorial designs, Journal of Combinatorial Designs **10** (2002) 17–26.
13. D.R. Stinson, Combinatorial characterizations of authentication codes, Designs, Codes and Cryptography **2** (1992) 175–187
14. G.H.J. van Rees, Private Communication (2014).
15. E.J. Williams, Experimental designs balanced for the estimation of residual effects of treatments, Australian Journal of Scientific Research **2** (1949) 149–168.
16. J. Yin, Construction of difference covering arrays, Journal of Combinatorial Theory, Series A **104** (2003) 327–339.
17. J. Yin, Cyclic difference packing and covering arrays, Designs, Codes and Cryptography **37** (2005) 281–292.