RM-257 AH-3 ES-13
July 1970

ON A METHOD OF SUM COMPOSITION OF ORTHOGONAL LATIN SQUARES II*

By

A. Hedayat[1)] and E. Seiden

Michigan State University

* This research was supported by NIH GM-05900-11 grant at Cornell University and NSF Grang GP-20537 at Michigan State University.

1) On leave from Cornell University.

Summary

A new method of construction of Latin squares and orthogonal Latin squares is introduced here. We use a method of sum composition as contrasted with product composition used by other authors. We shall show that, under certain regularity condition, it is possible to construct a Latin square or order n by composition of two Latin squares of orders n_1 and n_2, $n_1 + n_2 = n$. Then we prove three theorems regarding the construction of a pair of orthogonal Latin squares of order $n = n_1 + n_2$. The first two theorems provide a method of construction of a pair of orthogonal Latin squares of order $n = n_1 + n_2$ for $n_1 \geq 7$ except $n_1 = 13$, where $n_1 = p^\alpha$, p an odd prime or $n_1 = 2^\alpha$, α a positive integer provided that $n_2 = (n_1 - 1)/2$ and $n_2 = n_1/2$ respectively. In the third theorem we shall exhibit a method of construction of a pair of orthogonal Latin squares of order $p^\alpha + 3$, $p \geq 7$ when p is a prime and has any of the following forms: $3m + 1$, $8m + 1$, $8m + 3$, $24m + 11$, $60m + 23$, and $60m + 47$. Obviously these results include an infinite collection of orthogonal Latin squares of order $4t + 2$. We have also indicated possibilities of obtaining more results in several directions.

1. Introduction. Perhaps one of the most useful techniques for the construction of combinatorial systems is the method of composition. To mention some, here are few well-known examples: 1) If there exists a set of t orthogonal Latin squares or order n_1 and if there exists a set of t orthogonal Latin squares of order n_2, then there exists a set of t orthogonal Latin squares of order n_1n_2. 2) If there are Steiner triple systems or order v_1 and v_2, there is a Steiner triple system of order $v = v_1v_2$. 3) If H_1 and H_2 are two Hadamard matrices of order n_1 and n_2 respectively, then the Kronecker product of H_1 and H_2 is a Hadamard matrix of order n_1n_2. 4) If Room squares of order n_1 and

n_2 exist, then a Room square of order n_1n_2 exists. 5) If BIB (v_1,k,λ_1) and BIB (v_2,k,λ_2) exist and if $f(\lambda_2v_2^2) \geq k$, then BIB $(v_1v_2,k,\lambda_1\lambda_2)$ exists where $f(\lambda_2v_2^2)$ denotes the maximum number of constraints which are possible in an orthogonal array of size $\lambda_2v_2^2$, with v_2 levels, strength 2, and index λ_2. 6) As a final example, the existence of orthogonal arrays $(\lambda_iv_i^t,q_i,v_1,t)$, $i = 1,2,\ldots,r$ implies the existence of an orthogonal array $(\lambda v^t,q,v,t)$, where $\lambda = \lambda_1\lambda_2\cdots\lambda_r$, $v = v_1v_2\cdots v_r$, and $q = \min(q_1,q_2,\ldots,q_r)$.

The reader will note that each of the above examples involved a product type composition. The method that we will describe utilizes a sum type composition, by means of which one can possibly construct sets of orthogonal Latin squares for all $n \geq 10$.

2. Definitions. In the sequel by an $O(n,t)$ set we mean a set of t mutually orthogonal Latin squares of order n.

a) A transversal (directrix) of a Latin square L of order n on an n-set Σ is a collection of n cells such that the entries of these cells exhaust the set Σ and every row and column of L is represented in this collection. Two transversals are said to be parallel if they have no cell in common.

b) A collection of n cells is said to form a common transversal for an $O(n,t)$ set if the collection is a transversal for each of these t Latin squares. Similarly, two common transversals are said to be parallel if they have no cell in common.

Example. The underlined and paranthesized cells form two parallel common transversals for the following $O(4,2)$ set.

$$\begin{array}{cccc} 1 & 2 & (3) & \underline{4} \\ (2) & \underline{1} & 4 & 3 \\ \underline{3} & (4) & 1 & 2 \\ 4 & 3 & \underline{2} & (1) \end{array} \qquad\qquad \begin{array}{cccc} 1 & 2 & (3) & \underline{4} \\ (4) & \underline{3} & 2 & 1 \\ \underline{2} & (1) & 4 & 3 \\ 3 & 4 & \underline{1} & (2) \end{array}$$

3. Composing Two Latin Squares of Order n_1 and n_2.

A very natural question in the theory of Latin squares is the following: Given two Latin squares L_1 and L_2 of order n_1 and n_2 $(n_1 \geq n_2)$ respectively. In how many ways can one compose L_1 and L_2 in order to obtain a Latin square L_3 of order m, where m is a function of n_1 and n_2 only? This question can be partially answered as follows. First, it is well-known that the Kronecker product $L_3 = L_1 \otimes L_2$ is a Latin square of order $m = n_1n_2$ irrespective of the combinatorial structure of L_1 and L_2. Secondly, we show that if L_1 has a certain combinatorial structure, then one can construct a Latin square L of order $n = n_1 + n_2$. Naturally enough we call this procedure a "method of sum composition".

Even though our method of sum composition does not work for all pairs of Latin squares, it has an immediate application in the construction of orthogonal Latin squares including those of order $4t + 2$, $t \geq 2$. We emphasize that the combinatorial structure of orthogonal Latin squares constructed by the method of sum composition is completely different from those of known orthogonal Latin squares in the literature. Therefore, it is worthwhile to study these squares for the purpose of constructing other combinatorial systems derivable from sets of mutually orthogonal Latin squares.

We shall now describe the method of "sum composition". Let L_1 and L_2 be two Latin squares of order n_1 and n_2, $n_1 \geq n_2$, on two non-intersecting sets $\Sigma_1 = \{a_1, a_2, \ldots, a_{n_1}\}$ and $\Sigma_2 = \{b_1, b_2, \ldots, b_{n_2}\}$ respectively. If L_1 has n_2 parallel transversals then we can compose L_1 with L_2 to obtain a Latin square L of order $n = n_1 + n_2$. Note that for any pair (n_1, n_2), there exists L_1 and L_2 with the above requirement, except for $(2,1)$, $(2,2)$, $(6,5)$ and $(6,6)$.

To produce L put L_1 and L_2 in the upper left and lower right corner respectively. Call the resulting square C_1, which looks as follows:

$$C_1 = \begin{array}{|c|c|} \hline L_1 & \\ \hline & L_2 \\ \hline \end{array}$$

Name the n_2 transversals of L_1 in any manner from 1 to n_2. Now fill the cell $(i, n_1 + k)$, $k = 1,2,\ldots,n_2$, with that element of transversal k which appears in row i, $i = 1,2,\ldots,n_1$. Fill also the cell $(n_1 + k,j)$, $k = 1,2,\ldots,n_2$, with that element of transversal k which appears in column j, $j = 1,2,\ldots,n_1$. Call the resulting square C_2. Now every entry of C_2 is occupied with an element either from Σ_1 or Σ_2, but C_2 is obviously not a latin square on $\Sigma_1 \cup \Sigma_2$. However, if we replace each of the n_1 entries of transversal k with b_k, it is easily verified that the resulting square which we call L is a latin square of order n on $\Sigma_1 \cup \Sigma_2$.

The procedure described for filling the first n_1 entries of the row (column) $n_1 + k$ with the corresponding entries of transversal k is, naturally enough, called <u>the projection of transversal k on the first n_1 entries of row (column) $n_1 + k$</u>.

We shall now elucidate the above procedure via an example. Let $\Sigma_1 = \{1,2,3,4,5\}$, $\Sigma_2 = \{6,7,8\}$,

$$L_1 = \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{matrix} \quad \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} \qquad \text{and} \qquad L_2 = \begin{matrix} 6 & 7 & 8 \\ 7 & 8 & 6 \\ 8 & 6 & 7 \end{matrix} \ .$$

Note that the cells on the same curve in L_1 form a transversal.

$$C_1 = \begin{array}{|ccccc|ccc|} \hline 1 & 2 & 3 & 4 & 5 & & & \\ 5 & 1 & 2 & 3 & 4 & & & \\ 4 & 5 & 1 & 2 & 3 & & & \\ 3 & 4 & 5 & 1 & 2 & & & \\ 2 & 3 & 4 & 5 & 1 & & & \\ \hline & & & & & 6 & 7 & 8 \\ & & & & & 7 & 8 & 6 \\ & & & & & 8 & 6 & 7 \\ \hline \end{array} \qquad \text{and} \qquad C_2 = \begin{array}{|ccccc|ccc|} \hline 1 & 2 & 3 & 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 & 2 & 3 & 4 \\ 3 & 4 & 5 & 1 & 2 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 & 3 & 4 & 5 \\ \hline 1 & 3 & 5 & 2 & 4 & 6 & 7 & 8 \\ 5 & 2 & 4 & 1 & 3 & 7 & 8 & 6 \\ 4 & 1 & 3 & 5 & 2 & 8 & 6 & 7 \\ \hline \end{array}$$

And finally

$$L = \left|\begin{array}{ccccc|ccc} 6 & 7 & 8 & 4 & 5 & 1 & 2 & 3 \\ 7 & 8 & 2 & 3 & 6 & 4 & 5 & 1 \\ 8 & 5 & 1 & 6 & 7 & 2 & 3 & 4 \\ 3 & 4 & 6 & 7 & 8 & 5 & 1 & 2 \\ 2 & 6 & 7 & 8 & 1 & 3 & 4 & 5 \\ \hline 1 & 3 & 5 & 2 & 4 & 6 & 7 & 8 \\ 5 & 2 & 4 & 1 & 3 & 7 & 8 & 6 \\ 4 & 1 & 3 & 5 & 2 & 8 & 6 & 7 \end{array}\right|$$

which is a Latin square of order 8 on $\Sigma_1 \cup \Sigma_2 = \{1,2,\ldots,8\}$.

Remark. Note that it is by no means required that the projection of transversals on the rows and columns should have the same ordering. Indeed, for the fixed set of ordered n_2 transversals, we have $n_2!$ choices of projections on columns and $n_2!$ choices of projections on the rows. Hence we can generate at least $(n_2!)^2$ different Latin squares of order $n = n_1 + n_2$ composing L_1 and L_2.

4. Constructinn of $O(n,2)$ Sets by Method of Sum Composition.

In order to construct an $O(n,2)$ set for $n = n_1 + n_2$, we require that $n_1 \geq 2n_2$ and there should exist an $O(n_2,2)$ set, and an $O(n_1,2)$ set with $2n_2$ parallel transversals. It is well known that any $n \geq 10$ can be decomposed into $n_1 + n_2$, $n_1 = p^\alpha$, $n_1 \geq 2n_2$, $n_2 \geq 3$, $n_2 \neq 6$. Thus for any $n \geq 10$ there is a corresponding n_1 and n_2 which fulfill the above requirement. We now present three theorems which state that for certain n one can construct an $O(n,2)$ set by the method of sum composition.

Theorem 4.1. *Let $n_1 = p^\alpha \geq 7$ for any odd prime p and positive integer α, excluding $n_1 = 13$. Then there exists an $O(n,2)$ set which can be constructed by composition of two $O(n_1,2)$ and $O(n_2,2)$ sets for $n_2 = (n_1-1)/2$ and $n = n_1 + n_2$.*

We shall first give the method of construction and then a proof that the constructed set is an $O(n,2)$ set.

Construction. Let $B(r)$ be the $n_1 \times n_1$ square with element $r\alpha_i + \alpha_j$ in its (i,j) cell, α_i, α_j, $0 \neq r$ in $GF(n_1)$, $i,j = 1,2,\ldots,n_1$. Then it is easy to see that $\{B(1),B(x),B(y)\}$, $x \neq y$, $y = x^{-1}$, is an $O(n_1,3)$ set. Consider the n_1 cells in $B(1)$ with $\alpha_i + \alpha_j = k$ a fixed element in $GF(n_1)$. Then the corresponding cells in $B(x)$ and $B(y)$ form a common transversal for the set $\{B(x),B(y)\}$. Name this common transversal by k. It is then obvious that two common transversals k_1 and k_2, $k_1 \neq k_2$ are parallel and hence $\{B(x),B(y)\}$ has n_1 common parallel transversals. Now let $\{A_1,A_2\}$ be any $O(n_2,2)$ set, which always exists, on a set Ω non-intersecting with $GF(n_1)$. For any λ in $GF(n_1)$ we can find $(n_1-1)/2$ pairs of distinct elements belonging to $GF(n_1)$ such that the sum of the two elements of each pair is equal to λ. Let S and T denote the collection of the first and the second elements of these $(n_1-1)/2$ pairs respectively. Note that for a fixed λ the set S can be constructed in $(n_1-1)(n_1-3)\ldots1$ distinct ways. Now fix λ and let L_1 denote any of the $(n_2!)^2$ Latin squares that can be generated by the sum composition of $L(x)$ and A_1 using transversals determined by the n_2 elements of S. Let L_2 be the Latin square derived from the composition of $L(y)$ and A_2 using the n_2 transversals determined by the elements of T and the following projection rule: Project transversals t_i, $i = 1,2,\ldots,n_2$ on the row (column) which upon superposition of L_2 on L_1 this row (column) should be superimposed on the row (column) stemmed from the transversal $\lambda-t_i$. Shortly we shall prove that $\{L_1,L_2\}$ forms an $O(n,2)$ set.

The preceding arguments show that $\{L_1,L_2\}$ can be constructed non-isomorphically in at least $(n_1-3)(n_2!)^2[n_1(n_1-1)(n_1-3)\ldots1]$ ways. For instance in the case of $n_1 = 7$, there is at least 12096 non-isomorphic pairs of orthogonal Latin squares of order 10. Therefore, Euler has been wrong in his conjecture by a very wide margin.

<u>Proof</u>. The constructional procedure clearly reveals that:

A. L_1 and L_2 are Latin squares of order n on $GF(n_1) \cup \Omega$.

B. Upon superposition of L_1 on L_2 the following are true:

b_1. Every element of Ω appears with every other element of Ω.

b_2. Every element of Ω appears with every element of $GF(n_1)$.

b_3. Every element of $GF(n_1)$ appears with every element of Ω.

Therefore, all we have to prove is that every element of $GF(n_1)$ appears with every other element of $GF(n_1)$. To prove this recall that $B(x)$ is orthogonal to $B(y)$. However, since we removed the n_2 transversals from $B(x)$ determined by the n_2 elements of S and n_2 transversals from $B(y)$ determined by the n_2 elements of T therefore the following $2n_2n_1$ pairs have been lost.

$$(x\alpha_i + \alpha_j, y\alpha_i + \alpha_j) \text{ with } \alpha_i + \alpha_j = \gamma \text{ for any } \gamma \in GF(n_1), \gamma \neq \lambda.$$

We claim that the given projection rules guarantee the capture of these lost pairs by the $2n_2n_1$ bordered cells. To show this note that the superposition of the projected transversal s from $B(x)$ on the projected transversal $t = \lambda - s$ from $B(y)$ will capture the n_1 pairs.

$$(x\alpha_i + \alpha_j, y\alpha_i + \alpha_j) \text{ with } \alpha_i + \alpha_j = k_1(s,t) = (yt + s)(1 + y)^{-1}$$

if these transversals have been projected on row border and n_1 pairs

$$(x\alpha_i + \alpha_j, y\alpha_i + \alpha_j) \text{ with } \alpha_i + \alpha_j = k_2(s,t) = (ys + t)(1 + y)^{-1}$$

if these transversals have been projected on column border. Now because $k + k' = \lambda$ and if $s_1 \neq s_2$ then $k_1 \neq k_2$ and $k_1' \neq k_2'$ hence the $2n_2n_1$ pairs which have been resulted from the projection of transversals determined by S and T will jointly capture the $2n_2n_1$ lost pairs and thus a proof.

We shall now clarify the above constructional procedure by an example.

Example. Let $n_1 = 7$, $GF(7) = \{0,1,2,\ldots,6\}$. Then for $x = 2$, $y = x^{-1} = 4$ we have

$\{B(1),B(2),B(4)\} =$

$$\begin{array}{ccccccc} 0&1&2&3&4&5&6\\ 1&2&3&4&5&6&0\\ 2&3&4&5&6&0&1\\ 3&4&5&6&0&1&2\\ 4&5&6&0&1&2&3\\ 5&6&0&1&2&3&4\\ 6&0&1&2&3&4&5 \end{array} \qquad \begin{array}{ccccccc} 0&1&2&3&4&5&6\\ 2&3&4&5&6&0&1\\ 4&5&6&0&1&2&3\\ 6&0&1&2&3&4&5\\ 1&2&3&4&5&6&0\\ 3&4&5&6&0&1&2\\ 5&6&0&1&2&3&4 \end{array} \qquad \begin{array}{ccccccc} 0&1&2&3&4&5&6\\ 4&5&6&0&1&2&3\\ 1&2&3&4&5&6&0\\ 5&6&0&1&2&3&4\\ 2&3&4&5&6&0&1\\ 6&0&1&2&3&4&5\\ 3&4&5&6&0&1&2 \end{array}$$

For $n_2 = (n_1-1)/2 = 3$ let $\Omega_2 = \{7,8,9\}$ and

$\{A_1,A_2\} = \begin{array}{ccc} 7&8&9\\ 8&9&7\\ 9&7&8 \end{array}, \begin{array}{ccc} 7&8&9\\ 9&7&8\\ 8&9&7 \end{array}$. Finally for $\lambda = 0$, $S = \{1,2,3\}$ and $T = \{6,5,4\}$ we have $\{L_1,L_2\} =$

$$\begin{array}{ccccccc|ccc} 0&7&8&9&4&5&6&1&2&3\\ 7&8&9&5&6&0&1&2&3&4\\ 8&9&6&0&1&2&7&3&4&5\\ 9&0&1&2&3&7&8&4&5&6\\ 1&2&3&4&7&8&9&5&6&0\\ 3&4&5&7&8&9&2&6&0&1\\ 5&6&7&8&9&3&4&0&1&2\\ \hline 2&1&0&6&5&4&3&7&8&9\\ 4&3&2&1&0&6&5&8&9&7\\ 6&5&4&3&2&1&0&9&7&8 \end{array} \qquad \begin{array}{ccccccc|ccc} 0&1&2&3&7&8&9&6&5&4\\ 4&5&6&7&8&9&3&2&1&0\\ 1&2&7&8&9&6&0&5&4&3\\ 5&7&8&9&2&3&4&1&0&6\\ 7&8&9&5&6&0&1&4&3&2\\ 8&9&1&2&3&4&7&0&6&5\\ 9&4&5&6&0&7&8&3&2&1\\ \hline 3&0&4&1&5&2&6&7&8&9\\ 6&3&0&4&1&5&2&9&7&8\\ 2&6&3&0&4&1&5&8&9&7 \end{array}$$

the reader can easily verify that $\{L_1,L_2\}$ is an $O(10,2)$ set.

Corollary 4.1. The method of Theorem 4.1 produces infinitely many pairs of orthogonal Latin squares of order $4t + 2$.

Proof. Let $p \equiv 7 \pmod 8$ and α odd, then $p^{\alpha} = (8t + 5)/3$ and thus $n_1 + n_2 = 4t + 2$.

Remark. The method of Theorem 4.1 fails for $n_1 = 13$ only because there is no $O(6,2)$ set. Otherwise, there will be no otthogonality contradiction on the other parts of L_1 and L_2 with their 6×6 lower right square missing.

Theorem 4.2. Let $n_1 = 2^{\alpha} \geq 8$ for any positive integer α. Then there exists an $O(n,2)$ set which can be constructed by composition of two $O(n_1,2)$ and $O(n_2,2)$ sets for $n_2 = n_1/2$ and $n = n_1 + n_2$.

We shall here give only the method of construction. A similar argument as in Theorem 4.1 can be used that the constructed set is an $O(n,2)$ set.

<u>Construction</u>. In a similar fashion as in Theorem 4.1 construct the set $\{B(1),B(x),B(y)\}$ over $GF(2^{\alpha})$. Let also $\{A_1,A_2\}$ be any $O(n_2,2)$ set, which always exists, on a set Ω non-intersecting with $GF(2^{\alpha})$. For any $\lambda \neq 0$ in $GF(2^{\alpha})$ we can find $n_1/2$ pairs of distinct elements belonging to $GF(2^{\alpha})$ such that the sum of the two elements of each pair is equal to λ. Let S and T denote the collection of the first and the second elements of these $n_1/2$ pairs respectively. Note that for a fixed λ the set S can be constructed in $n_1(n_1-2(n_1-4)\ldots 1$ distinct ways. Now form L_1 from the sum composition of $B(x)$ and A_1 and L_2 from the sum composition of $B(y)$ and A_2 using the same projection rule as given in Theorem 4.1. Now $\{L_1,L_2\}$ is an $O(n,2)$ set.

<u>Example</u>. Let $n = 8$, $GF(8) = \{0,1,2,\ldots,7\}$ with the following addition (+) and multiplication (X) tables:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	6	4	3	7	2	5
2	2	6	0	7	5	4	1	3
3	3	4	7	0	1	6	5	2
4	4	3	5	1	0	2	7	6
5	5	7	4	6	2	0	3	1
6	6	2	1	5	7	3	0	4
7	7	5	3	2	6	1	4	0

X	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	3	4	5	6	7	1
3	0	3	4	5	6	7	1	2
4	0	4	5	6	7	1	2	3
5	0	5	6	7	1	2	3	4
6	0	6	7	1	2	3	4	5
7	0	7	1	2	3	4	5	6

Then for $x = 2$, $y = x^{-1} = 7$ we have

$\{B(1),B(2),B(7)\}$ =

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
1	0	6	4	3	7	2	5	2	6	0	7	5	4	1	3	7	5	3	2	6	1	4	0
2	6	0	7	5	4	1	3	3	4	7	0	1	6	5	2	1	0	6	4	3	7	2	5
3	4	7	0	1	6	5	2	4	3	5	1	0	2	7	6	2	6	0	7	5	4	1	3
4	3	5	1	0	2	7	6	5	7	4	6	2	0	3	1	3	4	7	0	1	6	5	2
5	7	4	6	2	0	3	1	6	2	1	5	7	3	0	4	4	3	5	1	0	2	7	6
6	2	1	5	7	3	0	4	7	5	3	2	6	1	4	0	5	7	4	6	2	0	3	1
7	5	3	2	6	1	4	0	1	0	6	4	3	7	2	5	6	2	1	5	7	3	0	4

For $n_2 = n_1/2 = 4$ let $\Omega = \{A,B,C,D\}$ and

$$\{A_1,A_2\} = \begin{array}{cccc} A & B & C & D \\ B & A & D & C \\ C & D & A & B \\ D & C & B & A \end{array} , \begin{array}{cccc} A & B & C & D \\ D & C & B & A \\ B & A & D & C \\ C & D & A & B \end{array}$$

Finally for $\lambda = 5$, $S = \{0,1,3,4\}$ and $T = \{5,7,6,2\}$ we have

$\{L_1,L_2\} =$

$$\begin{array}{cccccccc|cccc}
A & B & 2 & C & D & 5 & 6 & 7 & 0 & 1 & 3 & 4 \\
B & A & 0 & D & C & 4 & 1 & 3 & 6 & 2 & 5 & 7 \\
3 & 4 & A & 0 & 1 & D & B & C & 7 & 5 & 2 & 6 \\
C & D & 5 & A & B & 2 & 7 & 6 & 1 & 0 & 4 & 3 \\
D & C & 4 & B & A & 0 & 3 & 1 & 2 & 6 & 7 & 5 \\
6 & 2 & D & 5 & 7 & A & C & B & 3 & 4 & 0 & 1 \\
7 & 5 & B & 2 & 6 & C & A & D & 4 & 3 & 1 & 0 \\
1 & 0 & C & 4 & 3 & B & D & A & 5 & 7 & 6 & 2 \\
\hline
0 & 6 & 7 & 1 & 2 & 3 & 4 & 5 & A & B & C & D \\
2 & 1 & 3 & 6 & 0 & 7 & 5 & 4 & B & A & D & C \\
4 & 7 & 6 & 3 & 5 & 1 & 0 & 2 & C & D & A & B \\
5 & 3 & 1 & 7 & 4 & 6 & 2 & 0 & D & C & B & A
\end{array}
\qquad
\begin{array}{cccccccc|cccc}
0 & 1 & D & 3 & 4 & A & C & B & 5 & 7 & 6 & 2 \\
7 & 5 & C & 2 & 6 & B & D & A & 0 & 1 & 3 & 4 \\
D & C & 6 & B & A & 7 & 2 & 5 & 3 & 4 & 0 & 1 \\
2 & 6 & B & 7 & 5 & C & A & D & 1 & 0 & 4 & 3 \\
3 & 4 & A & 0 & 1 & D & B & C & 7 & 5 & 2 & 6 \\
A & B & 5 & C & D & 2 & 7 & 6 & 4 & 3 & 1 & 0 \\
C & D & 4 & A & B & 0 & 3 & 1 & 6 & 2 & 5 & 7 \\
B & A & 1 & D & C & 3 & 0 & 4 & 2 & 6 & 7 & 5 \\
\hline
4 & 2 & 7 & 6 & 3 & 5 & 1 & 0 & A & B & C & D \\
6 & 3 & 0 & 4 & 2 & 1 & 5 & 7 & D & C & B & A \\
5 & 0 & 3 & 1 & 7 & 4 & 6 & 2 & B & A & D & C \\
1 & 7 & 2 & 5 & 0 & 6 & 4 & 3 & C & D & A & B
\end{array}$$

which is an $O(12,2)$ set.

<u>Theorem 4.3. If a prime p has one of the following forms:</u>

I $3m + 1$

II $8m + 1$

III $8m + 3$

IV $24m + 11$

V $60m + 23$

VI $60m + 47$

<u>then, using the method of sum composition, it is possible to construct a pair of orthogonal Latin squares of order $p^\alpha + 3$. The method of construction depends on the form of p but does not depend on its specific value.</u>

<u>Proof</u>. We start indicating the method of proof for one form of p, say, $p = 3m + 1$. Other cases can be handled analogously. In accordance with the previous notation we choose three mutually orthogonal Latin squares $B(1)$, $B(x)$ and $B(y)$ with $y \neq x$, $y = x^{-1}$. Let $S = \{s_1,s_2,s_3\}$ and

$T = \{t_1, t_2, t_3\}$ denote the transversals projected from the squares $B(x)$ and $B(y)$. Furthermore we shall in this case make the elements of the pairs (s_i, t_i) $i = 1,2,3$ belong to the $n_1 +$ ith rows and columns of the resulting squares of size n. The problem is now to examine under what conditions will the ranges of the two functions $k_1(s_i, t_i)$ and $k_2(s_i, t_i)$ exhaust the set $S \cup T$ and be compatible with the restriction that the six values of this set are distinct.

Lets choose the following values for $k_1(s_i, t_i)$ and $k_2(s_i, t_i)$

$$k_1(s_1, t_1) = s_2 \qquad k_2(s_1, t_1) = t_2$$
$$k_1(s_2, t_2) = s_3 \qquad k_2(s_2, t_2) = t_3$$
$$k_1(s_3, t_3) = s_1 \qquad k_2(s_3, t_3) = t_1 \,.$$

It is easy to establish that this system of equations will be consistent provided that $y^2 + 3 = 0$. Any four elements of the set $S \cup T$ can be expressed as linear combination of the remaining two arbitrarily chosen. This means when -3 is a quadratic residue of p or alternatively $p = 3m + 1$ the above pattern gives a uniform rule for constructing two orthogonal squares of size $p^\alpha + 3$ for $p = 3m + 1$.

Here is one solution satisfying the above pattern. In this system s_1 and s_3 are arbitrary and the remaining variables are expressed as linear functions of s_1 and s_3.

$$s_2 = s_1(1 - y)/2 + s_3(1 + y)/2$$
$$t_1 = s_1/y + s_3(y - 1)/y$$
$$t_2 = s_1(y - 1)/2y + s_3(y + 1)/2y$$
$$t_3 = s_1(1 + y)/y - s_3/y \,.$$

For each of remaining patterns we shall also give one system of solutinns satisfying it.

Next we shall list the patterns which will yield the remainder of the theorem.

For II and III let

$$k_1(s_1,t_1) = s_2 \qquad k_2(s_1,t_1) = s_3$$
$$k_1(s_2,t_2) = t_3 \qquad k_2(s_2,t_2) = t_1$$
$$k_1(s_3,t_3) = s_1 \qquad k_2(s_3,t_3) = t_2 \,.$$

This system will give a distinct set of values for $S \cup T$ provided that $2y^2 + 1 = 0$ i.e. -2 is a quadratic residue or alternatively $p = 8m + 1$ or $p = 8m + 3$.

Here is a solution for this system of equations:

$$s_2 = s_1(1 - y) + s_3 y$$
$$t_1 = -s_1 y + s_3(1 + y)$$
$$t_2 = -2s_1 y + s_3(1 + 2y)$$
$$t_3 = -s_1(2y - 1) + 2s_3 y$$

Case IV. Take now:

$$k_1(s_1,t_1) = s_2 \qquad k_2(s_1,t_2) = t_3$$
$$k_1(s_2,t_2) = s_3 \qquad k_2(s_2,t_3) = t_1$$
$$k_1(s_3,t_3) = s_1 \qquad k_2(s_3,t_1) = t_2$$

In this case the condition for consistent and distinct solutions becomes $4y^2 + 6y + 3 = 0$ i.e. -1 and 3 or -3 and 1 have to be quadratic residues. Clearly the second case yields a subset of primes obtained in case I. Hence we will consider only the case when -1 and 3 are quadratic residues i.e. $p = 24m + 11$.

The following is a solution to this system of equations.

$$s_2 = t_3(2y^3 + 2y^2 + y)/(y + 1) - s_1(2y^3 - 2y^2 - 1)/(y + 1)$$
$$s_3 = -t_3 y + s_1(y + 1)$$
$$t_1 = t_3(2y^2 + 2y + 1) - 2s_1(y + 1)y$$
$$t_2 = t_3(y + 1) - s_1 y \,.$$

To establish the cases V and VI we may choose:

$$k_1(s_1,t_1) = s_2 \qquad k_2(s_1,t_3) = t_1$$
$$k_1(s_2,t_2) = s_3 \qquad k_2(s_2,t_2) = t_3$$
$$k_1(s_3,t_3) = s_1 \qquad k_2(s_3,t_1) = t_2 \;.$$

The condition becomes now $2y^2 + 3y + 3 = 0$. Hence the distinct solutions will be obtained provided that -3 and 5 or 3 and -5 are quadratic residues. Again a new class will be obtained only in the second case i.e. if and only if $p = 60m + 23$ or $p = 60m + 47$.

One possible solution of this system of equations is the following:

$$s_1 = s_3/(y + 1) + t_3y/(y + 1)$$
$$s_2 = s_3(2y + 1)/(y + 1) - t_3y/(y + 1)$$
$$t_1 = -s_3(2y^2 + y)/(y + 1) + t_3(2y^2 + 2y + 1)/(y + 1)$$
$$t_2 = s_3y/(y + 1) + t_3/(y + 1).$$

This concludes the proof.

Corollary 4.3. Each of the six cases enumerated in Theorem 4.3 gives infinitely many pairs of orthogonal Latin squares of the form $4t + 2$.

The proof is obvious.

Remark. We wish to remark that the patterns used here to prove Theorem 4.3 are not unique. We do know all the patterns which could be used to establish the theorem. We know in fact all the patterns which could be used for constructing a pair of orthogonal Latin squares of order $p^\alpha + 3$ using the method of sum composition. However some of the patterns are hard to analyze and we were not yet successful to overcome the difficulties. We hope that the remaining patterns would enable us to extend the theorem to include all forms of p.

Discussion. The necessary requirements for the construction of an $O(n,t)$ set, $n = n_1 + n_2$, $t < n_2$, by the method of sum composition are: The existence of an $O(n_1,t)$ set, $n_1 \geq tn_2$, with at least tn_2 common parallel transversals, and an $O(n_2,t)$ set. These conditions are obviously satisfied whenever n_1 and n_2 are prime powers.

While for some values of n there exists only a unique decomposition fulfilling the above requirements, for infinitely many other values of n there are abundant such decompositions.

We believe the restriction $y = x^{-1}$ imposed in the preceeding three theorems is not necessary. Even though we have not yet been able to remove this restriction but we have sufficient evidence to believe that this restriction is unnecessary. In fact we conjecture that for any x and y, $x \neq 1$, $y \neq x$, there exist suitable sets S and T together with a proper projection for which one can use the method of sum composition to construct pairs of orthogonal Latin squares at least of those orders given in these three theorems. To support this conjecture we have fully investigated the case $10 = 7 + 3$. For this case let $S = \{0,1,3\}$ and $T = \{2,4,5\}$. Now we show that any pair of x and y satisfying the above restriction can be used to construct a pair of orthogonal Latin squares of order 10. To give the complete list of solution let (a_1,a_2,a_3) and (b_1,b_2,b_3) be any two permutations of the set $\{8,9,10\}$. If we project transversals $(0,1,3)$ on the rows (a_1,a_2,a_3) and columns (b_1,b_2,b_3) in the formation of L_1, then the following table indicates what permutation of transversals $\{2,4,5\}$ should be projected on the rows (a_1,a_2,a_3) and columns (b_1,b_2,b_3) in the formation of L_2. Obviously these permutation will be a function of the pair (x,y).

Pair (x,y)	Rows a_1,a_2,a_3	Columns b_1,b_2,b_3
(2,3)	4, 2, 5	4, 2, 5
(2,3)	2, 5, 4	2, 5, 4
(2,4)	2, 5, 4	4, 2, 5
(2,5)	4, 2, 5	4, 2, 5
(2,6)	2, 5, 4	2, 5, 4
(3,4)	2, 5, 4	2, 5, 4
(3,5)	2, 5, 4	4, 2, 5
(3,5)	4, 2, 5	5, 4, 2
(3,5)	4, 2, 5	2, 5, 4
(3,5)	5, 4, 2	2, 5, 4
(3,6)	4, 2, 5	2, 5, 4
(3,6)	5, 4, 2	4, 2, 5
(4,5)	2, 5, 4	2, 5, 4
(4,6)	5, 4, 2	4, 2, 5
(4,6)	2, 5, 4	2, 5, 4
(4,6)	5, 4, 2	5, 4, 2

(This table is by no means exhaustive.)

The reader may note that whenever $y = x^{-1}$ in the above table the given solution(s) are different from the one provided by the method of Theorem 4.1.

Thus we can conclude that any pair of orthogonal Latin squares of order 7 based on the GF(7) can be composed with a pair of orthogonal Latin squares of order 3 and make a pair of orthogonal Latin squares of order 10. In addition, since we have six choices for (a_1,a_2,a_3) and (b_1,b_2,b_3) hence from every line in the above table we can produce 36 non-isomorphic 0(10,2) sets or $16 \times 36 = 576$ sets for the entire table. Since all these pairs are non-isomorphic with all previous pairs, produced by Theorem 4.1, thus by the method of sum composition one can at least produce 12,672 non-isomorphic 0(10,2) sets.

We believe that for other values of n_1 there are sets of S and T together with proper projections which make the restriction $y = x^{-1}$ unnecessary.

Let $n_1 = p^{\alpha}$, α a positive integer, $n_1 \geq 7$ and n_2 any positive integer except 1, 2 and 6 such that $2n_2 \leq n_1$. Then we conjecture that there exists an $O(n,2)$ set based on Galois field $GF(n_1)$ which can be composed with any arbitrary $O(n_2,2)$ set to produce an $O(n,2)$ set, $n = n_1 + n_2$. To support his conjecture and shed more light on the method of sum composition we present here some highlights of the results which we hope to complete and submit for publication shortly.

In the following table for each decomposition of n we shall give the value of x, the sets S and T with the rules of projection on rows and columns. The reader can check for himself that the corresponding values of k_1 and k_2 will exhaust the set $S \cup T$. Having the values of n_1, n_2, x and S and T one can easily, by our method of sum composition, construct an $O(n,2)$ set based on Galois field $GF(n_1)$ and compose it with any arbitrary $O(n_2,2)$ set to obtain an $O(n,2)$ set. Note that one can construct two nonisomorphic $O(22,2)$ sets by composition of 19 and 3 (see Theorem 4.3) or composition of 17 and 5 (see the following table).

$n = n_1 + n_2$	x	Set S	Set T	Projection on Rows	Projection on Columns
15 = 11 + 4	2	0,1,2,3	6,7,8,9	(0,7),(1,9),(2,6),(3,8)	(0,8),(1,6),(2,9),(3,7)
17 = 13 + 4	5	0,1,2,3	8,9,10,11	(0,9),(1,8),(2,11),(3,10)	(0,9),(1,8),(2,11),(3,10)
18 = 13 + 5	2	0,1,2,3,4	7,8,9,10,11	(0,8),(1,11),(2,7),(3,10),(4,9)	(0,7),(1,9),(2,10),(3,11),(4,8)
22 = 17 + 5	2	0,1,2,3,4	9,10,11,12,13	(0,10),(1,11),(2,12),(3,13),(4,9)	(0,10),(1,11),(2,12),(3,13),(4,9)

Note: In this table (s,t) in the fifth and sixth columns indicate that transversal s and t of the Latin squares L_1 and L_2 should be projected on row (column) of L_1 and L_2 such that upon superposition of L_1 and L_2 the transversal s in L_1 should be superimposed on transversal t in L_2.

Acknowledgment

We wish to acknowledge with thanks a stimulating discussion with Professor B. Stewart while working on this paper. He also presented us with two special families of solutions for constructing pairs of orthogonal Latin squares of order $p^{\alpha} + 3$.

REFERENCES

Hall, Marshall, Jr. (1967). Combinatorial Theory. Blaisdell Publishing Company, Massachusetts.

Ryser, J.R. (1963). Combinatorial Mathematics, No. 14 of the Carus Mathematical Monographs, Published by the Amer. Math. Assoc. of Amer., Distributed by John Wiley and Sons, Inc.