A Simple Construction for Orthogonal Latin Rectangles

Gary L. Mullen*
Department of Mathematics
The Pennsylvania State University
University Park, PA
16802

Jau-Shyong Shiue
Department of Mathematical Sciences
University of Nevada, Las Vegas
Las Vegas, NV
89154

1. Introduction

For $m \leq n$ an $m \times n$ latin rectangle is an $m \times n$ array consisting of the elements of $Z_n = \{0, 1, \ldots, n-1\}$ with the property that each row is a permutation of Z_n and no element occurs twice in any column. If $m = n$ we simply have a latin square of order n. Two such rectangles are orthogonal if upon superposition no ordered pair occurs twice, and a set of $t \geq 2$ such rectangles is said to be orthogonal if any two distinct rectangles are orthogonal. Such a set is complete if $t = n-1$. It is well known that sets of orthogonal latin squares and rectangles are useful in the design of statistical experiments, see for example Dénes and Keedwell [2] where the reader will find an excellent survey of the theory of latin squares and related objects.

In this note we discuss a simple number theoretic construction for sets of mutually orthogonal latin rectangles (MOLRs). Our results extend and generalize those of Quattrocchi [4] described in [2, p. 180] which are limited to $p \times pq$ rectangles where p is prime and no prime factor of q is less than p. While our construction does not always yield complete sets of MOLRs, we do obtain nontrivial collections of MOLRs. For $m \leq n \leq 30$ we indicate in Table 1 the maximum number of MOLRs constructible by our algorithm. In section 3 we discuss the construction of higher dimensional latin parallelepipeds.

In [1] Bose constructed a complete set of mutually orthogonal latin squares (MOLS) of order q whenever q is a prime power. This construction can be described as follows. If $0 \neq a \in F_q$ the finite field of order q, place the element $ax + y$ at the intersection of row x and column y of the a-th square. Hence for q a prime power one can always construct a complete set of $q-1$ MOLRs of size $m \times q$ for any $2 \leq m \leq q$.

*This author would like to thank the National Security Agency for partial support under grant agreement #MDA904-87-H-2023. The same author would like to thank the Mathematical Sciences Department of Clemson University for its hospitality when this note was written.

2. The Construction

By relabeling the symbols of a set of MOLRs, we may assume that the first row is in the standard order $0, 1, \ldots, n-1$. If $1 \leq k < n$ form an $m \times n$ rectangle (r_{ij}) where

$$r_{ij} \equiv ki + j \pmod{n}, \qquad 0 \leq i < m; \quad 0 \leq j < n. \tag{1}$$

If $ki + j_1 = ki + j_2$ then $j_1 = j_2$ so the rectangle is latin by row and it is latin by column provided $m \leq n/(k, n)$ where (k, n) denotes the greatest common divisor of k and n.

As one varies k how many distinct MOLRs of size $m \times n$ does (1) generate? Clearly if $m = n$ is a prime, then we obtain $n - 1$ MOLS of order n and our construction is the same as that of Bose [1].

As shown in Bose [1] the existence of $n-1$ MOLS of order n is equivalent to the existence of an affine plane of order n. Moreover a long standing conjecture postulates that every affine plane of pime order is desarquesian, see [2, p. 276]. If n is a prime the construction (1) leads to a desarguesian plane and so alternatively it is conjectured that all complete sets of MOLS of prime order are isomorphic, i.e. can be obtained from the construction (1) by applying a fixed permutation to the rows and a fixed (possibly different) permutation to the columns of each square in the set.

Thus in spite of the simplicity of our construction, it is conjectured that all complete sets of MOLS of prime order can be obtained from our construction. In general for $m \leq n$ let $N(m, n)$ denote the maximum number of MOLRs of size $m \times n$ that can be constructed by (1). The following algorithm provides a method for the computation of $N(m, n)$ for any $m \leq n$.

Step 1: Let $S(m, n) = \{k | n/m \geq (k, n), 1 \leq k < n\} = \{k_1, \ldots, k_l\}$ and note that $S(m_1, n) \subseteq S(m_2, n)$ if $m_1 > m_2$,

Step 2: Let $a = 3$. Solve

$$(a-1)(k_i - k_j) \equiv 0 \pmod{n} \tag{2}$$

Step 3: For a solution $\{k_i, k_j\}$ of (2), if $(k_i, n) > (k_j, n)$ eliminate k_i from $S(m, n)$. If $(k_i, n) = (k_j, n)$ eliminate k_j where $k_j > k_i$. Repeat for all solutions of (2). Repeat steps 2 and 3 with $a = 4, 5, \ldots, m$.

Step 4: Let $S'(m, n) = \{k'_1, \ldots, k'_t\}$ where for $i \neq j$, $\{k'_i, k'_j\}$ does not satisfy (2). For each $k' \in S'(m, n)$ use (1) to construct an $m \times n$ latin rectangle so that $N(m, n) = |S'(m, n)|$.

Proof: If $k' \in S'(m, n)$, since $(k, n) \leq n/m$, the rectangle is latin and two such rectangles are orthogonal if and only if the k's do not satisfy (2).

Example: Let $m = 5$ and $n = 10$ so that $S(5, 10) = \{1, 2, 3, 4, 6, 7, 8, 9\}$ and (2) becomes $4(k_i - k_j) \equiv 0 \pmod{10}$ whose solutions are (1,6), (2,7), (3,8), and

(4,9). Since (6,10) > (1,10), (6) is eliminated and similarly 2,4,8 are eliminated from $S(5,10)$ so that $S'(5,10) = \{1,3,7,9\}$ and hence $N(5,10) = 4$. Moreover the four MOLRs of size 5×10 given by (1) are

0123456789	0123456789	0123456789	0123456789
1234567890	3456789012	7890123456	9012345678
2345678901	6789012345	4567890123	8901234567
3456789012	9012345678	1234567890	7890123456

As a result of the algorithm we can prove

Theorem.

(A) $N(2,n) = n-1$ *for all* n,

(B) $N(3,n) = \begin{cases} n-1 & \text{if } n \text{ is odd} \\ \frac{n}{2}-1 & \text{if } n \text{ is even,} \end{cases}$

(C) *If* p *is prime* $N(p,n) = n-1$ *if all prime divisors of* n *are at least* p,

(D) $N(m,n) = n-1$ *if* $2 \leq m \leq p$ *where* p *is the smallest prime in* n,

(E) *If* $n = p_1^{e_1} \cdots p_r^{e_r}$ *with* p_i *distinct primes, then* $N(n,n) = \min_{1 \leq i \leq r}\{p_i - 1\}$,

(F) *If* p *is prime and* $a \leq b$, $N(p^a, p^b) = p^{b-a+1} - 1$,

(G) *If* $n = pq$ *with* p *and* q *prime, then* $N(q+1, pq) = p-1$.

Proof: Let $1 \leq k_1, k_2 < n$. For (A), (2) becomes $k_1 \equiv k_2 \pmod{n}$ so $k_1 = k_2$ and $N(2,n) = n-1$. For (B), (2) becomes $2(k_1 - k_2) \equiv 0 \pmod{n}$. The congruence $2x \equiv 0 \pmod{n}$ has one solution if n is odd and 2 solutions if n is even. Hence for n odd we have $k_1 = k_2$ so that $N(3,n) = n-1$. For n even, the two solutions are $x = 0$ and $n/2$. For $n/2$ the possible pairs (k_1, k_2) are $(\frac{n}{2} + r, r)$, $r = 1, \ldots, n-1$. If $n/(k,n) = 1$ then n divides k which is impossible and so $n/(k,n) = 2$ so that $k = n/2$. Hence for the pairs $(\frac{n}{2} + r, r)$ $r = 1, \ldots, n-1$, $k = n/2$ must be eliminated and we can choose only one component so that $N(3,n) = (n-2)/2$ for n even.

For (C) and (D), (2) becomes $(k_1 - k_2)(m-1) \equiv 0 \pmod{n}$. Let $d = (m-1, n)$ so $(m-1)x \equiv 0 \pmod{n}$ has exactly d solutions. Hence $N(m,n) = n-1$ if and only if $d = 1$ and $m \leq \min_{1 \leq k \leq n-1} \frac{n}{(k,n)}$. Let $n = p_1^{e_1} \ldots p_1^{e_r}$ be the prime factorization of n with $p_i < p_{i+1}$, $i = 1, \ldots, r-1$ and $e_j \geq 1$ for $j = 1, \ldots, r$. Thus $\min_{1 \leq k \leq n-1} \frac{n}{(k,n)} = p_1$. If $m \leq p_1$ then $(m-1, n) = 1$. Hence $N(m,n) = n-1$ if and only if $m \leq p$ where p is the smallest prime factor of n. This proves both (C) and the more general (D). For (E) suppose $p_1 < \cdots < p_r$ and let $n = p_1^{e_1} q$. If $1 \leq k < p_1^{e_1} q$ then k can be represented as $ap_1 + j$ with $1 \leq j \leq p_1 - 1$ and $0 \leq a \leq p_1^{p_1 - 1} q - 1$. We first eliminate all multiples of p_1. For the remaining k, we know that the pairs $(j, ap_1 + j)$ with $a \geq 1$ satisfy the congruence $(n-1)(k_i - k_j) \equiv 0 \pmod{p_1^{e_1} q}$. Hence by step 2 of our algorithm we eliminate all k except $1, 2, \ldots, p_1 - 1$ so that $N(n,n) = p_1 - 1$. By using

the algorithm and an argument similar to that used in the proof of (E) we obtain (F) and (G).

We note that (C) and (D) both generalize results of Quattrocchi [4] which gave complete sets only in the case of $p \times pq$ rectangles where each prime factor of q is not less than the prime p.

Table 1 gives the values of $N(m,n)$ for $n \leq 30$. As $N(2,n) = n-1$ and $N(m,p) = p-1$ for p prime, these values are not displayed.

Table 1

$m\backslash n$	4	6	8	9	10	12	14	15	16	18	20	21	22	24	25	26	27	28	30
3	1	2	3	8	4	5	6	14	7	8	9	20	10	11	24	12	26	13	14
4	1	1	3	2	4	3	6	4	7	3	9	6	10	7	24	12	8	13	5
5		1	1	2	4	2	6	4	3	3	4	6	10	4	24	12	8	6	5
6		1	1	2	1	2	6	2	3	3	2	6	10	4	4	12	8	6	2
7			1	2	1	1	6	2	3	2	2	6	10	2	4	12	8	6	1
8			1	2	1	1	1	2	3	2	2	2	10	2	4	12	8	2	1
9				2	1	1	1	2	1	2	2	2	10	2	4	12	8	2	1
10					1	1	1	2	1	1	2	2	10	2	4	12	2	2	1
11						1	1	2	1	1	1	2	10	2	4	12	2	2	1
12						1	1	2	1	1	1	2	1	2	4	12	2	2	1
13							1	2	1	1	1	2	1	1	4	12	2	2	1
14							1	2	1	1	1	2	1	1	4	1	2	2	1
15								2	1	1	1	2	1	1	4	1	2	1	1
16									1	1	1	2	1	1	4	1	2	1	1
17										1	1	2	1	1	4	1	2	1	1
18										1	1	2	1	1	4	1	2	1	1
19											1	2	1	1	4	1	2	1	1
20											1	2	1	1	4	1	2	1	1
21												2	1	1	4	1	2	1	1
22													1	1	4	1	2	1	1
23														1	4	1	2	1	1
24														1	4	1	2	1	1
25															4	1	2	1	1
26																1	2	1	1
27																	2	1	1
28																		1	1
29																			1
30																			1

3. Higher Dimensions

These ideas can be generalized to cubes and hypercubes of dimension $d \geq 3$. For example for $d = 3$ if $n_1 \leq n_2 \leq n_3 = n$, an $n_1 \times n_2 \times n_3$ latin parallelepiped of order n is an array with the property that if any two coordinates are fixed, no element is repeated in the third coordinate. A collection of three such parallelepipeds is said to be 3-orthogonal if upon superposition no ordered triple occurs twice, and a set is 3-orthogonal if any three distinct parallelepipeds are 3-orthogonal.

If $n \geq 3$ is prime then for any $n_1 \leq n_2 \leq n_3 = n$, if $k_1 k_2 k_3 \not\equiv 0 \pmod{n}$ then

$$r_{i_1 i_2 i_3} \equiv k_1 i_1 + k_2 i_2 + k_3 i_3 \pmod{n}, \quad 0 \leq i_e \leq n_e;\ e = 1,2,3 \qquad (3)$$

gives an $n_1 \times n_2 \times n_3$ latin parallelepiped of order n. Moreover if (k_1, k_2, k_3), (k_1', k_2', k_3'), (k_1'', k_2'', k_3''), are linearly independent over F_n, then (3) will yield a set of 3-orthogonal cubes and each cube is latin provided none of the k's are zero, (if some of the k's are 0, the corresponding cubes will not be latin but the set will remain 3-orthogonal). The maximum number $M(3,p,3)$ of vectors (k_1, k_2, k_3) over F_p (possibly with some 0 coordinates) with the property that any three are linearly independent over F_p is $p + 1$, see [3]. For example for $n = 3$ we may take the vectors (1,1,1), (2,1,1) (1,2,1) and (1,1,2) which will yield the four 3-orthogonal latin cubes of order 3 given by

012	012	021	012
120	201	102	120
201	120	210	201
120	120	102	201
201	012	210	012
012	201	021	120
201	201	210	120
012	120	021	201
120	012	102	012

These ideas will work for the construction of sets of k-orthogonal parallelpipeds of dimension $d \geq 2$ provided one knows the maximum number $M(k,p,d)$ of vectors of length d over F_p any k of which are linearly independent over F_p. Unfortunately as indicated in [3], the function $M(k,p,d)$,which is related to algebraic coding theory, is known only in a few special cases. Even the value of $M(d,p,d)$ is known only for $d \leq 5$.

References

1. R.C. Bose, *On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares*, Sankhyā 3 (1938), 323–338.
2. J. Dénes and A. D. Keedwell, *Latin Squares and their Applications*, Academic Press. New York (1974).
3. J. W. P. Hirschfeld, *Maximum sets in finite projective spaces*, in "Surveys in Combinatorics." London Math. Society, Lecture Note Series 82, edited by E.K. Lloyd, Camb. Univ. Press, Cambrige 1983, 55–76.
4. P. Quattrocchi, *S-spazi e sistemi de rettangoli latinia*, Atti Semi. Mat. Fis Univ. Modeva 17 (1968), 61–71.