Received: 22 December 2016 | Revised: 8 January 2019 | Accepted: 8 January 2019

DOI: 10.1002/jcd.21647

WILEY

RESEARCH ARTICLE

The enumeration of cyclic mutually nearly orthogonal Latin squares

Fatih Demirkale[1] | **Diane M. Donovan**[2] | **Janne I. Kokkala**[3] | **Trent G. Marbach**[4,5]

[1]Department of Mathematics, Yıldız Technical University, Esenler, Istanbul, Turkey

[2]School of Mathematics and Physics, Centre for Discrete Mathematics and Computing, University of Queensland, St Lucia, Brisbane, Queensland, Australia

[3]Department of Communications and Networking, School of Electrical Engineering, Aalto University, Espoo, Finland

[4]School of Mathematics and Physics, University of Queensland, St Lucia, Brisbane, Queensland, Australia

[5]School of Mathematical Sciences, Monash University, Clayton, Melbourne, Victoria, Australia

Correspondence
Trent G. Marbach, School of Mathematics and Physics, University of Queensland, St Lucia, Brisbane, Queensland 4072, Australia.
Email: trent.marbach@gmail.com

Funding information
Academy of Finland, Grant/Award Number: Project #289002; Monash eResearch Centre; eSolutions-Research Support Services

Abstract

In this paper, we study collections of mutually nearly orthogonal Latin squares (MNOLS), which come from a modification of the orthogonality condition for mutually orthogonal Latin squares. In particular, we find the maximum μ such that there exists a set of μ cyclic MNOLS of order n for $n \leq 18$, as well as providing a full enumeration of sets and lists of μ cyclic MNOLS of order n under a variety of equivalences with $n \leq 18$. This resolves in the negative a conjecture that proposed that the maximum μ for which a set of μ cyclic MNOLS of order n exists is $\lceil n/4 \rceil + 1$.

KEYWORDS

latin square, MNOLS, nearly orthogonal

1 | INTRODUCTION

The study of mutually orthogonal Latin squares (MOLS) is a subject that has attracted considerable attention. Such interest has been stimulated by the relevance of the field, with applications in error correcting codes, cryptographic systems, affine planes, compiler testing, and statistics (see [9]). Although, as is well known, there exists a set of $n - 1$ MOLS of order n

when n is a prime or a prime power, the largest number of MOLS of order n known to exist when n is composite is generally much smaller and such sets of MOLS are generally hard to find. Well-known examples of these facts are that there do not exist two MOLS of order 6, and it is unknown whether three MOLS of order 10 exist or not.

Formally, a *Latin square* of order n is an $n \times n$ array in which the n distinct symbols $\{0, ..., n-1\}$ are arranged so that each symbol occurs once in each row and once in each column. We index the rows and columns by $\{0, ..., n-1\}$. For a Latin square L of order n, we may write $(r, c, e) \in L$ to mean that L has a cell in row r and column c that contains symbol e. We assume that the three components of such a triple are taken mod n, so that $(r, c, e+n) = (r, c+n, e) = (r+n, c, e)$. The notation $(r, c, e) \in L$ is known as orthogonal array notation. We also write $L(r, c) = e$ when $(r, c, e) \in L$. A pair of Latin squares L_1, L_2 of order n are called *orthogonal* if the superimposition of L_1 and L_2 contains each ordered pair of symbols exactly once. A set of μ Latin squares are *mutually orthogonal* if they are pairwise orthogonal, and we refer to such a set as a *set of* MOLS.

Based upon the significance and usefulness that is exhibited in the study of MOLS, Raghavarao et al [17] introduced a modification to the definition of orthogonality to overcome restrictions for the case that n is a composite number that is even. A pair of Latin squares L_1, L_2 of even order n is called *nearly orthogonal* if the superimposition of L_1 and L_2 contains each ordered pair of symbols (ℓ, ℓ') exactly once, except in the case $\ell = \ell'$, where no such pair occurs, and in the case $\ell \equiv \ell' + n/2 \pmod{n}$, where such pairs occur twice. We consider collections of μ Latin squares of order n that are pairwise nearly orthogonal, which are denoted as collections of μ mutually nearly orthogonal Latin squares (MNOLS) of order n. Traditionally, these collections are unordered sets, although we will also consider ordered lists.

An *orderly algorithm* is a way of generating all examples of some combinatorial object, such that all equivalence classes appear in the generation, but during the generation, no two objects constructed are equivalent. This technique is typically attributed to [5] and [18]. A similar technique, called canonical augmentation [11], has been used to generate Latin rectangles by augmenting a row at a time (see also [8,14]). This is not the only method of enumerating Latin rectangles, and a variety of enumerative techniques have been applied to solve it (see [15] and the citations contained within). Recently, this work has lead to the enumeration of MOLS for order less than or equal to 9 [4]. In a similar vein, we will perform an orderly algorithm that generates collections of μ cyclic MNOLS of order n under certain equivalences. See [7] for a general reference on this kind of enumeration problem.

The pioneering work [17] on sets of μ MNOLS of order n investigated an upper bound on μ when n is fixed, and they showed that if there exists a set of μ MNOLS of order n, then $\mu \leq n/2 + 1$ for $n \equiv 2 \pmod{4}$ and $\mu \leq n/2$ for $n \equiv 0 \pmod{4}$. In the case that a set of μ MNOLS of order n obtains this bound, it is called a complete set of μ MNOLS of order n. They proceeded to explore the existence of sets of μ MNOLS of order n by investigating sets of μ cyclic MNOLS of order n; that is, each Latin square L has $L(r, c+1) \equiv L(r, c) + 1 \pmod{n}$ for all $r, c \in [0, n-1]$, recalling that the entries are taken mod n. The sets of μ MNOLS of order n that were found included single examples of sets of two cyclic MNOLS of order 4, sets of three cyclic MNOLS of order 6, and sets of three cyclic MNOLS of order 8, demonstrating that the bound is tight for $n = 4$. It was later shown [16] that there does not exist a set of four MNOLS of order 6, and so the bound is not tight for $n = 6$.

Further results [10] showed sets of three MNOLS of order n exist for even $n \geq 358$. The work in [10] also introduced a concept of equivalence between sets of μ cyclic MNOLS of order n called isotopic equivalence (details in Section 2). They found a number of isotopically

TABLE 1 The number of sets of μ MNOLS of order n under isotopic equivalence

n	6	8	10	12
$\mu = 3$	1	1	≥1	>1
$\mu = 4$	0	0	1	>1
$\mu = 5$	0	0	0	0

nonequivalent sets of μ cyclic MNOLS of order n for $n \leq 12$. The number of these sets of μ cyclic MNOLS of order n is given in Table 1.

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

1	2	3	0
3	0	1	2
0	1	2	3
2	3	0	1

A pair of Latin squares of order 4 that are nearly orthogonal.

The literature surrounding the search for the existence of sets of three cyclic MNOLS has been documented in [1,2]. These documents also gave further constructions that verified the existence of a set of three MNOLS of order n for all even $n \geq 6$, except perhaps when $n = 146$.

In the current paper, we find the maximum μ such that there exists a set of μ cyclic MNOLS of order n for $n \leq 18$ and provide a full enumeration of sets and lists of μ cyclic MNOLS of order n under a variety of equivalences with $n \leq 18$. This will resolve in the negative a conjecture of [10] that proposed the maximum μ for which a set of μ cyclic MNOLS of order n exists is $\lceil n/4 \rceil + 1$ (the maximum μ appears erroneously as $\lceil n/8 \rceil + 1$ in the original conjecture [19], and the maximum value we have written was the intended conjecture).

2 | FURTHER DEFINITIONS

A (μ, n)-difference set is a set of n μ-tuples $\{(a_k^1, ..., a_k^\mu) | 1 \leq k \leq n\}$ over the alphabet $\{0, ..., n-1\}$ in which $a_k^i \neq a_l^i$ for all $1 \leq k, l \leq n$ and $1 \leq i \leq \mu$, and the multiset of ordered differences modulo n between elements in two positions i, j, that is $\{a_k^i - a_k^j \pmod n | 1 \leq k \leq n\}$, does not contain 0, contains $n/2$ twice, and contains every other difference once [10]. We can define μ Latin squares, A_i, that form a collection of μ cyclic MNOLS of order n from a (μ, n)-difference set by defining the cells of the first columns as $A_i(r, 0) = a_r^i$ and each cell in subsequent columns by adding 1 (mod n) to the symbol of the corresponding cell in the previous column. It is also clear that this process is reversible, so a list of μ cyclic MNOLS of order n can be used to construct a (μ, n)-difference set.

We will enumerate both ordered lists and unordered sets of μ cyclic MNOLS of order n. A *set of* μ MNOLS of order n is a set $\{L_1, ..., L_\mu\}$ such that L_i, L_j are nearly orthogonal for $1 \leq i, j \leq \mu$, $i \neq j$. A *list of* μ MNOLS of order n is an ordered list $(L_1, ..., L_\mu)$ such that L_i, L_j are nearly orthogonal for $1 \leq i, j \leq \mu$, $i \neq j$. This distinction will be important when we enumerate collections of μ MNOLS of order n. We will write *collection* when a statement holds for either a list or set. A list of μ MNOLS of order n $(L_1, ..., L_\mu)$ is *reduced* if L_1 has its first row and column in natural order, that is, $(0, i, i), (i, 0, i) \in L_1$ for $i \in \{0, ..., n-1\}$.

TABLE 2 The number of collections of μ cyclic MNOLS of order n under set-isotopy equivalence

n	4	6	8	10	12	14	16	18
$\mu = 2$	1	2	9	68	1140	19 040	489 296	28 303 688
$\mu = 3$	0	1	1	73	4398	429 111	70 608 753	31 992 833 620
$\mu = 4$	0	0	0	1	2	117	14 672	8 354 783
$\mu = 5$	0	0	0	0	0	0	0	0

TABLE 3 The number of collections of μ cyclic MNOLS of order n under set-reduced equivalence

n	4	6	8	10	12	14	16	18
$\mu = 2$	2	12	136	2340	52 608	1 589 056	62 516 224	3 056 224 608
$\mu = 3$	0	6	16	2920	211 104	36 031 716	9 037 728 896	3 455 226 014 904
$\mu = 4$	0	0	0	20	96	8 638	1 870 592	902 182 968
$\mu = 5$	0	0	0	0	0	0	0	0

TABLE 4 The number of collections of μ cyclic MNOLS of order n under list-isotopy equivalence

n	4	6	8	10	12	14	16	18
$\mu = 2$	1	3	12	128	2224	38 000	977 696	56 603 408
$\mu = 3$	0	2	6	438	26 388	2 574 306	423 652 518	191 957 000 556
$\mu = 4$	0	0	0	12	48	2484	350 730	200 481 924
$\mu = 5$	0	0	0	0	0	0	0	0

TABLE 5 The number of collections of μ cyclic MNOLS of order n under list-reduced equivalence

n	4	6	8	10	12	14	16	18
$\mu = 2$	4	24	256	4640	105 216	3 178 112	125 026 304	6 112 406 016
$\mu = 3$	0	12	96	17 520	1 266 624	216 190 296	54 226 373 376	20 731 356 060 048
$\mu = 4$	0	0	0	480	2304	207 312	44 879 616	21 652 047 792
$\mu = 5$	0	0	0	0	0	0	0	0

3 | CYCLIC MNOLS

We saw previously that a collection of μ cyclic MNOLS of order n can be developed from a (μ, n)-difference set. Each (μ, n)-difference set will correspond to $n!$ distinct lists of μ cyclic MNOLS of order n, depending on which cells of the first column of the list of μ cyclic MNOLS are chosen to be filled with which μ-tuple from the (μ, n)-difference set. This partitions the lists of μ cyclic MNOLS of order n evenly into classes of size $n!$, and so from now, we will enumerate the number of (μ, n)-difference sets under a number of equivalences, and consequentially, we will have enumerated the number of collections of μ cyclic MNOLS of order n.

TABLE 6 The number of collections of two cyclic MNOLS of order 14, by their type and autotopy group sizes

$\lvert Is_s(\mathcal{L})\rvert$	$\lvert Is_l(\mathcal{L})\rvert$	#Type 0	#Type 1	#Total
1	1	3618	15 186	18 804
2	1	0	80	80
2	2	46	88	134
3	3	2	14	16
6	6	1	5	6
	Total	3667	15 373	19 040

TABLE 7 The number of collections of three cyclic MNOLS of order 14, by their type and autotopy group sizes

$\lvert Is_s(\mathcal{L})\rvert$	$\lvert Is_l(\mathcal{L})\rvert$	#Type 0	#Type 1	#Total
1	1	202 382	226 436	428 818
2	2	146	57	203
3	1	24	63	87
6	2	1	2	3
	Total	202 553	226 558	429 111

TABLE 8 The number of collections of four cyclic MNOLS of order 14, by their type and autotopy group sizes

$\lvert Is_s(\mathcal{L})\rvert$	$\lvert Is_l(\mathcal{L})\rvert$	#Type 0	#Type 1	#Total
1	1	67	26	93
2	1	3	8	11
2	2	1	0	1
3	1	4	7	11
6	2	1	0	1
	Total	76	41	117

TABLE 9 The number of collections of two cyclic MNOLS of order 16, by their type and autotopy group sizes

$\lvert Is_s(\mathcal{L})\rvert$	$\lvert Is_l(\mathcal{L})\rvert$	$\lvert Red_s(\mathcal{L})\rvert$	#Type 0	#Type 1	#Total
1	1	1	106 794	380 686	487 480
2	1	1	12	822	834
2	2	1	260	660	920
4	2	1	0	12	12
2	1	2	46	0	46
4	2	2	4	0	4
		Total	107 116	382 180	489 296

TABLE 10 The number of collections of three cyclic MNOLS of order 16, by their type and autotopy group sizes

$\lvert Is_s(\mathcal{L})\rvert$	$\lvert Is_l(\mathcal{L})\rvert$	$\lvert Red_s(\mathcal{L})\rvert$	#Type 0	#Type 1	#Total
1	1	1	36 845 488	33 760 273	70 605 761
2	2	1	2326	666	2992
		Total	36 847 814	33 760 939	70 608 753

TABLE 11 The number of collections of four cyclic MNOLS of order 16, by their type and autotopy group sizes

$\lvert Is_s(\mathcal{L})\rvert$	$\lvert Is_l(\mathcal{L})\rvert$	$\lvert Red_s(\mathcal{L})\rvert$	#Type 0	#Type 1	#Total
1	1	1	11 146	3401	14 547
2	1	1	28	79	107
2	2	1	7	2	9
2	1	2	8	0	8
4	1	4	1	0	1
		Total	11 190	3482	14 672

TABLE 12 The number of collections of two cyclic MNOLS of order 18, by their type and autotopy group sizes

$\lvert Is_s(\mathcal{L})\rvert$	$\lvert Is_l(\mathcal{L})\rvert$	$\lvert Red_s(\mathcal{L})\rvert$	#Type 0	#Type 1	#Total
1	1	1	4 378 529	23 914 135	28 292 664
2	1	1	0	3568	3568
2	2	1	1642	5414	7056
2	1	2	400	0	400
		Total	4 380 571	23 923 117	28 303 688

TABLE 13 The number of collections of three cyclic MNOLS of order 18, by their type and autotopy group sizes

$\lvert Is_s(\mathcal{L})\rvert$	$\lvert Is_l(\mathcal{L})\rvert$	$\lvert Red_s(\mathcal{L})\rvert$	#Type 0	#Type 1	#Total
1	1	1	12 650 027 871	19 342 805 458	31 992 833 329
3	1	1	47	176	223
3	1	3	0	68	68
		Total	12 650 027 918	19 342 805 702	31 992 833 620

Given a (μ, n)-difference set, we may 1) rearrange the order of all μ-tuples simultaneously using the same rearrangement on all μ-tuples; 2) multiply all symbols in all μ-tuples of the difference set by a, where $\gcd(a, n) = 1$; 3) add a constant to all symbols in all μ-tuples of the difference set; or any combination of 1), 2), and 3). These operations form a group G that acts on

TABLE 14 The number of collections of four cyclic MNOLS of order 18, by their type and autotopy group sizes

$\lvert \mathrm{Is}_s(\mathcal{L}) \rvert$	$\lvert \mathrm{Is}_l(\mathcal{L}) \rvert$	$\lvert \mathrm{Red}_s(\mathcal{L}) \rvert$	#Type 0	#Type 1	#Total
1	1	1	5 291 250	3 060 794	8 352 044
2	1	1	675	1799	2474
2	1	2	265	0	265
		Total	5 292 190	3 062 593	8 354 783

the set of all (μ, n)-difference sets. Let G_1 be the subgroup of operations of the form 1), G_2 be the subgroup of operations of the form 2), and G_3 be the subgroup of operations of the form 3). We can think of the elements of G as group actions that take a (μ, n)-difference set and a group element and produce another (μ, n)-difference set. The actions 2 and 3 are symmetry operations for difference sets (see [6]).

Two (μ, n)-difference sets are *set-isotopic* if one can be obtained from the other using the group actions in G, *list-isotopic* if one can be obtained from the other using group actions in both G_2 and G_3, *set-reduced-equivalent* if one can be obtained from the other using group actions in G_1, and *list-reduced-equivalent* if they are identical as sets.

For a given (μ, n)-difference set, $\mathcal{D}$, the set of all (μ, n)-difference sets set-isotopic to $\mathcal{D}$ is called its *set-isotopy class*. We similarly define the *list-isotopy class, set-reduced class*, and *list-reduced class*. We let C_n^μ denote a set of (μ, n)-difference sets that contains precisely one representative from each set-isotopy class.

We define $\mathrm{Is}_s(\mathcal{L})$ to be the set of group actions of G that fixes $\mathcal{L}$. Similarly, we define $\mathrm{Is}_l(\mathcal{L})$, $\mathrm{Red}_s(\mathcal{L})$, and $\mathrm{Red}_l(\mathcal{L})$, respectively.

Two sets of μ MNOLS of order n are *isotopic* if permuting the rows, columns, and symbols consistently among all Latin squares in one set yields the other set.

Lemma 3.1. *Two sets of μ cyclic MNOLS of order n are isotopic if and only if their two corresponding (μ, n)-difference sets are also set-isotopic.*

Proof. The reverse direction is trivial, as we can change the rows and symbols between the MNOLS in the same way as the rows and symbols were changed between the (μ, n)-difference sets. Some columns may need to be swapped, but this is easily seen.

For the forward direction, let the two Latin squares be $L = [\ell_{ij}]$ and $L' = [\ell'_{ij}]$. Consider that the difference $\ell'_{ij} - \ell_{ij}$ is the same for each j when we fix i. This means a permutation of the symbols will send the pairs of symbols with difference 1 to pairs of symbols of some constant difference x. The only way this can happen is if the permutation is of the form $i \mapsto xi + j$ with $\gcd(x, n) = 1$. A permutation of the rows will have no effect on the corresponding (μ, n)-difference sets, and any permutation of the columns is fixed by the permutation of the symbols (except for trivial cyclic shifts, which can be counteracted by changing the permutation of the symbols). ∎

We call a pair of collections of μ cyclic MNOLS of order n set-isotopic (resp. list-isotopic, set-reduced-equivalent, and list-reduced-equivalent) if their corresponding (μ, n)-difference sets

are also set-isotopic (resp. list-isotopic, set-reduced-equivalent, and list-reduced-equivalent). Note that this definition applies only to cyclic MNOLS and not general MNOLS.

The computation in this paper will find the number of (μ, n)-difference sets distinct up to list-isotopy, set-isotopy, list-reduction, and set-reduction for $n \leq 18$ and for each $2 \leq \mu \leq 5$.

Lemma 3.2. *Given $\mathcal{L} \in C_n^\mu$:*

1. *the number of list-isotopy classes within the set-isotopy class of $\mathcal{L}$ is*

$$\mu! \cdot |\mathrm{Is}_l(\mathcal{L})|/|\mathrm{Is}_s(\mathcal{L})|;$$

2. *the number of set-reduced classes within the set-isotopy class of $\mathcal{L}$ is*

$$\phi(n) \cdot n \cdot |\mathrm{Red}_s(\mathcal{L})|/|\mathrm{Is}_s(\mathcal{L})|; \text{ and}$$

3. *the number of list-reduced classes within the set-isotopy class of $\mathcal{L}$ is*

$$\phi(n) \cdot n \cdot \mu! \cdot |\mathrm{Red}_l(\mathcal{L})|/|\mathrm{Is}_s(\mathcal{L})| = \phi(n) \cdot n \cdot \mu!/|\mathrm{Is}_s(\mathcal{L})|.$$

Proof. By the orbit-stabilizer theorem. ∎

4 | CANONICAL FORMS

Given a partition of C_n^μ as $C_n^\mu = \cup_{i=1}^{\alpha} C_i$ with $C_i \cap C_j = \varnothing$ for $1 \leq i < j \leq \alpha$, a *canonical form* is a function $f: C_n^\mu \to C_n^\mu$ such that for all $\mathcal{L}, \mathcal{M} \in C_i$, $f(\mathcal{L}) = f(\mathcal{M})$ and $f(\mathcal{L}) \in C_i$. We will say that the lists within $\mathrm{Im}(f)$ are *canonical*. This allows us to represent each set-isotopy class of (μ, n)-difference sets by a single (μ, n)-difference sets. For Latin squares, there are procedures to find a canonical Latin square among an isotopy class, which usually make use of a program to find a canonical labeling of a graph, with implementations such as nauty [13]. While this is usually a computationally intensive task (having no known polynomial time algorithm), it will not form the bottleneck of the search, and so there is no need for such a sophisticated method. As such, we will take the lexicographically smallest (μ, n)-difference set in a set-isotopy class to be canonical. For (μ, n)-difference sets, we define $\{(k, a_k^2, ..., a_k^\mu)\}$ to be lexicographically smaller than $\{(k, b_k^2, ..., b_k^\mu)\}$ if there exists $k', \mu' \geq 0$ with $(k, a_k^2, ..., a_k^\mu) = (k, b_k^2, ..., b_k^\mu)$ for $1 \leq k < k'$, $a_k^i = b_k^i$ for $2 \leq i < \mu'$, and $a_{k'}^{\mu'} < b_{k'}^{\mu'}$.

5 | ALGORITHMS

There has been a history of errors in the enumeration of Latin squares (this history is described in [12]). As such, it has become standard practice in the enumeration of Latin squares and related structures to enumerate using multiple different methods and check the results are identical. We present an algorithm that completed the enumeration of (μ, n)-difference sets that were unique up to set-isotopism for $\mu \geq 2$ and $n \leq 18$, which includes information about $\mathrm{Is}_l(\mathcal{L})$, $\mathrm{Red}_s(\mathcal{L})$, and $\mathrm{Red}_l(\mathcal{L})$ for each (μ, n)-difference set $\mathcal{L}$. This

information can be used to deduce the number of list-reduced (μ, n)-difference sets. The program also includes a second method to count the number of list-reduced (μ, n)-difference sets by another method, meaning we have a way of verifying the accuracy of our results.

Within our program, we represent a (μ, n)-difference set by the list of columns $(C_1, ..., C_\mu)$, where $(C_1(i), ..., C_\mu(i))$ is an element of our difference set for each $1 \leq i \leq n$. Our algorithm will augment a further index to each element of the (μ, n)-difference set by augmenting a column C to the stored list of columns $(C_1, ..., C_\mu)$. Such a column, say $C_{\mu+1}$, has to satisfy the necessary and sufficient conditions:

1. each symbol in $\{0, ..., n-1\}$ occurs in $C_{\mu+1}$; and
2. the column $C_{\mu+1}$ is nearly orthogonal with all other columns (ie, $\{C_{\mu+1}(k) - C_i(k)\} = \{1, ..., n/2, n/2, ..., n-1\}$).

Let $R = \{r_1, ..., r_n\}$, $S = \{\sigma_1, ..., \sigma_n\}$, and $D_i = \{d_{i0}, ..., d_{i(n-1)}\}$ be pairwise disjoint sets, representing the rows, symbols, and differences of a column we would want to add, with $1 \leq i \leq \mu$. For each cell of C in row r_j containing symbol σ_k, consider the set $\{r_j, \sigma_k, d_{1(C_1(j)-k)}\}$. The collection of such sets, $\mathcal{F}$, when we consider all cells in some potential column must be a partition of the multiset $X = R \cup S \cup \bigcup_{i=1}^{\mu} \{d_{i1}, ..., d_{i\frac{n}{2}}, d_{i\frac{n}{2}}, ..., d_{i(n-1)}\}$. As such, this is an instance of the exact cover problem, and we can therefore use existing software such as LIBEXACT to find all possible columns that may be augmented to our list $(C_1, ..., C_\mu)$ to give a $(\mu + 1, n)$-difference set.

We may assume that the first column is in natural order (row i contains symbol i) and refer to such a column as I. The algorithm begins by generating all columns that could be augmented to this first column using LIBEXACT. In the case that the augmentation between the first column and the augmented second column corresponds to a $(2, n)$-difference set that is canonical, we place the second column into LIST1. For each second column C in LIST1, we again use LIBEXACT to find all columns that may successfully be augmented to (I, C), and we place all such third columns into LIST2. Construct a graph with vertices in LIST2, and edges connecting points C_a and C_b if (C_a, C_b) is a (μ, n)-difference set. Then each clique $(e_1, ..., e_\alpha)$ yields a $(\alpha + 2, n)$-difference set, given by $(I, C, e_1, ..., e_\alpha)$. For each clique, if the generated $(\alpha + 2, n)$-difference set, $\mathcal{L}$, is set-canonical, we calculate $|\mathrm{Red}_s(\mathcal{L})|$, $|\mathrm{Is}_l(\mathcal{L})|$, and $|\mathrm{Is}_s(\mathcal{L})|$ and store this information. After completion, we merge the results and use Lemma 3.2 to find the total number of classes.

Finding cliques is usually a hard problem. This is not an issue for our calculations as the clique size of our problem turns out to be very small. In fact, no cliques of size three existed in our graph, and the computation time to prove this was negligible within our program as a whole.

We used a brute force search over the set-isotopism operators to test canonicality and to calculate $|\mathrm{Red}_s(\mathcal{L})|$, $|\mathrm{Is}_l(\mathcal{L})|$, and $|\mathrm{Is}_s(\mathcal{L})|$. Again, the time required for this operation was negligible.

We also performed our checking step at the point of finding the clique. Each C_1 in LIST1 corresponds to $2\phi(n)n/|\mathrm{Is}_s((I, C_1))|$ list-reduced $(2, n)$-difference sets. Each clique of size $\mu - 2$ has $(\mu - 2)!$ ways of being augmented onto the list (I, C_1), yielding $(\mu - 2)!2\phi(n)n/|\mathrm{Is}_s((I, C_1))|$ list-reduced (μ, n)-difference sets. Summing over each of these values gives the total number of list-reduced (μ, n)-difference sets.

Algorithm 1: Algorithm

input : n;
output: A list with entries being lists of four integers $(\mathrm{Is}_s, \mathrm{Is}_l, \mathrm{Red}_s, count)$, where count is the number of set-isotopy classes of (μ, n)-difference sets $\mathcal{L}$ that have $(|\mathrm{Is}_s(\mathcal{L})|, |\mathrm{Is}_l(\mathcal{L})|, |\mathrm{Red}_s(\mathcal{L})|) = (\mathrm{Is}_s, \mathrm{Is}_l, \mathrm{Red}_s)$;

```
store ← ∅;
LIST1 ← ∅;
for C1 ∈ exactcover(I) do
    LIST1 ← LIST1 ∪ C1
for C1 ∈ LIST1 do
    vert(graph) ← ∅;
    edge(graph) ← ∅;
    LIST2 ← ∅;
    for C2 ∈ exactcover(I, C1) do
        LIST2 ← LIST2 ∪ C2
        vert(graph) ← vert(graph) ∪ C2
    for v1 ∈ LIST2 do
        for v2 ∈ LIST2 do
            if (v1, v2) are a (μ, n)-difference set then
                edge ← edge ∪ {{v1, v2}}
    for all cliques (α1, ..., α_{μ−2}) of size μ − 2 such that
     (I, C1, α1, ..., α_{μ−2}) is set-canonical do
        L ← the (μ, n)-difference set (I, C1, α1, ..., α_{μ−2})
        store ← store.add(Is_s(L), Is_l(L), Red_s(L))
```

6 | RESULTS AND CONCLUSIONS

The counts that were found appear in Tables 2–5. Comparing these results with the previously known cases in Table 1, we see that the new values of particular significance are when $\mu = 3$ and $n \in \{10, 12, 14, 16, 18\}$, when $\mu = 4$ and $n \in \{12, 14, 16, 18\}$, and when $\mu = 5$ and $n \in \{14, 16, 18\}$. The results when $\mu = 5$ disprove Conjecture 5.2 of [10] that proposed the maximum μ for which a set of μ cyclic MNOLS of order n exists is $\lceil n/4 \rceil + 1$, as there does not exist a set of five MNOLS of order 14, 16, and 18 as predicted by the conjecture. (In fact, the conjecture predicted a set of six cyclic MNOLS of order 18.)

For $n = 14$, the search consumed 14 minutes of CPU time and for $n = 16$ the search consumed 77 hours of CPU time, with negligible amounts of memory. As a means of comparison, running a depth first search for set-isotopic classes consumed 20 hours and 154 days of CPU time, respectively, and required 7GB of RAM (to save on repeated computation). The resulting (μ, n)-difference sets are of reasonable size and are provided online for examination and verification [3].

For $n = 18$, the search was conducted independently by two authors, consuming 2337 core-days and 4137 core-days, each with memory usage of only a few megabyte. With this program,

generating the sets of 2MNOLS of order 20 would take approximately 50 core-hours, and there are around $1.1 \cdot 10^9$ set-isotopy classes. For each of those, finding all μ-MNOLS would take approximately 50 core-seconds on average, so the total running time for $n = 20$ would be around 2000 core-years. Note that the times reported here refer to a logical core using hyperthreading; with a single physical core per thread, the core-time would be around 25% smaller.

We say a list of μ cyclic MNOLS of order n is of *type 0* if it is isotopically equivalent to a list of reduced μ cyclic MNOLS of order n, $\mathcal{L} = (L_1, \ldots, L_\mu)$, with $(0, 0, 1), (1, 0, 0) \in L_2$, and is of *type 1* otherwise. A set of μ MNOLS of order n is of type 0 if fixing the order in some way gives a list of μ MNOLS of order n of type 0 and is of type 1 otherwise.

A collection of μ cyclic MNOLS of order n contains a *row-intercalate* of difference d if two of its Latin squares L and M have two symbols e, e' with $e < e'$ and $e' - e = d$ such that $L(r, 0) = M(r', 0) = e$ and also $L(r', 0) = M(r, 0) = e'$, for some $r, r' \in \{0, \ldots, n-1\}$. Then it is clear that a collection of μ cyclic MNOLS of order n is of type 0 if and only if it contains a row-intercalate of difference d and $\gcd(d, n) = 1$. Clearly set-isotopy preserves type. In Tables 6–14, we show the number of set-isotopy classes of each type. Observe that the proportion of set-isotopy classes that are of type 0 increases as μ increases. This may be of interest in future searches for sets of μ cyclic MNOLS of order n where μ is relatively large. Considering each type individually may allow more efficient construction of those set-isotopy classes with non-trivial set-autotopy group, as each set-autotopy must map row-intercalates to row-intercalates. Note that $|\mathrm{Red}_s(\mathcal{L})| = 1$ for $n = 14$, so we omit the column for $|\mathrm{Red}_s(\mathcal{L})|$ in this case.

ACKNOWLEDGMENTS

The authors would like to thank the referees for their useful suggestions and comments. This work was supported in part by the Academy of Finland (Project #289002). This research was supported in part by the Monash eResearch Centre and eSolutions-Research Support Services through the use of the MonARCH HPC Cluster.

ORCID

Diane M. Donovan http://orcid.org/0000-0002-1329-3514
Janne I. Kokkala http://orcid.org/0000-0001-6986-7794
Trent G. Marbach http://orcid.org/0000-0002-3708-3095

REFERENCES

1. F. Demirkale et al., *Difference covering arrays and pseudo-orthogonal Latin squares*, Graphs Combin. **32** (2016), 1353–1374.
2. F. Demirkale, D. M. Donovan, and A. Khodkar, *Direct constructions for general families of cyclic mutually nearly orthogonal latin squares*, J. Combin. Des. **23** (2015), 195–203.
3. F. Demirkale, D.M. Donovan, J.I. Kokkala, and T.G. Marbach, *MNOLS data*. https://tinyurl.com/MNOLSenum
4. J. Egan and I. M. Wanless, *Enumeration of MOLS of small order*, Math. Comp. **85** (2016), 799–824.
5. I. A. Faradžev, Generation of nonisomorphic graphs with a given distribution of the degrees of vertices (in Russian), *Algorithmic Studies in Combinatorics*, **185**, Nauka, Moscow, Russia, 1978, 11–19.
6. M. Hall, *Cyclic projective planes*, Duke Math. J. **14** (1947), 1079–1090.
7. P. Kaski and P. R. J. ÖstergÅrd, Classification algorithms for codes and designs, *Algorithms and Computation in Mathematics*, Vol. **15**, Springer, Heidelberg, Germany, 2006.

8. G. Kolesova, C. W. H. Lam, and L. Thiel, *On the number of* 8×8 *Latin squares*, J. Combin. Theory Ser. A **54** (1990), 143–148.
9. C. Laywine and G. Mullen, Discrete mathematics using Latin squares, *Wiley-Interscience Series in Discrete Mathematics and Optimization*, Wiley, New York, NY, 1998.
10. P. C. Li and G. H. J. van Rees, *Nearly orthogonal latin squares*, J. Combin. Math. Combin. Comput. **62** (2007), 13–24.
11. B. D. McKay, *Isomorph-free exhaustive generation*, J. Algorithms **26** (1998), 306–324.
12. B. D. McKay, A. Meynert, and W. J. Myrvold, *Small latin squares, quasigroups and loops*, J. Combin. Des. **15** (2007), 98–119.
13. B. D. McKay and A. Piperno, *Practical graph isomorphism, II*, J. Symbolic Comput. **60** (2014), 94–112.
14. B. D. McKay and I. M. Wanless, *Most Latin squares have many subsquares*, J. Combin. Theory Ser. A **86** (1999), 322–347.
15. B. D. McKay and I. M. Wanless, *On the number of Latin squares*, Ann. Comb. **9** (2005), 335–344.
16. E. B. Pasles and D. Raghavarao, *Mutually nearly orthogonal latin squares of order 6*, Util. Math. **65** (2004), 65–72.
17. D. Raghavarao, S. S. Shrikhande, and M. S. Shrikhande, *Incidence matrices and inequalities for combinatorial designs*, J. Combin. Des. **10** (2002), 17–26.
18. R. C. Read, *Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations*, Algorithmic Aspects of Combinatorics (Conf., Vancouver Island, B.C., 1976). Volume 2 of Annals of Discrete Mathematics, North-Holland Publication, Amsterdam, The Netherlands, 1978, 107–120.
19. G. H. J. van Rees, *Private communication*, 2015.

How to cite this article: Demirkale F, Donovan DM, Kokkala JI, Marbach TG. The enumeration of cyclic mutually nearly orthogonal Latin squares. *J Combin Des*. 2019;27: 265–276. https://doi.org/10.1002/jcd.21647