ON EMBEDDING AND ENUMERATION OF ORTHOGONAL LATIN SQUARES

by

A. Hedayat and W. T. Federer

Cornell University

Abstract

In the following by an $O(n,t)$ set, we mean a set of t mutually orthogonal Latin squares of order n . An obvious and interesting problem in the theory of mutually orthogonal Latin squares is the following: Given an $O(n,r)$ set S with $r < n-1$, what is a necessary and sufficient condition under which S can be embedded in an $O(n,t)$ set, $t > r$. By utilizing some results given by H. B. Mann, we have opened a new avenue toward the concept of embedding and some theorems and propositions related to this idea have been obtained.

Another interesting problem is the determination of the number of Latin squares of order n which have no orthogonal mate, which have only one orthogonal mate,..., and which have n-2 orthogonal mates. A lower bound for n even (odd) on the number of orthogonally mateless (at least having one mate) Latin squares has been obtained. All Latin squares of order 3 through 7 have been classified in this manner.

Paper No. BU-194 in the Biometrics Unit series, and No. 583 in the Plant Breeding and Biometry series.

ON EMBEDDING AND ENUMERATION OF ORTHOGONAL LATIN SQUARES[1/]

By A. Hedayat and W. T. Federer

Cornell University

1. Introduction and Summary. The problem of determining whether or not a set of r mutually orthogonal Latin squares of order n, say an $O(n,r)$ set S, can be embedded in a larger set of t mutually orthogonal Latin squares of order n, has considerable mathematical importance and has importance in the construction of experimental designs. Hereafter by an $O(n,1)$ set we mean a set consisting of a single Latin square of order n. Now, an obvious and interesting problem in this area is to find a necessary and sufficient condition under which an $O(n,r)$ set can be embedded in an $O(n,t)$ set for $1 \leq r < t \leq n-1$.

Some of the principal published results on embedding follow: Mann [7] proved that if a Latin square L is of order $n=4t+2$ (or alternatively $4t+1$) with a subsquare of order $2t+1$ (or $2t$) in which all entries are from a set of $2t+1$ (or $2t$) numbers except for possibly t (or $[t-\frac{1}{2}]$) or less of the cells; then $S = \{L\}$ cannot be embedded in an $O(n,2)$ set. Thus, Mann's embedding conditions depend upon the value of n and the combinatorial structure of the set S . Parker [8] proved that if the $O(n,r)$ set S contains a sub $O(r+1,r)$ set, then S can be embedded in an $O(n,r+1)$ set only if $n = (r+1)^2$ or $n \geq (r+1)(r+2)$. These embedding conditions depend upon r, n, and the combinatorial structure of the set S. Shrikhande [11] proved that any $O(n,n-3)$ set S can be embedded in an $O(n,n-1)$ set for all $n > 4$. His result does not require any knowledge

---

1/ Partially supported by Public Health Research Grant GM-05900.

about the combinatorial structure of the set S. Bruck [1] who generalized Shrikhande's [11] results to some extent, utilized net theory to show that any $O(n,n-1-d)$ set S can be embedded in an $O(n,n-1)$ set regardless of the combinatorial structure of S provided that $n > (d-1)(d^3-d^2+d+2)/2$.

Utilizing the above results and some group theory, some new results have been found for embedding $O(n,r)$ sets in $O(n,t)$ sets, $r < t$. The results are presented in the form of several theorems, propositions and corollaries. The first proposition is concerned with a necessary and sufficient condition for embedding $O(n,2)$ sets in $O(n,3)$ sets. Theorem 3.1 gives a sufficient condition for embedding an $O(n,1)$ set in an $O(n,\lambda)$ set, $2 \leq \lambda \leq$ smallest prime in the prime power decomposition of n, less one. Theorem 3.2 states the conditions under which the method of theorem 3.1 fails for embedding certain $O(n,1)$ sets in a larger set. The next theorem states the conditions under which certain $O(n,1)$ sets cannot be embedded in a larger set. Few results on some properties of inverses of Latin squares and on products have also been presented.

An interesting problem related to the concept of embedding is the following: If $N(n,i)$ denotes the totality of all Latin squares of order n and degree i, $i = 1,2,\ldots,n-1$, what is the value of $N(n,i)$ for a given n? (A Latin square L of order n is said to be of degree r if L can be embedded in an $O(n,r)$ set, and r is the largest such integer.). This problem has been solved for $n = 2, 3,\ldots,7$ but little is known for any $n \geq 8$. Theorem 3.4 gives a lower bound for n even (odd) on the number of orthogonally mateless, degree 1, (at least of degree 2) Latin squares. All Latin squares of order 2,3,4,5,6 and 7 are classified with respect to the degree of orthogonality.

2. Preparatory Definitions. There are several forms of definitions of Latin and orthogonal Latin squares. The following forms are useful in proving the results obtained in the present paper.

Definition 2.1. A latin square of order n on a set Σ with n distinct elements is an nXn matrix whose rows and columns are each a permutation of the set Σ. Any Latin square L of order n may therefore be identified with a particular set of n different permutations $(p_1,p_2,\ldots,p_n)$ where p_i is the permutation associated with the i^{th} row; we denote this identification by $L = (p_1,p_2,\ldots,p_n)$ where = means is identified by '. Given that $L = (p_1,p_2,\ldots,p_n)$ is a Latin square, we define L^{-1} to be $(p_1^{-1}, p_2^{-1},\ldots,p_n^{-1})$. For any specified ordering of the elements in Σ, a Latin square L on Σ is said to be in standard form if the permutations associated with the first row and the first column of L are the identity permutations on Σ.

Definition 2.2. If $L_1 = (p_{11}, p_{12},\ldots,p_{1n})$ and $L_2 = (p_{21}, p_{22},\ldots,p_{2n})$ are two Latin squares of order n on an n-set Σ, then we may define L_1L_2 to be $L_3 = (p_{11}p_{21}, p_{12}p_{22},\ldots,p_{1n}p_{2n})$. The generalization to the product of $t > 2$ Latin squares follows immediately. (Apparently only Mann [6] and Hedayat and Federer [5] have utilized this definition in published literature.)

Properties of the Inverse, Power, and Product of Latin Squares.

(i) If L is a Latin square then L^{-1} is a Latin square and is unique.

(ii) If L is a Latin square then L^t, $t > 1$, is not necessarily a Latin square.

(iii) If L_i is a Latin square, $i = 1,2,\ldots,t$, then $L_1L_2\ldots L_t$ is not necessarily a Latin square.

(iv) $(L_1L_2\ldots L_{t-1}L_t)^{-1} = (L_t^{-1}L_{t-1}^{-1}\ldots L_2^{-1}L_1^{-1})$.

Definition 2.3. Let L_1 and L_2 be two Latin squares of order n on two n-sets Σ and Ω, respectively. Then, L_1 and L_2 are said to be orthogonal if the n^2 cells of the superimposed form of L_1 on L_2 is a permutation of the cartesian product set of Σ and Ω, viz., $\Sigma \times \Omega$. The notation $L_1 \perp L_2$ means that L_1 is orthogonal to L_2, and L_2 is called an orthogonal mate for L_1, and vice versa. L_1 is said to be orthogonally mateless if there is no L_2 such that $L_1 \perp L_2$. A set $S = \{L_1, L_2, \ldots, L_t\}$ is said to be a mutually orthogonal set of t Latin squares of order n if L_i is a Latin square of order n and $L_i \perp L_j$, $i \neq j$, $i, j = 1,2,\ldots,t$. Such a set is denoted as an $O(n,t)$ set. Since the maximum value that t is an $O(n,t)$ set can take is n-1, an $O(n,n-1)$ set is designated as a complete set.

3. The Results. It is easy to verify that the orthogonality relation $\perp$ does not have the transitivity property, viz., if L_1, L_2, and L_3 are three Latin squares such that $L_1 \perp L_2$ and $L_2 \perp L_3$ this does not imply that $L_1 \perp L_3$; in the following proposition, we give a necessary and sufficient condition guaranteeing the orthogonality of L_1 and L_3.

Proposition 3.1. Given $S = \{L_1, L_2\}$ is an $O(n,2)$ set and L_3 is a Latin square such that $L_2 \perp L_3$. Under these conditions $\bar{S} = \{L_1, L_2, L_3\}$ is an $O(n,3)$ set if and only if $L_1^{-1}L_3$ is a Latin square.

The proof follows directly from theorem 1 in [6]. It should be noted from the above that if $\{L_1, L_2, L_3\}$ is an $O(n,3)$ set, this implies that $L_1^{-1}L_2 \perp L_1^{-1}L_3$ and $L_2^{-1}L_1 \perp L_2^{-1}L_3$.

The following proposition establishes the relationship between the orthogonal mates of L and L^{-1} .

Proposition 3.2. If $L_1 \perp L_2$ and if X and Y are the two Latin squares such that $L_1X = L_2$ and $L_2Y = L_1$, then $L_1^{-1} \perp X$ and $L_2^{-1} \perp Y$.

Two nontrivial O(n,3) sets can be immediately constructed from a given O(n,3) set by noting the following. If $\{L_1,L_2,L_3\}$ is an O(n,3) set and if A,B,C and D are the Latin squares such that $L_1A = L_2$, $L_1B = L_3$, $L_2C = L_1$, and $L_2D = L_3$, then $\{L_1^{-1},A,B\}$ and $\{L_2^{-1},C,D\}$ are also O(n,3) sets.

Proposition 3.3. If L_1 and L_2 are two arbitrary Latin squares of order n and if L_1L_2 is a Latin square then $L_1 \perp L_1L_2$ and $L_1^{-1} \perp L_2$.

The following two lemmas were obtained from Mann [6]. The two corollaries following lemma 3.1 and the one following lemma 3.2 as well as theorem 3.2 are presented without proof.

Lemma 3.1. Let L be a Latin square of order n . If L^i, L^k, and L^{i-k} are Latin squares for i and k being two positive integers, then $L^k \perp L^i$ and $L^{i-k} \perp L^i$.

Corollary 3.1. If L is a Latin square such that L^2 is also a Latin square then $L \perp L^2$ and $L \perp L^{-1}$.

Corollary 3.2. If L is a Latin square of order n and if the L^i, i = 1,2,...,t, are Latin squares then $t \leq n-1$.

Lemma 3.2. $L = (p_1,p_2,\ldots,p_n)$ is a Latin square if and only if $p_ip_j^{-1}$ does not leave any symbol unchanged for $i \neq j$.

Corollary 3.3. Every cyclic permutation group of order n and degree n give rise to a Latin square of order n.

Definition 3.1. If $L = (p_1,p_2,\ldots,p_n)$ is a Latin square and if $G = \{p_1,p_2,\ldots,p_n\}$ forms a group then we say that L is based on the group G.

Theorem 3.1. Let $L = (p_1,p_2,\ldots,p_n)$ be any Latin square such that $\{p_1,p_2,\ldots,p_n\}$ is a cyclic permutation group. If $q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_t^{\alpha_t}$ is the prime power decomposition of n, then the set consisting of L, {L}, can be embedded in an $O(n,\lambda)$ set where $\lambda = q_1-1$ and where $q_1 = \min(q_1,q_2,\ldots,q_t)$ [5] .

Since a Latin square $L = (p_1,p_2,\ldots,p_n)$ can easily be obtained such that $G = \{p_1,p_2,\ldots,p_n\}$ is a cyclic permutation group and since $\lambda \geq 2$ for any odd number greater than unity, an $O(n,\lambda)$ set can easily be generated by the procedure of theorem 3.1. When $\lambda = n-1$, use of the method of this theorem produces a complete set of orthogonal Latin squares. No restriction is placed on the form of the generator of G, and this freedom is of importance in constructing certain classes of experimental designs.

If n, λ and L are defined as in theorem 3.1 and if n is a non-prime odd number we conjecture the following: The set $S = \{L,L^2,\ldots,L^\lambda\}$ which is an $O(n,\lambda)$ set (see [5]) cannot be embedded in an $O(n,\lambda+1)$ set.

Theorem 3.2. If $L = (p_1,p_2,\ldots,p_n)$ is a Latin square of order n and if $G = \{p_1,p_2,\ldots,p_n\}$ forms a (cyclic or not) permutation group, then there is no t such that $L^t \perp L$ if n is even [5].

This theorem demonstrates that if one has a Latin square of even order whose rows form a permutation group then it is pointless to search for an orthogonal mate to L through a power of L . The following restatement of a theorem previously published [5] shows that L is orthogonally mateless if this group is cyclic.

Theorem 3.3. If $L = (p_1,p_2,\ldots,p_n)$ is a Latin square of order n and if $G = \{p_1,p_2,\ldots,p_n\}$ forms a cyclic permutation group, then {L} cannot be embedded in an $O(n,2)$ set if n is even.

Definition 3.2. Two Latin squares L_1 and L_2 of order n on the set Σ are said to be equivalent or isomorphic if one can be derived from the other by some permutation of rows, and/or columns, and/or elements. The set of all equivalent Latin squares of order n on the set Σ is called a transformation set. A transformation set is said to be a cyclic transformation set if any (hence all)

members of the set is based on a cyclic permutation group. Note that there is only one cyclic transformation set with every family of Latin squares of order n.

A Latin square L of order n is said to be of degree r if L can be embedded in an $O(n,r)$ set, and r is the largest such integer. We now present a theorem for determining a lower bound for n even (odd) on the number of orthogonally mateless, degree 1 (at least of degree 2), Latin squares. An idea of the proportion of orthogonally mateless Latin squares is useful in searching for orthogonal mates using a computer and a random generation of squares.

Theorem 3.4. Let $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_t^{\alpha_t}$ be the prime power decomposition of n and let

$$W(n) = [(n-1)!]^3 \prod_{i=1}^{t} q_i / \prod_{i=1}^{t} (q_i - 1) \quad .$$

Then, (i) if n is even there exist at least W(n) Latin squares of order n having no orthogonal mates and (ii) if n is odd there exist at least W(n) Latin squares of order n having orthogonal mates.

To prove the theorem consider the n-set Σ on which the family of Latin squares is defined. The number of cyclic permutation groups of order n that can be formed from the n distinct symbols of Σ is $(n-1)!$. Also note that if σ is a generator of a cyclic permutation group G of order n on Σ then σ^k is also a generator for G for any k relatively prime to n. The preceding two facts together imply that we can only generate $(n-1)!/\phi(n)$ distinct cyclic permutation groups based on Σ, or equivalently there exist only $(n-1)!/\phi(n)$ standard Latin squares in the cyclic transformation set. $\phi(n)$ is the familiar Euler function and is the number of integers less than n and relatively prime to n. Also, from any given standard

Latin square $n!(n-1)!$ distinct Latin squares can be generated by row and column changes and these are all different from the Latin squares generated from any other standard Latin squares. Therefore, every cyclic transformation set contains $n!(n-1)![(n-1)!/\phi(n)]$ Latin squares. Since $\phi(n) = n(q_1-1)(q_2-1)\cdots(q_t-1)/q_1q_2\cdots q_t$, then the proof of (i) follows from theorem 3.3 and the proof of (ii) follows from theorem 3.1.

Some observations in the form of corollaries are presented below. These relate to the orthogonality of Latin squares of orders 3 to 7. A surprising result is the relatively large number of orthogonally mateless Latin squares of orders 4, 5, and 7.

Corollary 3.4. There is no orthogonally mateless Latin square of order 3.

There is only one transformation set associated with the family of Latin squares of order 3 [2]. This set is naturally cyclic. Hence, the proof of the corollary follows from theorem 3.1.

Corollary 3.5. If L is a Latin square of order 4 then either L is orthogonally mateless or S = {L} can be embedded in an $O(4,3)$ set.

In proving the corollary we note that the family of Latin squares of order 4 has two transformation sets [2] with one being cyclic. If L falls in the cyclic transformation set it is mateless by theorem 3.3. If L falls in the other transformation set, then {L} can be embedded in an $O(4,3)$ set. To prove the last statement it will be sufficient, using definition 3.2, to exhibit a non-cyclic Latin square L such that {L} can be embedded in an $O(4,3)$ set. As an example, let

$$L = \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{matrix} .$$

L is obviously not cyclic. L together with

$$L_1 = \begin{matrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{matrix} \quad \text{and} \quad L_2 = \begin{matrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{matrix} \quad \text{form an } O(4,3) \text{ set.}$$

Since $W(4) = 432$ and since there are 576 Latin squares of order 4, 3/4, or 75% of all Latin squares of order 4 are orthogonally mateless; the remaining 25% is a member of an $O(4,3)$ set. From this corollary we note that there is no $O(4,2)$ set which cannot be embedded in an $O(4,3)$ set.

Corollary 3.6. If L is a Latin square of order 5, then either L is orthogonally mateless or $S = \{L\}$ can be embedded in an $O(5,4)$ set.

From Fisher and Yates [2], we note that there are only two tranformation sets for Latin squares of order 5, with one of them being cyclic. If L falls in the cyclic set them $S = \{L\}$ can be embedded in an $O(5,4)$ set as shown in theorem 3.1. If L falls in the other transformation set then it is orthogonally mateless because this set is of the form $n = 4t+1$ and contains a sub-Latin square of order 2t [7]. As an example, the following Latin square of order 5 is non-cyclic and is orthogonally mateless because it contains a sub-latin square of order 2 (numbers underlined).

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 2 & \underline{4} & 1 & 5 & \underline{3} \\ 3 & 5 & 4 & 2 & 1 \\ 4 & 1 & 5 & 3 & 2 \\ 5 & \underline{3} & 2 & 1 & \underline{4} \end{matrix} .$$

Since $W(5) = 17,280$ and since there are 161,280 Latin squares of order 5; there are approximately 89% of all Latin squares of order 5 which are mateless.

Only about 11% can be a member of an $O(5,4)$ set. Note that this corollary states that there are no $O(5,2)$ and $O(5,3)$ sets which annot be embedded in an $O(5,4)$ set; it should also be pointed out that the last statement could be obtained from Shrikhande's [11] result stating that the existence of an $O(n,n-3)$ set, except for $n=4$, implies the existence of an $O(n,n-1)$ set.

Corollary 3.7. If L is a Latin square of order 6 then L is orthogonally mateless [2,10,12,13].

From theorem 3.4 $W(6) = 6!5!(60)$ is not a very good lower bound since 9408 standard Latin squares of order 6 have been enumerated (for example see [2]) resulting in a total of $6!5!(9408)$ Latin squares of order 6.

Corollary 3.8. If L is a Latin square of order 7 then L is orthogonally mateless, has only one mate, or can be embedded in an $O(7,6)$ set.

H. W. Norton (written communication) has used exhaustive enummerative techniques to study all possible Latin squares of order 7. 16,888,830 standard Latin squares of order 7 have been found to be orthogonally mateless, 53,130 standard Latin squares have been found to have only one mate, and only 120 standard Latin squares have been found to be in the complete $O(7,6)$ set. All $O(7,3)$, $O(7,4)$, and $O(7,5)$ sets can be embedded in an $O(7,6)$ set. From Shrikhande's results we know that the $O(7,4)$ and $O(7,5)$ sets can be embedded in an $O(7,6)$ set; the fact that an $O(7,3)$ set can also be embedded in an $O(7,6)$ set is interesting.

From theorem 3.4 we expect at least $7!6!(120)$ Latin squares which can be embedded in an $O(7,6)$ set. This agrees with H. W. Norton's results exactly in that he obtained 120 standard Latin squares or $7!6!(120)$ Latin squares of order 7 which can be embedded in an $O(7,6)$ set.

The above results are summarized in terms of standard Latin squares. To obtain the total number of squares in the class multiply the given number by $n!(n-1)!$.

TABLE I

Distribution of Standard Latin Squares of Orders 2 to 7 With Respect to the Degree of Orthogonality

	Number and Percent(%) of Standard Latin Squares					
n	$0((n,1))$	$0((n,2))$	$0((n,3))$	$0((n,4))$	$0((n,5))$	$0((n,6))$
2	1(100)	-	-	-	-	-
3	0(0)	1(100)	-	-	-	-
4	3(75)	0(0)	1(25)	-	-	-
5	50(89)	0(0)	0(0)	6(11)	-	-
6	9408(100)	0(0)	0(0)	0(0)	0(0)	-
7*	16,888,830	53,130	0(0)	0(0)	0(0)	120

* percentages are 99.6857, 0.3136, 0, 0, 0, and 0.0007, respectively.

The symbol $0((n,\lambda))$ means that an $0(n,\lambda)$ set cannot be embedded in an $0(n,\lambda+1)$ set, i.e., the set is locked. We know little or nothing for all $n > 7$. Sounds incredible, doesn't it? Unfortunately, it is true. Therefore, we are still far from being able to state that there are no further problems left to be solved in the theory of mutually orthogonal Latin squares, or that the theory of mutually orthogonal Latin squares is completely solved for prime power orders. For many the exhibition of one $0(n,n-1)$ set or equivalently one Latin square of order n and degree n-1 is the end of the theory for that n . They have not really bothered to ask themselves such questions as:

(a) How many non-isomorphic $O(n,n-1)$ sets do exist, if any at all? This question is very important. To cite merely one instance, if we know that there exists a unique $O(n,n-1)$ set except up to isomorphism, then we know the uniqueness of finite projective ~~geometry~~ plane for that order. The uniqueness of finite projective ~~geometry~~ plane is shown up to and including 8 (order 6 being excluded).

(b) How many non-isomorphic $O((n,i))$ sets, $i = 1,2,\ldots,n-2$ exist?

(c) How to exhibit those sets in (a) and (b)?

(d) etc.

Acknowledgement. The detailed and constructive comments of a referee were very useful in making the paper more readable and in correcting some errors. His efforts are greatly appreciated.

REFERENCES

[1] Bruck, R. H. (1963). Finite nets II, uniqueness and embedding. Pacific J. Math. 13:421-457.

[2] Fisher, R. A. and Yates, F. (1934). The 6 x 6 Latin squares. Proc. Camb. Phil. Soc. 30:492-507.

[3] Hall, M. Jr., Swift, J. D. and Walker, R. J. (1956). Uniqueness of the finite projective plane of order S. Math. Tables Aid Compt. 10:186-194.

[4] Hall, M. Jr. (1967). Combinatorial Theory. Blaisdell Pub. Co., Massachusetts.

[5] Hedayat, A. and Federer, W. T. (1969). An application of group theory to the existence and non-existence of orthogonal Latin squares. Biometrika, 56:547-551.

[6] Mann, H. B. (1942). The construction of orthogonal Latin squares. Ann. Math. Statist. 13:418-423.

[7] Mann, H. B. (1944). On orthogonal Latin squares. Amer. Math. Soc. Bull. 50:249-257.

[8] Parker, E. T. (1962). Non-extendability condition on mutually orthogonal Latin squares. Proc. Amer. Math. Soc. 13:219-221.

[9] Ryser, H. J. (1963). Combinatorial Mathematics. No. 14 of the Carus Math. Monographs. Published by the Math. Assoc. of Amer., Distributed by Wiley, New York.

[10] Saxena, P. N. (1950). A simplified method of enumerating Latin squares by MacMahon's differential operators I. J. Ind. Soc. Agric. Statist. 2:161-188.

[11] Shrikhande, S. S. (1961). A note on mutually orthogonal Latin squares. Sankhyā, Series A, 23:115-116.

[12] Tarry, G. (1900). Le problème des 36 officiers. C.R. Assoc. Fr. Av. Sci. 1:122-123.

[13] Tarry, G. (1901). Le problème des 36 officiers. C.R. Assoc. Fr. Av. Sci. 2:170-203.