Sets of MOLSs generated from a single Latin square

Hau Chan and Dinesh G. Sarvate

ABSTRACT. The aim of this note is to present an observation on the families of square matrices generated by repeated application of a simple operation on Latin squares, which in special cases give complete families of self-orthogonal and mutually orthogonal idempotent Latin squares with the inclusion of a specific Latin square in these families produces complete families of MOLSs.

1. Introduction

A Latin square of order n is an n by n array such that each element from an n-set, say $\{1, 2, \cdots, n\}$, appears exactly once in each row and in each column. The $(i, j)^{th}$ element of a Latin square L is usually denoted by $L(i,j)$.

EXAMPLE 1. *The following is a Latin square of order* 5.

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

.

DEFINITION 1. *A Latin square L of order n is idempotent if $L(i,i) = i$ for $1 \leq i \leq n$.*

Note that we can relabel the elements using the diagonal of the Latin square above to obtain an idempotent Latin square of order 5,

2000 *Mathematics Subject Classification.* Primary 05B05.

Key words and phrases. Latin Square, Quasigroup, Orthogonal Array, Symmetric Latin Square, Idempotent Latin Square, Self-Orthogonal Latin Square .

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

.

A Latin square can be viewed as a quasigroup $(L, \circ)$ if we label its rows and columns by the same symbols and define $i \circ j$ to be the $(i, j)^{th}$ element of L.

DEFINITION 2. *A Latin square L of order n is symmetric if L(i,j)=L(j,i) for all* $1 \leq i,j \leq n$.

Note that, both Latin squares of order 5 given above are symmetric.

An idempotent Latin square and a symmetric Latin square exist for any order n, however a symmetric idempotent Latin square (SILS) exists only for odd n [**9**].

DEFINITION 3. *Two Latin squares L and $L^{'}$ of the same order, say n, are orthogonal if every ordered pair $(i, j), 1 \leq i, j \leq n$, appears exactly once when L and $L^{'}$ are superimposed on each other.*

In other words, two Latin squares L and $L^{'}$ of the same order are *orthogonal* if L(a,b) = L(c,d) and $L^{'}$(a,b) = $L^{'}$(c,d), implies a = c and b = d. A Latin square which is orthogonal to its transpose is called a self-orthogonal Latin square (SOLS). It is known that self-orthogonal Latin squares exist for all orders $n \notin \{2,3,6\}$. A self-orthogonal Latin square has at least one transversal (its main diagonal) and therefore any self-orthogonal Latin square can be transformed into an idempotent Latin square by relabeling the symbols. See [**4**], and [**8**].

EXAMPLE 2.

1	7	6	5	4	3	2
3	2	1	7	6	5	4
5	4	3	2	1	7	6
7	6	5	4	3	2	1
2	1	7	6	5	4	3
4	3	2	1	7	6	5
6	5	4	3	2	1	7

SOLS of order n=7.

Latin squares L_1,...,L_m are *mutually orthogonal*, or pairwise orthogonal, if for all i, j, $1 \leq$ i $<$ j $\leq$ m, L_i and L_j are orthogonal . A set of $n - 1$ MOLS of side n is called a *complete set* of MOLSs.

This note is inspired by a construction of a combinatorial design called beautifully ordered balanced incomplete block design. A balanced incomplete block design BIBD(v,k,λ) is a set S of v elements together with a collection of b k-subsets of S, called blocks, where each pair of distinct elements occurs in exactly λ blocks.

DEFINITION 4. *If each of the blocks of a* BIBD(v,k,λ) *is ordered such that for any k_1 indices $i_1, i_2, \cdots, i_{k_1}$ the sub-blocks $\{a_{i_1}, a_{i_2}, \cdots, a_{i_{k_1}}\}$ of all ordered blocks $\{a_1, a_2, \cdots, a_k\}$ of the* BIBD(v,k,λ) *form a* BIBD(v,k_1,λ_1) *then the collection of ordered blocks is called a Beautifully Ordered Balanced Incomplete Block Design,* BOBIBD$(v,k,\lambda,k_1,\lambda_1)$ *where* $2 \leq k_1 \leq k$-1.

A general construction of BOBIBD$(v,4,12,2,2)$ based on mutually orthogonal Latin squares is given in [**2**]. However, this general construction is not applicable for $v=6$ as there are no MOLSs of order 6. A BOBIBD$(6,4,12,2,2)$ was constructed using the following quasigroup $(L,\circ)$ and a corresponding square generated from $(L,\circ)$.

$a \circ b$

1	6	2	5	3	4
4	2	6	3	1	5
2	5	3	6	4	1
5	3	1	4	6	2
6	1	4	2	5	3
3	4	5	1	2	6

$(a \circ b) \circ b$

1	4	6	2	4	2
5	2	5	6	3	3
4	1	3	1	6	4
6	5	2	4	2	5
3	6	1	3	5	1
2	3	4	5	1	6

These two squares of order 6 which, when superimposed, all 36 possible ordered pairs result. Hence, the blocks $\{\{a,b,a\circ b,(a\circ b)\circ b\} \mid 1 \leq a \neq b \leq 6\}$ give a BOBIBD$(6,4,12,2,2)$. The aim of this note is to explore the technique of applying $(a \circ b) \circ b$ on Latin squares repeated to get a complete set of MOLSs.
Interestingly, the results obtained here are also related with the results obtained by Graham and Roberts [**5**], [**6**], and [**7**]. We have also used their specific Latin squares to generate the corresponding families of complete MOLSs in this note.

LEMMA 1. *(Lemma 2 Graham and Roberts [**7**]) Any set of mutually orthogonal Latin squares can contain at most one symmetric Latin square.*

All families generated in this paper contain exactly one symmetric idempotent Latin square. Graham and Roberts [**5**] gave the following definition.

DEFINITION 5. *An orthogonal set of Latin squares, $\{A_1,A_2,\ldots,A_r\}$, is called orthogonal, self-orthogonal or OSO, if $\{A_1^T,A_2,A_2^T,\ldots,A_r,A_r^T\}$ is an orthogonal set. In this case, the set $\{A_1^T,A_2,A_2^T,\ldots,A_r,A_r^T\}$ is called the expansion of the OSO set $\{A_1,A_2,\ldots,A_r\}$.*

Graham and Roberts used S(n) to denote the size of a maximal OSO set. All families generated in this paper contain a maximal size OSO set.

By a result of Brayton, Coppersmith, and Hoffman, S(n) $\geq$ 1 for n $\neq$ 2, 3, 6. Moreover, S(n) $\leq$ N(n)/2 [**5**].

Graham and Roberts [**7**] defined C^- as the Latin square of order n with each entries $c^-_{i,j}$ = i - j (mod n) and used it to obtain a complete set of mutually orthogonal Latin squares.

A well known method to obtain a complete set of mutually orthogonal Latin squares of prime order p, $\{A_1,A_2,...,A_{p-1}\}$, is to use the formula $L_x(i,j) = i + xj(\text{mod } p)$, for the $(i,j)^{th}$ entry of Latin Square L_x, where $x = 1, 2, ..., p-1$.

The MOLSs constructed in the next section by applying the operation $(a \circ b) \circ b$ repeatedly may produce the above complete set of MOLSs or some other family of MOLSs depending on the Latin Square used as the generator. For example, the second Latin square of order 7 given in section 2.2 produces a different family than the one obtained by the above well known method.

2. Main Result

Definition 6. *A First Class Generated by an idempotent Latin square L of order n, FCG(L) is an ordered set* $\{L = L_1, L_2, \cdots\}$ *of idempotent (not necessarily Latin squares) squares of order n which is generated as follows: let* $(i,j)^s$ *denote the* $(i,j)^{th}$ *entry of* L_s. *Then* $(i,j)^s = ((i,j)^{s-1}, j)^1$.

Note that (i,j)^2 = $(i \circ j) \circ j$ if L_1 is considered as quasigroup (L,$\circ$).

Example 3. *An FCG(L) of order 5.*

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

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

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

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

We say that $FCG(L)$ has a *length* of 4. Notice that $FCG(L)$ contains two self-orthogonal Latin squares, which are mutually orthogonal:

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

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

In addition, the family contains exactly one symmetric idempotent Latin square, L_3 is the transpose of self-orthogonal idempotent Latin square

L_2, and L_4 is not a Latin square. $\{L_2\}$ is an example of OSO of Graham and Roberts [**5**]. Also note that $\{L_2, L_3\}$ is the expansion of OSO $\{L_2\}$.

All together the family contains exactly 3 MOLSs which are idempotent. Moreover, if we use the idea of Graham and Roberts and include C^- in the family, we obtain a complete set of mutually orthogonal Latin squares.

Given an appropriate idempotent Latin square of prime order p, one can generate a family of mutually orthogonal idempotent self-orthogonal Latin squares of order p, by applying the operation (aob)ob repeatedly. The family contains $p-2$ MOLSs and exactly one symmetric idempotent Latin square of order p. These MOLSs together with C^- form a complete set of MOLSs.

2.1. Symmetric Idempotent Latin square. We can construct a symmetric idempotent Latin square using the following result.

LEMMA 2. *Let n=2m+1 where m is a positive integer. Define* $L_{i,j} = (m+1)\times(i+j)$ *mod n, then* $L_{i,j}$ *is a symmetric idempotent Latin square of order n* [*page* 339,[**1**]].

For example, we have generated families for $n = 3, 5$, and 11 using the Latin squares given below. All families generated by these Latin squares have exactly one symmetric idempotent Latin square (the generator Latin square), and $(p-3)$ self-orthogonal idempotent Latin squares. The next table gives a partial listing of the results for primes up to 100 to demonstrate that we don't always get a complete family of MOLS.

EXAMPLE 4.

- $n = 3$

1	3	2
3	2	1
2	1	3

.

- $n = 5$

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

.

- $n = 11$

1	7	2	8	3	9	4	10	5	11	6
7	2	8	3	9	4	10	5	11	6	1
2	8	3	9	4	10	5	11	6	1	7
8	3	9	4	10	5	11	6	1	7	2
3	9	4	10	5	11	6	1	7	2	8
9	4	10	5	11	6	1	7	2	8	3
4	10	5	11	6	1	7	2	8	3	9
10	5	11	6	1	7	2	8	3	9	4
5	11	6	1	7	2	8	3	9	4	10
11	6	1	7	2	8	3	9	4	10	5
6	1	7	2	8	3	9	4	10	5	11

.

Table 1. Partial Summary where generator is a symmetric idempotent Latin square

Order n	Number of SILS	Number of SOLS	Total
3	1	0	1
5	1	2	3
7	1	1	2
11	1	8	9
13	1	10	11
17	1	6	7
19	1	16	17
23	1	9	10
29	1	26	27
31	1	3	4
37	1	34	35
41	1	18	19
43	1	12	13
47	1	21	22
53	1	50	51
59	1	56	57
61	1	58	59
67	1	64	65
71	1	33	34
73	1	7	8
79	1	37	38
83	1	80	81
89	1	9	10
97	1	46	47

2.2. Self-Orthogonal Latin square. The following Lemma is well known, for example, see [**10**].

LEMMA 3. *Let a, b* $\in Z_n$. *We define an n by n array* $L = (l_{i,j})$, *with symbols in* Z_n, *by the formula* $l_{i,j} = ai + bj \pmod n$, *where gcd(a,n) = 1, gcd(b,n) = 1, and gcd(*a^2 *-* b^2*, n) = 1. It is known that L is a self-orthogoanl Latin square of order n.*

Using self-orthogonal idempotent Latin square L of order n, we can construct corresponding FCG(L), with $n-3$ SOLs and a symmetric idempotent Latin square. There are several Latin squares of the same order. Here we present only two such examples. Computer checking is done for larger primes as well as all primes less than 100. The results are summarized in Table 2.

EXAMPLE 5.

- $n = 7$

1	5	4	7	6	3	2
7	2	5	3	1	4	6
6	4	3	1	2	7	5
3	6	2	4	7	5	1
2	3	7	6	5	1	4
5	7	1	2	4	6	3
4	1	6	5	3	2	7

.

- *Another example for n = 7 that gives a different family of MOLS.*

1	4	7	3	6	2	5
6	2	5	1	4	7	3
4	7	3	6	2	5	1
2	5	1	4	7	3	6
7	3	6	2	5	1	4
5	1	4	7	3	6	2
3	6	2	5	1	4	7

.

- $n = 11$

1	6	11	5	10	4	9	3	8	2	7
8	2	7	1	6	11	5	10	4	9	3
4	9	3	8	2	7	1	6	11	5	10
11	5	10	4	9	3	8	2	7	1	6
7	1	6	11	5	10	4	9	3	8	2
3	8	2	7	1	6	11	5	10	4	9
10	4	9	3	8	2	7	1	6	11	5
6	11	5	10	4	9	3	8	2	7	1
2	7	1	6	11	5	10	4	9	3	8
9	3	8	2	7	1	6	11	5	10	4
5	10	4	9	3	8	2	7	1	6	11

.

- *Another example for* $n = 11$

1	11	10	9	8	7	6	5	4	3	2
3	2	1	11	10	9	8	7	6	5	4
5	4	3	2	1	11	10	9	8	7	6
7	6	5	4	3	2	1	11	10	9	8
9	8	7	6	5	4	3	2	1	11	10
11	10	9	8	7	6	5	4	3	2	1
2	1	11	10	9	8	7	6	5	4	3
4	3	2	1	11	10	9	8	7	6	5
6	5	4	3	2	1	11	10	9	8	7
8	7	6	5	4	3	2	1	11	10	9
10	9	8	7	6	5	4	3	2	1	11

.

TABLE 2. Partial Summary where generator is an idempotent SOLS

Order n	Number of SILS	Number of SOLS	Total	A and B used
7	1	4	5	A=3, B=5
11	1	8	9	A=2, B=3
13	1	10	11	A=3, B=7
17	1	14	15	A=2, B=3
19	1	16	17	A=2, B=5
23	1	20	21	A=2, B=13
29	1	26	27	A=2, B=23
31	1	28	29	A=2, B=11
37	1	34	35	A=2, B=31
41	1	38	39	A=2, B=5
43	1	40	41	A=2, B=7
47	1	44	45	A=2, B=11
53	1	50	51	A=2, B=13
59	1	56	57	A=2, B=17
61	1	58	59	A=2, B=23
67	1	64	65	A=2, B=31
71	1	68	69	A=2, B=37
73	1	70	71	A=2, B=41
79	1	76	77	A=2, B=59
83	1	80	81	A=2, B=61
89	1	86	87	A=2, B=73
97	1	94	95	A=2, B=13

It is natural to ask the following questions :

(1) Which symmetric idempotent Latin squares (with the given pattern or some other structure) or self orthogonal idempotent Latin squares generate a complete family of MOLSs?
(2) How to characterize the symmetric idempotent Latin squares and self-othogonal idempotent Latin squares which will generate a complete family of MOLSs?

Tables 1 and 2 provide strong support for the following conjecture:

CONJECTURE 1. *For every prime p, there exists an idempotent Latin square of order p, such that the first class generated by L, FCG(L), with the operation* $(a \circ b) \circ b$*, together with* C^{-}*, gives a complete set of self-orthogonal idempotent Latin square.*

ACKNOWLEDGEMENT 1. *The authors wish to thank professors George Graham and Charles Roberts for providing their papers. Dinesh Sarvate would like to thank the Department of Mathematics at the College of Charleston for providing summer support.*

References

[1] R. A. Brualdi, *Introductory Combinatorics*, Third Edition, Prentice Hall, New Jersey, 1999.
[2] H. Chan and D. G. Sarvate, Beautifully Ordered Balanced Incomplete Block Designs, JCMCC, accepted.
[3] C. J. Colbourn, J. H. Dinitz, and I. M. Wanless, *Latin Squares*, The Handbook of Combinatorial Designs, edited by C. J. Colbourn and J. H. Dinitz, Chapman/CRC Press, Boca Raton, Fl., 2007, 135-152.
[4] N. J. Finizio and L. Zhu, *Self-Orthogonal Latin Squares (SOLS)*, The Handbook of Combinatorial Designs, edited by C. J. Colbourn and J. H. Dinitz, Chapman/CRC Press, Boca Raton, Fl., 2007, 211-219.
[5] G. P. Graham, and C. E. Roberts, *Projective Planes and Complete Sets of Orthogonal, Self-Orthogonal Latin Squares.* Congressus Numerantium 184(2007): 161-172.
[6] G. P. Graham, and C. E. Robert,. *Enumeration and Isomorphic Classification of Self-Orthogonal Lain Squares.* The Journal of Combinatorial Mathematics and Combinatorial Computing. 59(2006): 101-118.
[7] G. P. Graham, and C. E. Roberts, *Complete Sets of Orthogonal, Self-Orthogonal Latin Squares.* Ars Combinatoria. 64(2002): 193-198.
[8] R. Julian, R. Abel, C. J. Colbourn, and J. H. Dinitz, *Mutualy Orthogonal Latin Squares (MOLS)*, The Handbook of Combinatorial Designs, edited by C. J. Colbourn and J. H. Dinitz, Chapman/CRC Press, Boc Raton, FL.,2007, 160-193.
[9] C. C. Lindner and C. A. Rodger, *Design Theory*, CRC Press, Boca Raton, 1997.
[10] D. Stinson, *Combinatorial Designs, Constructions and Analysis*, Springer-Verlag, New York, 2004.

(A. One) College of Charleston, Dept. of Math., Charleston, SC, 29424
E-mail address: sarvated@cofc.edu

(A. Two) College of Charleston, Dept. of Math., Charleston, SC, 29424
E-mail address: hchan@edisto.cofc.edu