I. CONSTRUCTION OF THREE MUTUALLY ORTHOGONAL LATIN SQUARES BY THE METHOD OF SUM COMPOSITION

II. GEOMETRICAL CONSTRUCTION OF NEW FAMILIES OF GENERALIZED YOUDEN DESIGNS

Dissertation for the Degree of Ph. D.

MICHIGAN STATE UNIVERSITY

CHING-JUNG WU

1976

This is to certify that the

thesis entitled

I. CONSTRUCTION OF THREE MUTUALLY ORTHOGONAL LATIN SQUARES BY THE METHOD OF SUM COMPOSITION.
II. GEOMETRICAL CONSTRUCTION OF NEW FAMILIES OF GENERALIZED YOUDEN DESIGNS

presented by

Ching-Jung Wu

has been accepted towards fulfillment
of the requirements for

Ph.D. degree in Statistics and Probability

Major professor

Date July 26, 1976

ABSTRACT

I. CONSTRUCTION OF THREE MUTUALLY ORTHOGONAL LATIN SQUARES BY THE METHOD OF SUM COMPOSITION

II. GEOMETRICAL CONSTRUCTION OF NEW FAMILIES OF GENERALIZED YOUDEN DESIGNS

By

Ching-Jung Wu

Two independent problems are considered in this thesis. The first problem contained in Chapters I and II deals with the construction of three orthogonal Latin squares by sum composition. In the second problem (Chapter III) new families of Generalized Youden Designs are constructed.

In Chapter II two methods of construction of three orthogonal Latin squares are discussed. We construct $O(n,3)$ sets by composition of an $O(n_1,3)$ and an $O(r,3)$ set with $n = n_1 + r$, where $n_1 = p^m$, p a prime, $r = \frac{p^m-1}{d}$, $d \geq 3$. Based on $GF(n_1)$, the $O(n_1,3)$ is formed by $B(x_1)$, $B(x_2)$, $B(x_3)$; where for any $\lambda \in GF(n_1)$, $\lambda \neq 0$, $B(\lambda)$ is the $n_1 \times n_1$ square with the element $\lambda\alpha_i + \alpha_j$ in its (i,j) cell, $\alpha_i, \alpha_j \in GF(n_1)$.

New families of GYD's for $v = s^m$, s a power of a prime, are constructed in Chapter III. The method of construction is geometrical. In particular this extends the construction of GYD's for $m = 2$ obtained by Ruiz and Seiden (1974). The designs constructed here would not have been obtained by the technique used in Ruiz and Seiden.

I. CONSTRUCTION OF THREE MUTUALLY ORTHOGONAL LATIN SQUARES BY THE METHOD OF SUM COMPOSITION

II. GEOMETRICAL CONSTRUCTION OF NEW FAMILIES OF GENERALIZED YOUDEN DESIGNS

By

Ching-Jung Wu

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Department of Statistics and Probability

1976

TO MY MOTHER

AND

CHIOU-YEE

ACKNOWLEDGMENTS

I wish to express my sincere appreciation to Dr. Esther Seiden, under whose direction this thesis was written, for her guidance and constant encouragement.

I would also like to thank Dr. Dennis C. Gilliland, Dr. James Hannan and Dr. Habib Salehi for their help in the final review of the manuscript . Thanks also go to the Department of Statistics and Probability, Michigan State University and the National Science Foundation for their financial support during my stay at Michigan State University. I would also like to thank Noralee Burkhardt who demonstrated both patience and skill in typing this dissertation.

TABLE OF CONTENTS

CHAPTER I

SUM COMPOSITION OF LATIN SQUARES

1.1 Introduction and Definitions

K. Yamamoto (1961) introduced the idea of constructing orthogonal Latin squares by a method of sum composition. The method has been generalized by R. Guerin (1966) and this author has christened it "Yamamoto's Method". A. Hedayat and E. Seiden (1969) introduced a simple method of constructing orthogonal Latin squares of order $n = n_1 + n_2$ provided that n_1 is a power of a prime. Their method of construction was based on some properties of $GF(n_1)$.

Horton (1974) extended a theorem of Hedayat and Seiden. Some further results were obtained by F. Ruiz and E. Seiden (1974). Yet all known results on Hedayat and Seiden's method of sum composition were concerned with the construction of two orthogonal Latin squares, until in 1973 Hedayat gave a construction of three orthogonal Latin squares of order 46. In his construction Hedayat used squares of order 41 and 5. It should be mentioned however that examples of three mutually orthogonal Latin squares constructed by the method of sum composition were available in the literature. Chi-Chi Shin (1965) published a paper in Chinese describing a construction of orthogonal Latin squares by the method of sum composition and presented three orthogonal Latin squares of order 46, 93, 106, 118, 154, with $n_1 = 41, 89, 101, 109, 137$ respectively. The construction of Shin was based on a special

representation of squares of order n_1 which applied to primes but not to powers of primes. In fact that construction could be considered a generalization of Parker's construction of two orthogonal Latin squares of order 10, although Parker did not refer to a method of sum composition.

This part of the thesis was inspired by that example of three mutually orthogonal Latin squares of order 46 constructed by Hedayat. We use sum composition, a general method of Headyat and Seiden, to construct three orthogonal Latin squares of order $n = n_1 + n_2$ where n_1 is a power of a prime and n_2 is an integer divisor of n_1-1. As a result of a theorem proved by P.J. Cameron et al. (1975), we can assert an effective construction of three mutally orthogonal Latin squares by the method of sum composition whenever it could be expected to be possible to carry it out. The result of this part of the thesis thus clears up a problem which has existed for at least six years in this area. It is our hope that this result will stimulate further research in this area and in other related areas as well.

Definition 1.1.1. A Latin square of order n is a square matrix with n^2 entries of n different elements, none of them occurring twice within any row or column of the matrix.

Definition 1.1.2. Two Latin squares of order n are orthogonal if upon superimposition each of the n^2 pairs occurs exactly once.

A system of two orthogonal Latin squares of order n will be referred to as a $O(n,2)$ set.

Definition 1.1.3. r Latin squares of order n are mutually orthogonal if any two of them are orthogonal.

A system of r mutually orthogonal Latin squares of order n will be referred to as a $O(n,r)$ set.

Definition 1.1.4. A transversal of a Latin square of order n is a set of n cells, exactly one in each row and column, such that all symbols appear exactly once as entries in the set.

Two or more transversals are parallel or disjoint if they have no cell in common.

Definition 1.1.5. A common transversal of a set of Latin squares of the same order is a set of cells which form a transversal for each square.

Example 1.1.1.

$$L_1 = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$$

$$L_2 = \begin{bmatrix} 1 & 2 & (3) & \underline{4} \\ \underline{2} & (1) & 4 & 3 \\ 3 & 4 & \underline{1} & (2) \\ (4) & \underline{3} & 2 & 1 \end{bmatrix} \qquad L_3 = \begin{bmatrix} 1 & 2 & (3) & \underline{4} \\ \underline{3} & (4) & 1 & 2 \\ 4 & 3 & \underline{2} & (1) \\ (2) & \underline{1} & 4 & 3 \end{bmatrix}$$

$$L_4 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$

L_1 is the only Latin square of order 2; it has no transverals at all.

The paranthesized cells and the underlined cells in L_2, L_3 form two common parallel transversals of the $O(4,2)$ set formed by L_2, L_3: The $O(4,3)$ set formed by L_2, L_3, L_4 has no common transversals.

1.2. Sum Composition of Two Latin Squares

Let L_1 and L_2 be two Latin squares of orders n_1 and n_2, $n_1 \geq n_2$, on two disjoint sets of varieties $\Sigma_1 = \{a_1, a_2, \ldots, a_{n_1}\}$ and $\Sigma_2 = \{b_1, b_2, \ldots, b_{n_2}\}$ respectively, and let L_1 have at least n_2 parallel transversals. Then we can compose L_1 with L_2 to obtain a Latin square L of order $n = n_1 + n_2$. Denote this Latin square by $L(L_1, L_2)$.

To produce $L(L_1, L_2)$ select arbitrary n_2 parallel transversals from L_1 and name the n_2 transversals of L_2 in any manner from 1 to n_2. In a square of order n fill the upper left and lower right corner with L_1 and L_2 respectively. Fill the cells $(i, n_1 + k)$, $k = 1,2,\ldots,n_2$, with that element of transversal k which appears in row i, $i = 1,2,\ldots,n_1$. Similarly fill the cells $(n_1 + k, j)$ $k = 1,2,\ldots,n_2$ with that element of transversal k which appears in column j, $j = 1,2,\ldots,n_1$. Finally replace each of the n_1 elements of transversal k with b_k, $k = 1,2,3,\ldots,n_2$, it is easily seen that the resulting square $L(L_1, L_2)$ is a Latin square of order n on $\Sigma_1 \cup \Sigma_2$.

The procedure just described of filling the first n_1 entries of column (row) $n_1 + k$ is called horizontal (vertical) projection of transversal k on column (row) $n_1 + k$, $k = 1,2,\ldots,n_2$.

Example 1.2.1. Let $\Sigma_1 = \{1,2,3\}$ and $\Sigma_2 = \{A,B\}$ and

$$L_1 = \begin{array}{ccc} \underline{1} & (2) & 3 \\ 2 & \underline{3} & (1) \\ (3) & 1 & \underline{2} \end{array} \qquad L_2 = \begin{array}{cc} A & B \\ B & A \end{array}$$

Note that the parenthesized and underlined cells of L_1 form two parallel transversals.

The resulting Latin square L is

$$L(L_1,L_2) = \begin{array}{ccccc} A & B & 3 & 1 & 2 \\ 2 & A & B & 3 & 1 \\ B & 1 & A & 2 & 3 \\ 1 & 3 & 2 & A & B \\ 3 & 2 & 1 & B & A \end{array}$$

1.3. Principles of Construction of $O(n,r)$ Sets by Means of Sum Composition.

We start with two important lemmas (Hedayat, 1973) which are needed in the construction of $O(n,r)$ sets.

Let $B(\gamma)$ be the $n_1 \times n_1$ square with elements $\gamma\alpha_i + \alpha_j$ in its (i,j) cell α_i,α_j, $\gamma \neq 0$ in $GF(n_1)$, the Galois field of order n_1, $i,j = 1,2,\ldots,n_1$ and let $L[B(\gamma)]$ be $n \times n$ square with $B(\gamma)$ in its $n_1 \times n_1$ top left corner subsquare, where $n > n_1$.

It is well known that $\{B(\lambda),B(x_1),B(x_2)\}$ form an $O(n,3)$ set if λ,x_1,x_2 are distinct non-zero. Note that the n_1 cells in $B(x_1)$ and $B(x_2)$ corresponding to the n_1 cells in $B(\lambda)$ with a fixed entry, say t, form a common transversal for $\{B(x_1),B(x_2)\}$. We call this transversal in $B(x_1)$ and $B(x_2)$ by $T(t)$. It is clear that as t goes over $GF(n_1)$ we have n_1 parallel transversals for $\{B(x_1),B(x_2)\}$.

Lemma 1.3.1. Let $B(\lambda)$, $B(x_1)$, $B(x_2)$, $L[B(x_1)]$, $L[B(x_2)]$ and $T(t)$ be defined as above, where λ, x_1,x_2 are non-zero elements in $GF(n_1)$ and $x_1 \neq x_2$. Then the n_1 pairs obtained by the vertical projection of transversal $T(t_1)$ in $B(x_1)$ and transversal $T(t_2)$

in $B(x_2)$ onto the same row of $L[B(x_1)]$ and $L[B(x_2)]$ are the same as the n_1 pairs obtained by transversal $T(K_v(\lambda,x_1,x_2,t_1,t_2)$ in $B(x_1)$ and in $B(x_2)$ where

$$K_v(\lambda,x_1,x_2,t_1,t_2) = \frac{x_1t_1(\lambda-x_2) - x_2t_2(\lambda-x_1)}{\lambda(x_1 - x_2)} \quad . \tag{1.3.1}$$

Note that the transversal $K_v(\lambda,x_1,x_2,t_1,t_2)$ will be referred to as transversal recovered by the vertical projections of $T(t_1)$ and $T(t_2)$.

Proof: The n_1 entries corresponding to transversal $T(t_1)$ in $B(x_1)$ can be written as

$$x_1\alpha_i + \alpha_j \quad \text{with} \quad \lambda\alpha_i + \alpha_j = t_1.$$

From the last equation above we get $\alpha_i = \frac{t_1 - \alpha_j}{\lambda}$.

Upon the vertical projection of transversal $T(t_1)$ onto the r-th row of $L[B(x_1)]$, we get the n_1 entries

$$x_1 \frac{t_1 - \alpha_j}{\lambda} + \alpha_j = \frac{x_1t_1}{\lambda} + \frac{\lambda - x_1}{\lambda} \alpha_j \ , \ j = 1,2,\ldots,n_1.$$

Note that the above expression has nothing to do with the value of r. Similarly, the n_1 entries of the r-th row of $L[B(x_2)]$ upon the vertical projection of transversal $T(t_2)$ onto it can be expressed in the following form

$$\frac{x_2t_2}{\lambda} + \frac{\lambda - x_2}{\lambda} \alpha_j \ : \ j = 1,2,\ldots,n_1.$$

Thus the n_1 pairs obtained by the n_1 entries of the r-th row of $L[B(x_1)]$ and $L[B(x_2)]$ are

$$\frac{x_1 t_1}{\lambda} + \left(\frac{\lambda - x_1}{\lambda}\alpha_j, \frac{x_2 t_2}{\lambda} + \frac{\lambda - x_2}{\lambda}\alpha_j\right) \quad j = 1,2,3,\ldots,n_1. \qquad (1)$$

Now suppose that there exists a transversal $T(K_v)$ in $B(x_1)$ and $B(x_2)$ such that the n_1 pairs obtained from the corresponding entries of this transversal is exactly the n_1 pairs given in (1). Then the n_1 pairs obtained from the corresponding cells of this transversal in $B(x_1)$ and $B(x_2)$ are

$$\left(\frac{x_1 K_v}{\lambda} + \alpha_j' \frac{\lambda - x_1}{\lambda}, \frac{x_2 K_v}{\lambda} + \alpha_j' \frac{\lambda - x_2}{\lambda}\right) \quad , j = 1,2,\ldots,n_1. \qquad (2)$$

The n_1 pairs in (1) and the n_1 pairs in (2) are the same, we obtained

$$\frac{x_1 t_1}{\lambda} + \alpha_j \frac{\lambda - x_1}{\lambda} = \frac{x_1 K_v}{\lambda} + \alpha_j' \frac{\lambda - x_1}{\lambda}$$

$$\frac{x_2 t_2}{\lambda} + \alpha_j \frac{\lambda - x_2}{\lambda} = \frac{x_2 K_v}{\lambda} + \alpha_j' \frac{\lambda - x_2}{\lambda} \quad .$$

If $x_2 \neq \lambda$, upon multiplication of the second equation by $\frac{\lambda - x_1}{\lambda - x_2}$ and its subtraction from the first equation we get:

$$\frac{x_1 t_1}{\lambda} - \frac{x_2 t_2}{\lambda} \frac{\lambda - x_1}{\lambda - x_2} = \frac{x_1 K_v}{\lambda} - \frac{x_2 K_v}{\lambda} \frac{\lambda - x_1}{\lambda - x_2}$$

which gives the following expression for K_v

$$K_v = \frac{x_1 t_1(\lambda - x_2) - x_2 t_2(\lambda - x_1)}{\lambda(x_1 - x_2)} \quad . \qquad \text{Q.E.D.}$$

Similarly we can prove the following.

Lemma 1.3.2. Assumption as in Lemma 1.3.1. Then the n_1 pairs obtained by the horizontal projection of transversal $T(t_1)$ in $B(x_1)$ and transversal $T(t_2)$ in $B(x_2)$ onto the same column of $L[B(x_1)]$ and

$L[B(x_2)]$ are the same as the n_1 pairs obtained by the transversal $T(K_h(\lambda,x_1,x_2,t_1,t_2))$ where

$$K_h(\lambda,x_1,x_2,t_1,t_2) = \frac{t_1(\lambda - x_2) - t_2(\lambda - x_1)}{x_1 - x_2} \quad . \tag{1.3.2}$$

Note the transversal K_h is referred as transversal recovered by the horizontal projection of $T(t_1)$ and $T(t_2)$.

The following corollaries are the immediate consequences of Lemma 1.3.1 and Lemma 1.3.2.

Corollary 1.3.1.

(i) $K_v(\lambda,x_1,x_2,t_1,t_2) = t_1$ or t_2 if and only if $t_1 = t_2$.

(ii) $K_h(\lambda,x_1,x_2,t_1,t_2) = t_1$ or t_2 if and only if $t_1 = t_2$.

Corollary 1.3.2. If $t_1 \neq t_2$, then

$$K_v(\lambda,x_1,x_2,t_1,t_2) + K_h(\lambda,x_1,x_2,t_1,t_2) = t_1 + t_2$$

if and only if $x_1x_2 = \lambda^2$.

The following lemma which can be thought of as the general principle for construction of two orthogonal Latin squares by sum composition is also an immediate consequence of the above lemmas and corollaries.

Lemma 1.3.3. Let $n_1 = p^\alpha$, p a prime and α a positive integer, and let n_2 be a positive integer such that $n_1 \geq 2n_2$ and two orthogonal Latin squares of order n_2 exist, say $\{L_1,L_2\}$.

If we can select distinct nonzero elements λ,x_1,x_2 in $GF(n_1)$, such that two sets of parallel transversals determined by the elements of $B(\lambda)$ in $B(x_i)$, say $T_i = \{T(t_{ij}): t_{ij} \in GF(n_1), j = 1,2,3,\ldots,n_2\}$, $i = 1,2$, exist, $T_1 \cap T_2 = \phi$ and such that there

exist n_2 pairs $\{(t_{1i},t_{2j})$: $i,j = 1,2,3,\ldots,n_2$, no two pairs having the same first or second component$\}$ such that

$$\{K_v(\lambda,x_1,x_2,t_{1i},t_{2j})\} \cup \{K_h(\lambda,x_1,x_2,t_{1i},t_{2j})\} = T_1 \cup T_2,$$

then $L(B(x_1),L_1)$ and $L(B(x_2),L_2)$ are orthogonal Latin squares of order $n = n_1 + n_2$.

Note $\{K_v(\lambda,x_1,x_2,t_{1i},t_{2j})\}$ and $\{K_h(\lambda,x_1,x_2,t_{1i},t_{2j})\}$ are usually denoted by $K_v(1,2)$ and $K_h(1,2)$ where the pair $(1,2)$ refers to the pair (x_1,x_2).

This lemma can be extended to a general principle for the construction of r mutually orthogonal Latin squares which we state in the following way.

Principle 1.3. Let $n_1 = p^{\alpha}$, p a prime and α a positive integer, and let n_2 be a positive integer such that $n_1 \geq rn_2$ and r mutually orthogonal Latin squares of order n_2 exist, say $\{L_1,L_2,\ldots,L_r\}$.

If we can select distinct nonzero elements $\lambda,x_1,x_2,x_3,\ldots,x_r$ in $GF(n_1)$, such that r sets of parallel transversals determined by the elements of $B(\lambda)$ in $B(x_i)$, say $T_i = \{T(t_{i1}),\ldots,T(t_{in_2})\}$, $i = 1,2,\ldots,r$, exists, $T_i \cap T_j = \phi$, $i \neq j$, and such that

$$K_v(i,j) \cup K_h(i,j) = T_i \cup T_j,\ i,j = 1,2,3,\ldots,r.$$

Then $\{L(B(x_1),L_1), L(B(x_2),L_2),\ldots,L(B(x_r),L_r)\}$ is an $O(n,r)$ set, where $n = n_1 + n_2$.

1.4. Known Results on the Method of Sum Composition

All the known results concerned with the construction of two orthogonal Latin squares by sum composition have been rigorously developed by Hedayat and Seiden, from 1969 to 1974. Ruiz and Seiden in 1972 have also discovered some new results in this area. Their works will be summarized as follows.

Hedayat and Seiden (1974) .

Theorem 1.4.1. If $n = n_1 + n_2$, $n_1 = p^\alpha \geq 7$ and $n_2 = [\frac{n_1}{2}]$, then an $0(n,2)$ design can be constructed by sum composition.

Theorem 1.4.2. If $n = n_1 + n_2$, $n_1 = p^\alpha \geq 7$ and $n_2 = 3$, then an $0(n,2)$ design can be constructed by sum composition.

Theorem 1.4.3. If $n = n_1 + n_2$, $n_1 = p^\alpha \geq 7$, $p = 4m+1$ or $8m+3$, $m = 1,2,3,\ldots$, and $n_2 = 4$, then an $0(n,2)$ design can be constructed by sum composition.

Theorem 1.4.4. If $n = n_1 + n_2$, $n_1 = p^\alpha \geq 13$, $p = 4m+1$, $m = 1,2,3,\ldots$, and $n_2 = 5$, then an $0(n,2)$ design can be constructed by sum composition.

Ruiz and Seiden (1974).

Theorem 1.4.5. If $n = n_1 + n_2$, $n_1 = p^\alpha \geq 11$, $p = 7m+1$, $7m+2$ or $7m+4$, $m = 1,2,3,\ldots$, and $n_2 = 4$, then an $0(n,2)$ design can be constructed by sum composition.

Theorem 1.4.6. If $n = n_1 + n_2$, $n_1 = p^\alpha$, and n_2 = even (excluding 2 and 6), $n_1 \geq 2n_2$, then one can construct an $0(n,2)$ design by sum composition.

CHAPTER II

CONSTRUCTION OF $O(p^n+r,3)$ SETS BY SUM COMPOSITION

2.1 Some Conditions for Construction of $O(p^n+r,3)$ Sets

Let p be a prime and $r = \frac{p^n-1}{d}$, where $d \geq 3$, $n = 1,2,3,\ldots$, $r \geq 3$. Let G be a multiplicative subroup of order r in the finite field $GF(p^n)$. Without loss of generality we may assume that G is generated by an element t in $GF(p^n)$, i.e. $G = \{1,t,t^2,t^3,\ldots,t^{r-1}\}$. Now consider the pairs $(t_1,t_2) = (t^u,t^{u+s_1})$, $(t_1,t_3) = (t^u,t^{u+s_2})$, $(t_2,t_3) = (t^u,t^{u+s_3})$, where s_1,s_2,s_3 are some fixed integers and $u = 0,1,2,\ldots,r-1$. By principle 1.3 if one can find elements $a,b,c,$ and distinct nonzero elements $,x_1,x_2,x_3$ in $GF(p^n)$ such that $a^{-1}b$, $b^{-1}c$, $c^{-1}a$ are all not in the subgroup G, and such that $\{K_v(\lambda,x_1,x_2,at_1,bt_2)\}$ captures $\{bt_2\}$, $\{K_h(\lambda,x_1,x_2,at_1,bt_2)\}$ captures $\{at_1\}$, $\{K_v(\lambda,x_1,x_3,at_1,ct_3)\}$ captures $\{ct_3\}$, $\{K_h(\lambda,x_1,x_3,at_1,ct_3)\}$ captures $\{at_1\}$, $\{K_v(\lambda,x_2,x_3,bt_2,ct_3)\}$ captures $\{ct_3\}$, $\{K_h(\lambda,x_2,x_3,bt_2,ct_3)\}$ captures $\{bt_2\}$, then three mutually orthogonal Latin squares of order p^n+r can be constructed if $O(r,3)$ sets exist. More precisely we may set up the following equations:

$$(2.1A)\quad \begin{cases} K_v(\lambda,x_1,x_2,at^u,bt^{u+s_1}) = bt^{u+s_1}\cdot t^k \\ K_h(\lambda,x_1,x_2,at^u,bt^{u+s_1}) = at^u\cdot t^m \end{cases} \qquad u = 0,1,2,3,\ldots,r-1$$

$$(2.1B)\quad \begin{cases} K_v(\lambda, x_1, x_3, at^u, ct^{u+s_2}) = ct^{u+s_2}\cdot t^i \\ K_h(\lambda, x_1, x_3, at^u, ct^{u+s_2}) = at^u\cdot t^j \end{cases} \qquad u = 0,1,2,3,\ldots,r-1$$

$$(2.1C)\quad \begin{cases} K_v(\lambda, x_2, x_3, bt^u, ct^{u+s_3}) = ct^{u+s_3}\cdot t^\ell \\ K_h(\lambda, x_2, x_3, bt^u, ct^{u+s_3}) = bt^u\cdot t^n \end{cases} \qquad u = 0,1,2,3,\ldots,r-1$$

for some integers $1 \le k,n,i,j,\ell,n < r$.

Now we consider the system (A) first, by equation (1.3.1) and (1.3.2) in Lemma 1.3.1 and Lemma 1.3.2 respectively, it follows that

$$(A')\quad \begin{cases} \dfrac{x_2(\lambda - x_1) - ab^{-1}t^{-s_1}x_1(\lambda - x_2)}{\lambda(x_2 - x_1)} = t^k, & 1 \le k < r \\ \dfrac{(x_2 - \lambda) - a^{-1}bt^{s_1}(x_1 - \lambda)}{x_2 - x_1} = t^m. & 1 \le m < r\ . \end{cases}$$

By the second equation of (A'),

$$x_2 = \frac{x_1(a^{-1}bt^{s_1} - t^m) - a^{-1}bt^{s_1}\lambda + \lambda}{1 - t^m} \qquad (1)$$

By (1) and first equation of (A'), the following computation can be easily carried out:

$$[x_1(a^{-1}bt^{s_1} - t^m) - a^{-1}bt^{s_1}\lambda + \lambda](\lambda - x_1) - ab^{-1}t^{-s_1}x_1[\lambda(1 - t^m)$$
$$- x_1(a^{-1}bt^{s_1} - t^m) + a^{-1}bt^{s_1}\lambda - \lambda] = \lambda t^k[x_1(a^{-1}bt^{s_1} - t^m)$$
$$- a^{-1}bt^{s_1}\lambda + \lambda - (1 - t^m)x_1]$$

or

$$x_1^2(1 - ab^{-1}t^{-s}1t^m - a^{-1}bt^s1 + t^m) + x_1(2a^{-1}bt^s1\lambda - 2\lambda - \lambda t^m$$
$$+ ab^{-1}t^{-s}1\lambda t^m + \lambda t^k - \lambda a^{-1}bt^s1t^k) + \lambda^2(1 - t^k)(1 - a^{-1}bt^s1) = 0$$

or

$$x_1^2(1 - ab^{-1}t^{-s}1t^m)(1 - a^{-1}bt^s1) + \lambda x_1(1 - a^{-1}bt^s1)(-2 + t^k$$
$$+ ab^{-1}t^{-s}1t^m) + \lambda^2(1 - t^k)(1 - a^{-1}bt^s1) = 0$$

or

$$[x_1(1 - ab^{-1}t^{-s}1t^m) - \lambda(1 - t^k)][x_1(1 - a^{-1}bt^s1) - \lambda(1 - a^{-1}bt^s1)] = 0.$$

under the assumption that $x_1 \neq \lambda$, $x_2 \neq \lambda$ and $a^{-1}b \notin G$. We must have

$$x_1 = \frac{\lambda(1 - t^k)}{1 - ab^{-1}t^{-s}1t^m} \tag{2}$$

By (1) and (2),

$$x_2 = \frac{\lambda(1 - a^{-1}bt^s1t^k)}{1 - t^m} . \tag{3}$$

It's clear that

$$x_1 = x_2 \quad \text{iff} \quad (1 - a^{-1}bt^s1)(t^k - ab^{-1}t^{-s}1t^m) = 0.$$

But $a^{-1}b \notin G$. Thus $x_1 \neq x_2$.

Similarly from system (B) and system (C) we should get the following solutions for x_1, x_3 and x_2, x_3 respectively.

$$X_1 = \frac{\lambda(1 - t^i)}{1 - ac^{-1}t^{-s_2}t^j} \tag{4}$$

$$X_3 = \frac{\lambda(1 - a^{-1}ct^{s_2}t^i)}{1 - t^j} \tag{5}$$

$$X_2 = \frac{\lambda(1 - t^\ell)}{1-bc^{-1}t^{-s_3}t^n} \tag{6}$$

$$X_3 = \frac{\lambda(1 - b^{-1}ct^{s_3}t^\ell)}{1 - t^n} \tag{7}$$

Note that

(B')

$$t^i = \frac{x_3(\lambda - x_1) - ac^{-1}t^{-s_2}x_1(\lambda - x_3)}{\lambda(x_3 - x_1)} \quad , 1 \le i < r$$

$$t^j = \frac{(x_3 - \lambda) - a^{-1}ct^{s_2}(x_1 - \lambda)}{x_3 - x_1} \quad , 1 \le j < r$$

(C')

$$t^\ell = \frac{x_3(\lambda - x_2) - bc^{-1}t^{-s_3}x_2(\lambda - x_1)}{\lambda(x_3 - x_2)} \quad , 1 \le \ell < r$$

$$t^n = \frac{(x_3 - \lambda) - b^{-1}ct^{s_3}(x_1 - \lambda)}{(x_3 - x_2)} \quad , 1 \le n < r .$$

(2) = (4) implies that

$$x_1 = \frac{\lambda(1 - t^k)}{1 - ab^{-1}t^{-s_1}t^m} = \frac{\lambda(1-t^i)}{1 - ac^{-1}t^{-s_2}t^j} \tag{2.1.1}$$

(3) = (6) implies that

$$x_2 = \frac{\lambda(1 - a^{-1}bt^{s_1}t^{k})}{(1 - t^{m})} = \frac{\lambda(1 - t^{\ell})}{1 - bc^{-1}t^{-s_3}t^{n}} \qquad (2.1.11)$$

(5) = (7) implies that

$$x_3 = \frac{\lambda(1 - a^{-1}ct^{s_2}t^{i})}{1 - t^{j}} = \frac{\lambda(1 - b^{-1}ct^{s_3}t^{\ell})}{1 - t^{n}} \qquad (2.1.111)$$

From now on we assume that $t^{k+m} = t^{i+j} = t^{\ell+n} = 1$. By (2.1.111),

$$1 - ac^{-1}t^{-s_2}t^{j} = \frac{ab^{-1}t^{s_3-s_2}t^{\ell-i}(1 - t^{j})(1 - bc^{-1}t^{-s_3}t^{n})}{(1 - t^{n})}.$$

This and (2.1.1) imply that

$$\frac{1}{1 - bc^{-1}t^{-s_3}t^{n}} = \frac{(1 - t^{k})(1 - t^{j})ab^{-1}t^{s_3-s_2}t^{\ell-i}}{(1 - t^{n})(1 - t^{i})(1 - ab^{-1}t^{-s_1}t^{m})}$$

The last equation and (2.1.11) then implies that

$$\frac{(1 - t^{\ell})(1 - t^{k})(1 - t^{j})ab^{-1}t^{s_3-s_2}t^{\ell-i}}{(1 - t^{n})(1 - t^{i})(1 - ab^{-1}t^{-s_1}t^{m})} = \frac{1 - a^{-1}bt^{s_1}t^{k}}{1 - t^{m}} .$$

Since $t^{\ell+n} = t^{i+j} = t^{m+k} = 1$, it follows immediately from the last equation above that

$$(1 - a^{-1}bt^{s_1}t^{k})^2 = (1 - t^{k})^2t^{s_3-s_2+s_1}t^{2(\ell-i)}.$$

If $t^{s_3-s_2+s_1}$ is a quadratic residue, this is true when t has even index or $s_3 = s_2 + s_1$ is chosen to be zero or even integer, then we get the following solution

$$a^{-1}b = \frac{1 \mp (1 - t^k)t^p}{t^{s_1+k}}$$

where $2p = s_3 - s_2 + s_1 + 2(\ell-i) \pmod r$.

From (2.1.I) and (2.1.II)

$$ac^{-1} = \frac{[1 \mp (1 - t^k)t^p] - [\mp (1 - t^i)t^p]}{[1 \mp (1 - t^k)t^p]t^{-s_2+j}}$$

$$1 - a^{-1}ct^{s_2}t^i = \frac{\pm (1 - t^i)t^p}{[1 \mp (1 - t^k)t^p] - [\mp (1 - t^i)t^p]} \tag{8}$$

and

$$bc^{-1} = \frac{t^{p+k} \pm (1 - t^\ell)}{t^{-s_3+n+p+k}}$$

$$1 - b^{-1}ct^{s_3+\ell} = \frac{\pm (1 - t^\ell)}{t^{p+k} \pm (1 - t^\ell)} \tag{9}$$

Taking upper sign in (8) and (9) and substituting the right hand sides of (8) and (9) for $1 - a^{-1}ct^{s_2+i}$ and $1 - b^{-1}ct^{s_3+\ell}$ respectively in (2.1.III), we find that

$$\frac{t^\ell}{t^{p+k} + 1 - t^\ell} = \frac{t^{p+i}}{1 + t^{p+k} - t^{p+i}}.$$

This implies that $t^{p+i-\ell} = 1$ provided that $1 + t^{p+k} \neq 0$. But $2p = s_3 - s_2 + s_1 + 2(\ell-i) \pmod r$. We must have $s_3 - s_2 + s_1 \equiv 0 \pmod r$. Hence we have the following theorem:

Theorem 2.1.1. Under the set-up (2.1a), (2.1b), (2.1c) and the assumption that $t^{m+k} = t^{\ell+n} = t^{i+j} = 1$, the necessary and sufficient condition for $a^{-1}b$, bc^{-1} and ac^{-1} having

solution is that $s_3 - s_2 + s_1 \equiv 0 \pmod r$. In this case the solution is given by

$$a^{-1}b = \frac{1 - t^p + t^{p+k}}{t^{s_1+k}}$$

$$bc^{-1} = \frac{1 - t^{\ell} + t^{p+k}}{t^{-s_3+k+j}}$$

and

$$ac^{-1} = \frac{1 - t^{\ell} + t^{p+k}}{(1 - t^p + t^{p+k}) \cdot t^{-s_2+j}}$$

where $p = \ell + j \pmod r$.

In order to assure an effective construction of three mutually orthogonal Latin squares of order $p^n + r$, we must have solutions for $a^{-1}b$, bc^{-1} and ac^{-1} to be such that $a^{-1}b$, bc^{-1} and ac^{-1} are all not in the subgroup G.

Theorem 2.1.2. Under the assumptions that $t^{m+k} = t^{\ell+n} = t^{i+j} = 1$ and $s_3 - s_2 + s_1 \equiv 0 \pmod r$, if there exists a, $1 \leq a \leq r$, such that the set $\{1 + t^a - t^b : t^b \in G_r\}$ distributes in at least three cosets associated with the subgroup G_r, then we can construct three orthogonal Latin squares of order $p^n + r$ by sum composition provided that three orthogonal Latin squares of order r exists

Proof. By Theorem 2.1.1 with $p + k = \ell + j + k = a$.

Remark 2.1.1. If we take lower sign in (8) and (9), similarly as above, we get very easily that the consistency of the solutions for $a^{-1}b$, bc^{-1} and ac^{-1} implies that $t^{p+i-\ell} = -1$. This means that one may

take lower sign in (8) and (9) when r is even. But when r is even it's readily seen that this is a special case of Theorem 2.1.2.

Remark 2.1.2. For computational convenience, we may choose $a = 0$ and search for two elements in the set $\{2 - t^i : t^i \in G_r\}$ such that they are in the different cosets (other than the group G_r itself).

Remark 2.1.3. In Theorem 2.1.2 the condition that the set $\{1 + t^a - t^b : t^b \in G_r\}$ intersects at least three cosets of G_r is the same as that in Chi -Chi Shin's (1965) first solution for construction of $O(p + r,3)$ set.

Remark 2.1.4. The values of x_1, x_2, x_3 can be found as follows:

By (2) and (3) $$x_1x_2 = \lambda^2 a^{-1} b t^{s_1+2k}$$

By (4) and (5) $$x_1x_3 = \lambda^2 a^{-1} c t^{s_2+2i}$$

By (6) and (7) $$x_2x_3 = \lambda^2 b^{-1} c t^{s_3+2\ell} .$$

From the above three equations, it follows that

$$x_1^2 = \lambda^2 (a^{-1}b)^2 t^{2(s_1+k+i-\ell)} .$$

Therefore

$$x_1 = -\lambda (a^{-1}b) t^{s_1+k-j-\ell} \tag{10}$$

$$x_2 = -\lambda\, t^{k+j+\ell} \tag{11}$$

and

$$x_3 = -\lambda (b^{-1}c) t^{s_3-k+\ell-j} \tag{12}$$

where $\lambda \neq 0$ and $\lambda \in GF(p^n)$.

<u>Example 2.1.1.</u> $p = 13$. $\frac{p-1}{3} = 4 = r$.

A subgroup of order 4 is $G_4 = \{1,2^3,2^6,2^9\} = \{1,8,12,5\}$. The set $\{2-t^i : t^i \in G_4\} = \{1,7,3,10\}$. It is clear that 7 and 3 are in different cosets. Since $2 - t = 7$ and $2 - t^2 = 3$, by Theorem 2.1.1 and Theorem 2.1.2. We may take $t^{p+k} = t^{\ell+j+k} = 1$ and $t^{\ell} = t$, $t^{\ell+j} = t^2$, i.e. we may take $\ell = 1$, $\ell + j = 2$ and $\ell + j + k = 4$. Since $s_3 - s_2 + s_1 = 0 \pmod 4$, the following solutions for $k,m,i,j,\ell,n,s_1,s_2,s_3$ can be chosen:

$k = 2$	$i = 3$	$\ell = 1$	$s_1 = 2$
$m = 2$	$j = 1$	$n = 3$	$s_2 = 0$
			$s_3 = 2$

Then by Theorem 2.1.1,

$$a^{-1}b = 3, \quad bc^{-1} = 9, \quad ac^{-1} = 3 .$$

We may take $a = 1$, then $b = 3$, $c = 9$. We may take $\lambda = 1$, then by Remark 2.1.4,

$$x_1 = 3, \quad x_2 = 12, \quad x_3 = 10.$$

$$\{(at_1,bt_2)\} = \{(t^u,3t^{u+s_1}) : u = 0,1,2,3,\ s_1 = 2\}$$
$$= \{(1,10),\ (8,2),\ (12,3),\ (5,11)\}.$$

$$\{(at_1,ct_3)\} = \{(t^u,9t^{u+s_2}) : u = 0,1,2,3,\ s_2 = 0\}$$
$$= \{(1,9),\ (8,7),\ (12,4),\ (5,6)\}.$$

$$\{(bt_2,ct_3)\} = \{(3t^u, 9t^{u+s_3}) : u = 0,1,2,3,\ s_3 = 2\}$$
$$= \{(3,4),\ (11,6),\ (10,9),\ (2,7)\}.$$

$$\{K_v(\lambda,x_1,x_2,at_1,bt_2)\} = \{bt^{u+s_1+k} : b = 3,\ u = 0,1,2,3,\ s_1 = 2,\ k = 2\}$$
$$= \{3,11,10,2\}.$$

$$\{K_h(\lambda,x_1,x_2,at_1,bt_2)\} = \{at^{u+m} : a = 1,\ u = 0,1,2,3,\ m = 2\}$$
$$= \{12,5,1,8\}.$$

$$\{K_v(\lambda,x_1,x_3,at_1,ct_3)\} = \{ct^{u+s_2+i} : c = 9,\ u = 0,1,2,3,\ s_2 = 0,\ i = 3\}$$
$$= \{6,9,7,4\}.$$

$$\{K_h(\lambda,x_1,x_3,at_1,ct_3)\} = \{at^{u+j} : a = 1,\ u = 0,1,2,3,\ j = 1\}$$
$$= \{8,12,5,1\}.$$

$$\{K_v(\lambda,x_2,x_3,bt_2,ct_3)\} = \{ct^{u+s_3+\ell} : c = 9,\ u = 0,1,2,3,\ s_3 = 2,\ \ell = 1\}$$
$$= \{6,9,7,4\}.$$

$$\{K_h(\lambda,x_2,x_3,bt_2,ct_3)\} = \{bt^{u+n} : b = 3,\ u = 0,1,2,3,\ n = 3\}$$
$$= \{2,3,11,10\}.$$

It is clear from the above that transversals at_1, bt_2 and ct_3 are mutually exclusive, moreover $\{at_1\} \cup \{bt_2\} = \{K_v(\lambda,x_1,x_2,at_1,bt_2)\} \cup \{K_h(\lambda,x_1,x_2,at_1,bt_2)\}$, $\{at_1\} \cup \{ct_3\} = \{K_v(\lambda,x_1,x_3,at_1,ct_3)\} \cup \{K_h(\lambda,x_1,x_3.at_1,ct_3)\}$ and $\{bt_2\} \cup \{ct_3\} = \{K_v(\lambda,x_2,x_3,bt_2,ct_3)\} \cup \{K_h(\lambda,x_2,x_3,bt_2,ct_3)\}$. Therefore by principle 1.3 three orthogonal Latin squares of order 17 can be constructed by sum composition. They are constructed as follows.

$L(B(3),L_1)$ $\{at_1\} = \{1,8,12,5\}$

0	A	2	3	4	D	6	7	B	9	10	11	C	1	8	12	5
A	4	5	6	D	8	9	B	11	12	0	C	2	3	10	1	7
6	7	8	D	10	11	B	0	1	2	C	4	A	5	12	3	9
9	10	D	12	0	B	2	3	4	C	6	A	8	7	1	5	11
12	D	1	2	B	4	5	6	C	8	A	10	11	9	3	7	0
D	3	4	B	6	7	8	C	10	A	12	0	1	11	5	9	2
5	6	B	8	9	10	C	12	A	1	2	3	D	0	7	11	4
8	B	10	11	12	C	1	A	3	4	5	D	7	2	9	0	6
B	12	0	1	C	3	A	5	6	7	D	9	10	4	11	2	8
1	2	3	C	5	A	7	8	9	D	11	12	B	6	0	4	10
4	5	C	7	A	9	10	11	D	0	1	B	3	8	2	6	12
7	C	9	A	11	12	0	D	2	3	B	5	6	10	4	8	1
C	11	A	0	1	2	D	4	5	B	7	8	9	12	6	10	3
3	1	12	10	8	6	4	2	0	11	9	7	5	A	B	C	D
11	9	7	5	3	1	12	10	8	6	4	2	0	B	A	D	C
10	8	6	4	2	0	11	9	7	5	3	1	12	C	D	A	B
2	0	11	9	7	5	3	1	12	10	8	6	4	D	C	B	A

where $L_1 =$

A	B	C	D
B	A	D	C
C	D	A	B
D	C	B	A

$L(B(12),L_2)$, $\{bt_2\} = \{10,2,3,11\}$

0	1	B	C	4	5	6	7	8	9	A	D	12	10	2	3	11
12	B	C	2	3	4	5	6	7	A	D	10	11	8	0	1	9
B	C	0	1	2	3	4	5	A	D	8	9	10	6	11	12	7
C	11	12	0	1	2	3	A	D	6	7	8	B	4	9	10	5
9	10	11	12	0	1	A	D	4	5	6	B	C	2	7	8	3
8	9	10	11	12	A	D	2	3	4	B	C	7	0	5	6	1
7	8	9	10	A	D	0	1	2	B	C	5	6	11	3	4	12
6	7	8	A	D	11	12	0	B	C	3	4	5	9	1	2	10
5	6	A	D	9	10	11	B	C	1	2	3	4	7	12	0	8
4	A	D	7	8	9	B	C	12	0	1	2	3	5	10	11	6
A	D	5	6	7	B	C	10	11	12	0	1	2	3	8	9	4
D	3	4	5	B	C	8	9	10	11	12	0	A	1	6	7	2
1	2	3	B	C	6	7	8	9	10	11	A	D	12	4	5	0
3	5	7	9	11	0	2	4	6	8	10	12	1	A	B	C	D
11	0	2	4	6	8	10	12	1	3	5	7	9	C	D	A	B
10	12	1	3	5	7	9	11	0	2	4	6	8	D	C	B	A
2	4	6	8	10	12	1	3	5	7	9	11	0	B	A	D	C

where $L_2 =$

A	B	C	D
C	D	A	B
D	C	B	A
B	A	D	C

$L(B(10), L_3)$, $\{ct_3\} = \{9,7,4,6\}$

0	1	2	3	C	5	D	B	8	A	10	11	12	9	7	4	6
10	11	12	C	1	D	B	4	A	6	7	8	9	5	3	0	2
7	8	C	10	D	B	0	A	2	3	4	5	6	1	12	9	11
4	C	6	D	B	9	A	11	12	0	1	2	3	10	8	5	7
C	2	D	B	5	A	7	8	9	10	11	12	0	6	4	1	3
11	D	B	1	A	3	4	5	6	7	8	9	C	2	0	10	12
D	B	10	A	12	0	1	2	3	4	5	C	7	11	9	6	8
B	6	A	8	9	10	11	12	0	1	C	3	D	7	5	2	4
2	A	4	5	6	7	8	9	10	C	12	D	B	3	1	11	0
A	0	1	2	3	4	5	6	C	8	D	B	11	12	10	7	9
9	10	11	12	0	1	2	C	4	D	B	7	A	8	6	3	5
6	7	8	9	10	11	C	0	D	B	3	A	5	4	2	12	1
3	4	5	6	7	C	9	D	B	12	A	1	2	0	11	8	10
12	3	7	11	2	6	10	1	5	9	0	4	8	A	B	C	D
5	9	0	4	8	12	3	7	11	2	6	10	1	D	C	B	A
1	5	9	0	4	8	12	3	7	11	2	6	10	B	A	D	C
8	12	3	7	11	2	6	10	1	5	9	0	4	C	D	A	B

where

$L_3 =$

A	B	C	D
D	C	B	A
B	A	D	C
C	D	A	B

2.2. Construction of $O(p^n+r,3)$ sets when $r = 4, 5$ and 7.

In this section one assumes that p is an odd prime and $\frac{p^n-1}{d} = r$, where $d \geq 3$, $r \geq 3$. Although for $r = 3$, three orthogonal Latin squares of order $p^n + 3$ cannot be constructed by sum composition, yet there exists a, $1 \leq a \leq 3$, such that the set $\{1 + t^a - t^b : t^b \in G_r = \{1,t,t,t^2\}\}$ distributes in at least three cosets. The proof of this and that of the cases for $r = 4,5,6$ are all similar to each other. Thus only a complete proof for $r = 7$ will be given.

Theorem 2.2.1. For $r = 3$, if $p \neq 7$, then $\{2 - t^i : t^i \in G_r = \{1,t,t^2\}\}$ distributes in three cosets.

Theorem 2.2.2. For $r = 4$, if $p \geq 7$, then $\{2 - t^i : t^i \in G_r = \{1,t,t^2,t^3\}\}$ distributes in at least three cosets. Hence three orthogonal Latin squares of order $p^n + 4$ can be constructed by sum composition.

Theorem 2.2.3. For $r = 5$, if $p \neq 11$, then $\{1 + t - t^i : t^i \in G_r = \{1,t,t^2,t^3,t^4\}\}$ distributes in at least three cosets. Hence three orthogonal Latin squares of order $p^n + 5$ can be constructed by sum composition.

Theorem 2.2.4. For $r = 7$. $p \neq 29$, the set $\{1 + t^2 - t^i : t^i \in G_r = \{1,t,t^2,t^3,t^4,t^5,t^6\}\}$ distributes in at least three cosets. Hence three orthogonal Latin squares of order $p^n + 7$ can be constructed by sum composition.

In order to prove Theorem 2.2.4, we need the following lemmas.

Lemma 2.2.1. Let $d \cdot r = p^n - 1$, $d \geq 3$, $r \geq 3$, and e be a primitive root in $GF(p^n)$. If $G_r = \{1, t, t^2, \ldots, t^{r-1}\}$, with $t = e^d$, is a multiplicative subgroup of order r in $GF(p^n)$ and if $0 \leq m, k_1, k_2, \ell_1, \ell_2 \leq r - 1$, $k_1 \neq k_2$, $1 + t^m \neq 0$, $k_2 - k_1 = \pm (\ell_2 - \ell_1) \bmod r$. Then the following system (*) cannot hold.

$$(*) \qquad \begin{aligned} 1 + t^m - t^{k_1} &= e^i t^{\ell_1} \\ 1 + t^m - t^{k_2} &= e^i t^{\ell_2} \end{aligned}$$

where $0 \leq i < d$. In other words, if $1 + t^m - t^{k_1} = e^i t^{\ell_1}$, then

$$1 + t^m - t^{k_2} \neq e^i t^{\ell_1 + k_2 - k_1} \quad \text{or} \quad e^i t^{\ell_1 - k_2 + k_1} .$$

Proof. Assume the system (*) holds. Then we would have

$$t^{k_2} - t^{k_1} = e^i (t^{\ell_1} - t^{\ell_2})$$

i.e.
$$t^{k_1}(t^{k_2 - k_1} - 1) = -e^i t^{\ell_1}(t^{\ell_2 - \ell_1} - 1) \tag{1}$$

$$t^{k_1}(t^{k_2 - k_1} - 1) = e^i t^{\ell_2}(t^{\ell_1 - \ell_2} - 1) . \tag{2}$$

If $k_2 - k_1 = \ell_2 - \ell_1$, (1) would imply that $t^{k_1} + e^i t^{\ell_1} = 0$. But the first equation of (*) would become $1 + t^m = 0$ which contradicts the hypothesis that $1 + t^m \neq 0$.

If $k_2 - k_1 = \ell_1 - \ell_2$, (2) would imply that $t^{k_1} = e^i t^{\ell_2}$ which is clearly impossible for $1 \leq i < d$. For $i = 0$, one has $t^{k_1} = t^{\ell_2}$, i.e. $k_1 = \ell_2$. But then (*) becomes one equation.

Lemma 2.2.2. Notations as in Lemma 2.2.1. The following system cannot hold.

$$1 + t^m - t^k = e^i t^{u+j} \tag{1}$$

$$1 + t^m - t^\ell = e^i t^u \tag{2}$$

(*)

$$1 + t^m - t^{k+s} = e^i t^{n+j} \tag{3}$$

$$1 + t^m - t^{\ell+s} = e^i t^n \tag{4}$$

where $1 \leq m \leq r$, $1 \leq i < d$, $t = e^d$, $1 \leq j < r$.

Proof. If the system (*) holds, then

(1) - (2) one gets $t - t^k = e^i t^u (t^j - 1)$

(3) - (4) one gets $t^s(t^\ell - t^k) = e^i t^n (t^j - 1)$.

From the above two equations one has

$$t^s = t^{n-u} \quad .$$

Hence $s = n - u \pmod r$. But by Lemma 2.2.1 (2) and (4) cannot hold simultaneously if $s = n - u \pmod r$. Q.E.D.

Lemma 2.2.3. Let $G = \{1, t, t^2, \ldots, t^{r-1}\}$ be a multiplicative subgroup of order r in the field $GF(p^n)$, where $r \geq 5$ and $3 \leq k < r$. Then $1 + t^2 = t + t^k$ iff $1 + t^2 + t^3 + \ldots + t^{k-1} = 0$ iff $1 + t^3 = t^k + t^{k+1}$.

Proof. $1 + t^2 = t + t^k$ iff $1 - t = -t^2 + t^k$ iff $1 = -t^2(1 + t + t^2 + \ldots + t^{k-3})$ iff $1 + t^2 + \ldots + t^{k-1} = 0$. Since $r \geq 5$, $1 - t^2 \neq 0$, we have that $1 + t^2 + t^3 + \ldots + t^{k-1} = 0$ iff $(1 - t^2)(1 + t^2 + t^3 + \ldots + t^{k-1}) = 0$ iff $1 + t^3 = t^k + t^{k+1}$. Q.E.D.

Lemma 2.2.4. When $r = 7$, $1 + t^2 \neq t + t^k$ for $k = 0,1,2,3,4,5,6$.

Proof. It is clear that $1 + t^2 \neq t + t^k$ for $k = 0,1,2,3$.

(1) For $k = 4$, if $1 + t^2 = t + t^4$, then by Lemma 2.2.3 and the fact that $1 + t + t^2 + \ldots + t^6 = 0$, we must have that $t + t^4 + t^5 + t^6 = 0$.

But when $k = 4$, by Lemma 2.2.3 again $1 + t^3 = t^4 + t^5$. Then $t + (1 + t^3) + t^6 = 0$. Since $1 + t^2 + t^3 = 0$, it follows that $t - t^2 + t^6 = 0$. This implies that $1 + t^2 - t^3 = 0$. This is impossible since $1 + t^2 + t^3 = 0$.

(2) For $k = 5$, if $1 + t^2 = t + t^5$, by Lemma 2.2.3, $1 + t^2 + t^3 + t^4 = 0$. Then $t + t^5 + t^6 = 0$, $1 + t^4 + t^5 = 0$. Since $1 + t^2 + t^3 + t^4 = 0$, we have $t^2 + t^3 - t^5 = 0$, i.e.

$$1 + t - t^3 = 0 \qquad (A)$$

But by Lemma 2.2.3 $1 + t^3 = t^5 + t^6$. This and $t + t^5 + t^6 = 0$ would imply that

$$1 + t + t^3 = 0 \ . \qquad (B)$$

By (A) and (B) it is clear that $1 + t^2 \neq t + t^5$.

(3) For $k = 6$, by Lemma 2.2.3 with $k = r - 1$, it is clear that $1 + t^2 \neq t + t^{r-1}$. In particular $1 + t^2 \neq t + t^6$ for $r = 7$.

Corollary 2.2.4. When $r = 7$, $1 + t^2 \neq t^5 + t^6$.

Proof. It is obvious that $1 + t^2 = t^5 + t^6$ iff $1 + t^2 + t^3 = 0$. By Lemma 2.2.3, $1 + t^2 = t^5 + t^6$ iff $1 + t^2 = t + t^4$. But by Lemma 2.2.4 $1 + t^2 \neq t + t^4$. Hence $1 + t^2 \neq t^5 + t^6$.

Lemma 2.2.5. Let $r > k \geq i \geq 3$. Then $1 + t^2 = t^i + t^k$ iff $1 + t + 2t^2 + 2t^3 + \ldots + 2t^{i-1} + t^i + \ldots + t^{k-1} = 0$.

Proof. Since $1 + t^2 = t^i + t^k$ iff $1 - t^i = -t^2 + t^k$ iff $1 + t + \ldots + t^{i-1} = -t^2(1 + t + \ldots + t^{k-1})$, it is obvious that $1 + t^2 \neq t^3 + t^5$. By Lemma 2.2.5, $1 + t^2 \neq t^3 + t^{r-1}$. In fact the

the following lemma is true.

Lemma 2.2.6. When $r = 7$, $1 + t^2 \neq t^3 + t^k$ for $k = 3,4,5,6$.

Proof. It remains to show that $1 + t^2 \neq 2t^3$ and $1 + t^2 \neq t^3 + t^4$.

(1) Suppose that $1 + t^2 = 2t^3$. By Lemma 2.2.5, $1 + t + 2t^2 = 0$. This implies that $-t^2 - t^5 + t^6 = 0$ since $(1 + t + t^2) + t^3(1 + t + t^2) + t^6 = 0$. Hence $1 + t^3 - t^4 = 0$, $(1 - t^4) + t^3 = 0$, $(1 - t^2)(1 + t^2) + t^3 = 0$. By assumption $1 + t^2 = 2t^3$, we have $2t^3(1 - t^2) + t^3 = 0$. Since $t^3 \neq 0$, $2(1 - t^2) + 1 = 0$, i.e. $2t^2 \equiv 3 \pmod p$. Since $1 + t + 2t^2 \equiv 0$, we have that $t = -4 \pmod p$. But when $t = -4 \pmod p$, and $2t^2 \equiv 3 \pmod p$, we must have that $29 \equiv 0 \pmod p$. But as $p = 29$, we may choose a subgroup of order $7 = \{1, t = 16, t^2 = 24, t^3 = 7, t^4 = 25, t^5 = 6, t^6 = 20\}$. Therefore when $r = 7$, $1 + t^2 \neq 2t^3$.

(2) Assume that $1 + t^2 = t^3 + t^4$. By Lemma 2.2.5 $1 + t + 2t^2 + t^3 = 0$. Hence $-t^2 + t^4 + t^5 + t^6 = 0$ or $1 + t + t^2 = t^5$. This and $1 + t + 2t^2 + t^3 = 0$ imply that

$$t^2 + t^3 + t^5 = 0$$

or

$$1 + t + t^3 = 0.$$

But $1 + t + 2t^2 + t^3 = 0$. Therefore if $1 + t^2 = t^3 + t^4$ we must have that $2t^2 \equiv 0 \pmod p$. Since p is odd prime, it is impossible.

Q.E.D.

Corollary 2.2.5. Let $r > k \geq 4$. Then $1 + t^2 = t^4 + t^k$ iff $1 + t + 2t^2 + 2t^3 + t^4 + \ldots + t^{k-1} = 0$.

Proof. It is trivial by Lemma 2.2.5 with $i = 4$.

It is clear that $1 + t^2 \neq t^4 + t^6$ when $r \neq 4$ and by Corollary 2.2.5, we have the following lemma.

Lemma 2.2.7. Let $r > k \geq 4$ and $r = 7$. Then $1 + t^2 \neq t^4 + t^k$.

Proof. It suffices to show that $1 + t^2 \neq 2t^4$ and $1 + t^2 \neq t^4 + t^5$.
(1) Suppose $1 + t^2 = 2t^4$. By Corollary 2.2.5 $1 + t + 2t^2 + 2t^3 = 0$. Since $1 + t \neq 0$, $2t^2 + 1 = 0$, $t^2 = -\frac{1}{2}$. Since $1 + t + t^2 + t^3 + \ldots + t^6 = 0$, we have that $6t = -5 \pmod p$. Then as $p = 3$, $1 + t^2 \neq 2t^4$. Without loss of generality, we may assume that $p \neq 3$. Then $6t = -5$ and $2t^2 + 1 = 0$ imply that

$$43 \equiv 0 \pmod p.$$

But if $p = 43$, we can choose a subgroup of order 7 which is generated by $t = 41$ such that $1 + t^2 \neq 2t^4$.
(2) Suppose $1 + t^2 = t^4 + t^5$. By Corollary 2.2.5, $1 + t + 2t^2 + 2t^3 + t^4 = 0$. But $1 + t + 2t^2 + 2t^3 + t^4 = 0$ iff $-t^2 - t^3 + t^5 + t^6 = 0$ iff $1 + t = t^3 + t^4$ iff $t^3 = 1$. This is impossible. Hence $1 + t^2 \neq t^4 + t^5$. Q.E.D.

Lemma 2.2.8. When $r = 7$, $1 + t^2 - t^i$, $i = 1,3,4,5,6$ are all not in the subgroup $G = \{1,t,t^2,\ldots,t^6\}$ of $GF(p^n)$, where $p^n - 1 = dr$, $d \geq 3$.

Proof. By Lemma 2.2.4, Corollary 2.2.4, Lemma 2.2.6 and Lemma 2.2.7, it suffices to show that $1 + t^2 \neq 2t^5$ and $1 + t^2 \neq 2t^6$.
(i) Suppose $1 + t^2 = 2t^5$. By Lemma 2.2.5, we get

$$1 + t + 2t^2 + 2t^3 + 2t^4 = 0 \qquad (A)$$

Since $1 + t + t^2 + t^3 + t^4 + t^5 + t^6 = 0$ and $t^2 \neq 0$, it follows

from (A) that

$$1 + t + t^2 = t^3 + t^4 \qquad (B)$$

(A) - (B) $\times\ t^2$, we get $1 + t + 2t^5 + 2t^6 = 0$

$$1 + t + (1 + t^2) + t(1 + t^2) = 0$$

since $1 + t^2 = 2t^5$.

$$2 + 2t + t^2 + t^3 = 0 \ . \qquad (C)$$

(A) - (C), we get

$$1 + t = t^2 + t^3 + 2t^4 \ .$$

By (B),

$$2t^2 + t^4 = 0$$

$$t^2 + 2 = 0.$$

Hence

$$2t^5 = 1 + t^2 = 1.$$

The last two equations give $8t = -1$. Solving the system

$\begin{cases} 8t = -1 \\ t^2 + 2 = 0 \end{cases}$ (mod p), we have that $129 \equiv 0 \bmod p$. Since $p \neq 3$, we should have $43 \equiv 0 \bmod p$. But for $p = 43$, we may choose a subgroup of order 7 which is generated by $t = 41$. Then $t^2 + 2 = 6 \not\equiv 0 \bmod 43$. Therefore $1 + t^2 \neq 2t^5$.

(ii) Suppose $1 + t^2 = 2t^6$. Then $1 - t^6 = -t^2(1 - t^4) =$ $-t^2(1-t^2)(1 + t^2)$

$$1 + 2t^2 + 2t^4 = 0 \qquad (D)$$

$$1 + 2t^2(1 + t^2) = 0$$

$$1 + 2t^2 \cdot 2t^6 = 0$$

$$t = -\tfrac{1}{4} .$$

Since $1 + t + t^2 + t^3(1 + t^2) + t^2(t^2 + t^4) = 0$ and $1 + t^2 = 2t^6$, $t^2 + t^4 = -\frac{1}{2}$, it is clear that

$$5t^2 + 2t + 2 = 0 \qquad (E)$$

Substituting $t = -\frac{1}{4}$ into (E), we must have that

$$29 \equiv 0 \pmod{p}.$$

But if $p = 29$, we may choose a subgroup of order 7 which is generated by $t = 16$ which gives $1 + t^2 = 25 \neq 40 = 2t^6 \bmod 29$. Thus $1 + t^2 \neq 2t^6$.

Lemma 2.2.9. When $r = 7$, $p \neq 29$, $1 + t^2 \neq t^k$, $k = 1,2,3,4,5,6$.

Proof. It is clear that $1 + t^2 \neq t^2$ and $1 + t^2 \neq t$.

(i) Suppose $1 + t^2 = t^3$. Since $1 + t + t^2 + t^3 + t^4 + t^5 + t^6 = 0$, it follows that

$$1 + t + t^2 + t^4 = 0.$$

Then

$$t^3 + t^5 + t^6 = 0$$

$$1 + t^2 + t^3 = 0.$$

This is impossible, since $1 + t^2 = t^3$.

(ii) Suppose $1 + t^2 = t^4$, then $1 + t + t^2 + t^3 + t^4 + t^5 + t^6 = 0$ gives

$$t^4 + t^5 + t^8 + t^5 = 0$$

$$1 + 2t + t^4 = 0.$$

Since $t^4 = 1 + t^2$,

$$2 + 2t + t^2 = 0 \ . \qquad \text{(A)}$$

On the other hand,

$$2(1 + t) = -t^2$$

$$4(1 + t)^2 = t^4.$$

But $t^4 = 1 + t^2$, hence

$$3 + 8t + 3t^2 = 0 \qquad \text{(B)}$$

From (A) and (B), it is readily seen that $2t = 3$, $t = 3/2$. Thus $1 + (\frac{3}{2})^2 = (\frac{3}{2})^4$

$$29 \equiv 0 \mod p.$$

But $p \neq 29$, therefore $1 + t^2 \neq t^4$.

(iii) Suppose $1 + t^2 = t^5$. Then $1 + t^2 + t(1 + t^2) + t^4 + t^5 + t^6 = 0$ implies that

$$t^4 + 2t^5 + 2t^6 = 0$$

$$2t^2 + 2t + 1 = 0 \ . \qquad \text{(C)}$$

Since $1 + t^2 = t^5$,

$$t^5 + t^2 + 2t = 0$$

$$2 + t + t^4 = 0 \qquad \text{(D)}$$

$$(1 + t^2)^2 = t^{10}$$

$$1 + 2t^2 + t^4 = t^3.$$

By (C),

$$-2t + t^4 = t^3 \quad \text{or} \quad 2 + t^2 = t^3 \ . \qquad \text{(E)}$$

By (D),

$$2t^3 + t^4 + t^7 = 0.$$

By (E),

$$2(2 + t^2) + t^4 + 1 = 0$$

$$4 + 2t^2 - (1 + t) = 0 \qquad \text{by (D).}$$

Hence

$$2t^2 - t + 3 = 0 \ . \qquad \text{(F)}$$

From (C) and (F), it follows that $3t = 2$, $t = \frac{2}{3}$. By (F) and $t = \frac{2}{3}$, we must have that $29 \equiv 0 \bmod p$. But $p \neq 29$. Therefore $1 + t^2 \neq t^5$.

(iv) Suppose $1 + t^2 = t^6$. Then $1 + t + t^2 + t^3(1 + t^2) + t^4(1 + t^2) = 0$ implies that

$$1 + t + 2t^2 + t^3 = 0$$

$$1 + 2t^2 + t(1 + t^2) = 0$$

$$1 + 2t^2 + 1 = 0$$

$$t^2 + 1 = 0.$$

This is impossible. Q.E.D.

Lemma 2.2.10. Let $r = 7$, $p^n - 1 = 7d$, $d \geq 3$. Then $1 + t^2 - t^i$, $i = 1,3,4,5,6$ cannot be all in a coset $\{e^u, e^u t, e^u t^2, \ldots, e^u t^6\}$, where $1 \leq u < d$.

Proof. By Lemma 2.2.1 and Lemma 2.2.2 it is not hard to see that the following system cannot hold.

$$1 + t^2 - t = e^u t^{m_1}$$

$$1 + t^2 - t^3 = e^u t^{m_3}$$

$$1 + t^2 - t^4 = e^u t^{m_4}$$

$$1 + t^2 - t^5 = e^u t^{m_5}$$

$$1 + t^2 - t^6 = e^u t^{m_6}$$

where $m_i \in \{0,1,2,3,4,5,6\}$.

Now Theorem 2.2.4 is easily seen to be a trivial consequence of Lemma 2.2.8, Lemma 2.2.9 and Lemma 2.2.10.

Note if $p = 29$, we may take $G = \{1, 2^4, 2^8, 2^{12}, 2^{16}, 2^{20}, 2^{24}\}$ $= \{1,16,24,7,25,23,20\}$. Then

$$2 - t = -14 = 15 = 2^{27} \in 2^3 \cdot G_7$$

$$2 - t^4 = -23 = 6 = 2^6 \in 2^2 \cdot G_7$$

$$2 - t^6 = -18 = 11 = 2^{25} \in 2 \cdot G_7 .$$

Therefore we have the following theorem.

Theorem 2.2.5. Let p be odd prime, $p^n - 1 = 7d$, $d \geq 3$. Then three orthogonal Latin squares of order $p^n + 7$ can be constructed by sum composition.

2.3. Theorem on the construction of $0(p^n + r,3)$ sets by sum composition.

Recently P.J. Cameron, J.I. Hall, J.H. van Lint, T.A. Springer and H.C.A. van Tilberg have proved that under quite general situations the set $\xi + G_r = \{\xi + t^i | t^i \in G_r\}$ has a nonempty intersection with at least three cosets of G_r in $GF(p^n)$ where $G_r = \{1,t,t^2,\ldots,t^{r-1}\}$, $p^n - 1 = dr$, $d \geq 3$, $r \geq 3$. This theorem which will be stated very precisely at the end of this sections, gives a real nice and complete conclusion about the construction of $0(p^n + r, 3)$ sets by sum composition. The following lemmas and theorems although just solved parts of our problem. Yet they have their own advantage in the construction of $0(p^n + r, 3)$ sets by sum composition. Therefore we state them here for the sake of completeness.

Lemma 2.3.1. For p an odd prime, and $\frac{p^n-1}{d} = r$, $n > 1$, r is odd number, then there exists an element $t^k \in G_r$ such that $2 - t^k \neq 0$ and $2 - t^k \notin G_r$.

Proof. (i) Since the pairwise appearances of $2-t^\ell = t^i$ and r is odd, if there exists t^ℓ such that $2 - t^\ell = 0$, then there is at least one t^k such that $2-t^k \neq 0$ and $2-t^k \notin G_r$.

(ii) If $2 \notin G_r$, and $2 - t^i \in G_r$ for all $i = 1,2,3,\ldots,r-1$, then

$$2(r-1) - 2\left(\sum_{i=1}^{r-1} t^i\right) = 0.$$

But $\sum_{i=0}^{r-1} t^i = 0$, we have $2(r-1) - 2(-1) = 0$ or equivalently $2r = 0 \pmod p$. Since p is odd, $r = 0 \pmod p$. It is clear that this is impossible. Q.E.D.

Lemma 2.3.2. For p an odd prime, $\frac{p^n-1}{d} = r$, $n > 1$, r is even and $r + 1 \neq 0 \bmod p$. Then there is an element $t^k \in G_r$ such that $2 - t^k \neq 0$ and $2 - t^k \notin G_r$.

Proof. Since the pairwise appearances of $2 - t^i = t^j$ and r is even there is at least one element $t^k \in G_r$ such that $2 - t^k \notin G_r$. If there are two elements $2 - t^{k_1}$, $2 - t^{k_2} \notin G_r$, we are done. So without loss of generality, we may assume that there is only one element such that $2 - t^k \notin G_r$ and it suffices to show that $2 - t^k \neq 0$.

Suppose $2 - t^k = 0$. Since $2 - t^i \in G_r$, for all $i \neq k$, it follows that

$$2(r - 2) - 2 \sum_{\substack{i=1 \\ i \neq k}}^{r-1} t^i = 0.$$

But $\sum_{i=0}^{r-1} t^i = 0$ and $t^k = 2$. Hence $r + 1 = 0 \pmod p$ which is impossible by assumption. Q.E.D.

Lemma 2.3.3. Let p be an odd prime and $r = \frac{p^n-1}{d}$, $n > 1$, $d \geq 3$. If there is i, $1 \leq i < d$, such that $i(p-1)$ is not divisible by d and $2 - t^k = e^i t^m$ for some t^k, t^m in G_r where e is a primitive element in $GF(p^n)$. Then by means of sum composition, the existence of $O(r,3)$ set implies that of $O(p^n + r, 3)$ set.

Proof.

$$2 - t^k = e^i t^m$$

$$(2 - t^k)^p = e^{ip} t^{pm}$$

$$2 - t^{pk} = e^{ip} t^{pm}.$$

Since $i(p-1)$ is not divisible by d, e^i and e^{ip} cannot be in the same cosets of G_r. Q.E.D.

Theorem 2.3.1. Let p be an odd prime, and $p^n-1 = dr$, $n > 1$, $d \geq 3$. If $(d,p-1) = 1$ and $r+1 \not\equiv 0 \bmod p$, then by means of sum composition, one can construct $O(p^n+r,3)$ set provided that $O(r,3)$ set exists.

Proof. Since $(d,p-1) = 1$ and p is odd, it is clear that d is odd. Hence r is even. By Lemma 2.3.2, there exists i,k,m such that $2 - t^k = e^i t^m$ where $1 \leq i < d$, $1 \leq k,m < r$. Since $(d,p-1) = 1$ and $i < d$, by Lemma 2.3.3, the theorem follows.

The following two corollaries are an immediate consequence of the theorem 2.3.1.

Corollary 2.3.1. Let $p = 3$. $r = \frac{p^n-1}{d}$, $n > 1$, d is odd, $r + 1 \not\equiv 0 \bmod 3$. If $O(r,3)$ set exists, then one can construct $O(3^n+r,3)$ set by sum composition.

Corollary 2.3.2. Let $p = 5$ and $r = \frac{p^n-1}{d}$, $n > 1$, d is odd, $r+1 \not\equiv 0 \bmod 5$. If $O(r,3)$ set exists, then one can construct $o(5^n+r,3)$ set by sum composition.

From section 2.2 we have exceptions for $r = 3$, 4 and 5. As one can see very easily that $p = 7$ is excluded if $r = 3$, and $p = 3$ or 5 are excluded if $r = 4$. Similarly $p = 11$ is excluded if $r = 5$. These indicate that two cases have to be excluded, i.e.

(a) If G_r is a multiplicative group of a subfield of $GF(p^n)$

(b) If G_r is the subgroup of index 2 in a multiplicative group of a subfield of $GF(p^n)$.

In fact the above exceptions appear in a very natural way as one can see from the following theorem which has been proved recently by the joint effort of five persons as stated at the beginning of this section.

Theorem 2.3.2. Let p be a prime, $K = GF(p^n)$, $p^n - 1 = rd$ where $r \geq 3$ and $d \geq 3$. $\xi \in K$, $(\xi \neq 0)$ and let G_r be the subgroup of order r in K^x. Then the set

$$\xi + G_r = \{\xi + t^i \mid t^i \in G_r\}$$

has a nonempty intersection with at least 3 cosets of G_r in K^x unless

(i) G_r is the multiplicative group of a subfield of K and $\xi \in G$.

(ii) G_r is the subgroup of index 2 in the multiplicative group of a subfield K_1 of K and $\xi \in K_1$.

(iii) $r = 3$ and $\xi \in G_r$ or $-\xi \in G_r$.

(iv) $r = 4$ and $\xi \in G_r$.

(v) $r = 5$, $p = 2$, $\xi \in G_r$.

Note $-1 - t^i$ cannot be in the subgroup $G_5 = \{1, t, t^2, t^3, t^4\}$ for $i = 1,2,3,4$, hence Theorem 2.2.3 holds for $p = 2$ by (v) of Theorem 2.3.2. It is obvious that 2 or -2 cannot be in G_3 if $p \neq 3$ and 7. It is also obvious that $-1 - t^i$ is in G_3 for $i = 1,2$, hence $p = 2$ is excluded by (iii) of Theorem 2.3.2. Therefore Theorem 2.2.1 and (iii) of Theorem 2.3.2 have the same conclusion. Similarly Theorem 2.2.2 and (iv) of Theorem 2.3.2 have the same conclusion. In fact for $r \geq 4$ by Theorem 2.3.2 we get the following theorem which is the best possible result we can get in construction of $O(p^n+r,3)$ sets by sum composition.

Theorem 2.3.3. Let p be a prime, $p^n-1 = dr$, $d \geq 3$, $r \geq 4$, n a positive integer. Then if three orthogonal Latin squares of order r

exist, we can construct three orthogonal Latin squares of order p^n+r by sum composition unless

(i) G_r is a multiplicative group of a subfield of $GF(p^n)$.

(ii) G_r is the subgroup of index 2 in a multiplicative group of a subfield of $GF(p^n)$.

2.4. Alternative Construction of $O(p^n+r,3)$ sets by Sum Composition.

If in (2.1.B), we let $K_v(\lambda,x_1,x_3,at_1,ct_3)$ capture $\{at_1\}$ and $K_h(\lambda,x_1,x_3,at_1,ct_3)$ capture $\{ct_3\}$ and keeps (2.1.A) and (2.1.C), then similar to the previous case we can get a different set of conditions for construction of $O(p^n+r,3)$ sets. Although by no means we can improve the result of Theorem 2.3.3, yet in the construction of $O(p^n+r,4)$ sets this construction may give some help. Thus we state it here for the sake of reference. As in Section 2.1, through this section we assume that $t^{m+k} = t^{\ell+n} = t^{i+j} = 1$.

Let

$$K_v(\lambda,x_1,x_3,at^u,ct^{u+s_2}) = at^u t^i$$

$$K_h(\lambda,x_1,x_3,at^u,ct^{u+s_2}) = ct^{u+s_2}t^j \qquad u = 0,1,\ldots,r-1. \tag{2.4.B}$$

where

$$t^i = \frac{x_1(\lambda - x_3) - a^{-1}ct^{s_2}x_3(\lambda - x_1)}{\lambda(x_1 - x_3)} \quad , 1 \le i < r$$

$$t^j = \frac{(x_1 - \lambda) - ac^{-1}t^{-s_2}(x_3 - \lambda)}{x_1 - x_3} \quad . 1 \le j < r .$$

Interchanging x_1 and x_3, a^{-1} and a, c^{-1} and c, $-s_2$ and s_2, by the results in section 2.1, we must have that

$$x_1 = \frac{\lambda(1 - ac^{-1}t^{-s_2}t^i)}{1 - t^j}$$

$$x_3 = \frac{\lambda(1 - t^i)}{1 - a^{-1}ct^{s_2}t^j} .$$

Since we keep (2.1.A) and (2.1.C) unchanged, (2.1.I), (2.1.II) and (2.1.III) turn out to be

$$x_1 = \frac{\lambda(1 - ac^{-1}t^{-s_2}t^i)}{1 - t^j} = \frac{\lambda(1 - t^k)}{1 - ab^{-1}t^{-s_1}t^m} \qquad (2.4.I)$$

$$x_2 = \frac{\lambda(1 - a^{-1}bt^{s_1}t^k)}{1 - t^m} = \frac{\lambda(1 - t^\ell)}{1 - bc^{-1}t^{-s_3}t^n} \qquad (2.4.II)$$

$$x_3 = \frac{\lambda(1 - t^i)}{1 - a^{-1}ct^{s_2}t^j} = \frac{\lambda(1 - b^{-1}ct^{s_3}t^\ell)}{1 - t^n} \qquad (2.4.III)$$

By (2.4.III),

$$\frac{t^i(1 - t^j)}{a^{-1}ct^{s_2+j}(1 - ac^{-1}t^{-s_2+i})} = \frac{(1 - b^{-1}ct^{s_3}t^\ell)}{1 - t^n} .$$

By (2.4.I),

$$\frac{ab^{-1}t^{-s_1+m+i}(1 - a^{-1}bt^{s_1}t^k)}{a^{-1}ct^{s_2+j+k}(1 - t^m)} = \frac{1 - b^{-1}ct^{s_3}t^\ell}{1 - t^n} .$$

By (2.4.II),

$$(1 - bc^{-1}t^{-s_3}t^n)^2 = \frac{a^2(1 - t^\ell)^2t^{m+n+i}}{c^2t^{s_1+s_2+s_3+k+\ell+j}} .$$

If $t^{s_1+s_2+s_3}$ is a quadratic residue, this is true in particular when t has even index, or $s_1 + s_2 + s_3$ is even, then we have the following solutions.

$$1 - bc^{-1}t^{-s_3+n} = \pm \frac{a}{c}(1 - t^{\ell})t^{-q+(m+n+i)} \tag{2.4.1}$$

where $2q = s_1 + s_2 + s_3 \pmod r$.

Substituting (2.4.1) in (2.4.11), we have that

$$1 - a^{-1}bt^{s_1+k} = \pm \frac{c}{a}(1 - t^{m})t^{q-(m+n+i)}$$

equivalently

$$1 - ab^{-1}t^{-s_1+m} = \pm \frac{c}{b}(1 - t^{k})t^{-s_1+q-(k+n+i)} . \tag{2.4.2}$$

Substituting (2.4.2) in (2.4.1), we have that

$$1 - ac^{-1}t^{-s_2+i} = \pm \frac{b}{c}(1 - t^{j})t^{s_1-q+(k+n+i)} . \tag{2.4.3}$$

By (2.4.1), (2.4.2) and (2.4.3), it follows that the following system holds

$$\begin{aligned} &\pm a(1 - t^{\ell})t^{-q+(m+n+i)} + bt^{-s_3+n} - c = 0 \\ &a - bt^{s_1+k} \mp c(1 - t^{m})t^{q-(m+n+i)} = 0 \\ &at^{-s_1+i} \pm b(1 - t^{j})t^{s_1-q+(k+n+i)} - c = 0 \end{aligned} \tag{2.4.(*)}$$

In order that a,b and c have non-zero solutions, we must have

$$\begin{vmatrix} \pm (1 - t^{\ell}) t^{-q+(m+n+i)} & t^{-s_3+n} & -1 \\ 1 & -t^{s_1+k} & \mp (1 - t^{m}) t^{q-(m+n+i)} \\ t^{-s_2+i} & \pm (1-t^{j}) t^{s_1-q+(k+n+i)} & -1 \end{vmatrix} = 0$$

It is not hard to get from above determinant that the condition turns out to be

$$\pm t^{-s_2-s_3+q} \mp t^{-s_2-s_3+q-m} - t^{s_1-s_2+k+i} \mp t^{s_1-q+k+i}$$

$$\pm t^{s_1-q+n} \pm t^{s_1-q+k} \mp t^{s_1-q} + t^{-s_3+n} = 0 \qquad (2.4.4)$$

Let $q = \frac{1}{2}(s_1 + s_2 + s_3) = 0$ and $s_2 = 0$. We have that (2.4.4) is satisfied when lower sign is taken.

Under conditions $q = 0$ and $s_2 = 0 \bmod r$, (2.4.(*)) becomes

$$\begin{aligned} -a(1 - t^{\ell}) t^{m+n+i} + bt^{-s_3+n} - c &= 0 \\ a - bt^{s_1+k} + c(1 - t^{m}) t^{-(m+n+i)} &= 0 \\ at^{i} - b(1 - t^{j}) t^{s_1+(k+n+i)} - c &= 0 \end{aligned}$$

Solving above system for a and b in terms of c, we get very easily that

$$a = \frac{t^{k+j} - t^{k} - t^{j}}{t^{n+i} - t^{n} - t^{i}} \times c$$

$$b = \frac{t^{m+\ell} - t^{m} - t^{\ell}}{t^{s_1}(t^{n+i} - t^{i} - t^{n})} \times c .$$

Thus we have the following solutions for ab^{-1}, bc^{-1} and ac^{-1}:

$$ab^{-1} = \frac{t^{s_1+k}(t^{m+j} - t^j + 1)}{t^{\ell}(t^{m+n} - t^m + 1)} \tag{2.4.5}$$

$$bc^{-1} = \frac{t^{\ell}(t^{m+n} - t^m + 1)}{t^{s_1+i}(t^{n+j} - t^n + 1)} \tag{2.4.6}$$

$$ac^{-1} = \frac{t^{k}(t^{m+j} - t^j + 1)}{t^{i}(t^{n+j} - t^n + 1)} \tag{2.4.7}$$

Similar to the Remark 2.1.3, it is not hard to find the following solutions for x_1, x_2 and x_3. They are

$$x_1 = -\lambda bc^{-1}t^{s_1+k+n+i} \tag{2.4.8}$$

$$x_2 = -\lambda a^{-1}ct^{k-n-i} \tag{2.4.9}$$

$$x_3 = -\lambda ab^{-1}t^{s_3-k-n+i} \tag{2.4.10}$$

Similar to Theorem 2.1.1 and Theorem 2.1.2 we can get the following two theorems.

Theorem 2.4.1. Let $t^{m+k} = t^{\ell+n} = t^{i+j} = 1$. Then a sufficient condition for ab^{-1}, bc^{-1} and ac^{-1} having solution is that $s_1 + s_3 = s_2 = 0$ mod r. In this case the solutions for ab^{-1}, bc^{-1} and ac^{-1} are given by (2.4.5), (2.4.6) and (2.4.7), respectively.

Theorem 2.4.2. Let $t^{m+k} = t^{\ell+n} = t^{i+j} = 1$. If there are elements t^{s_1}, t^{s_3}, t^m, t^n, t^j such that

(i) $s_2 = 0$ mod r, $s_1 + s_3 = 0$ (mod r)

(ii) $1 - t^m + t^{m+n}$, $1 - t^n + t^{n+j}$ and $1 - t^j + t^{j+m}$ are in three different cosets of G_r.

Then $O(p^n+r,3)$ set can be constructed by sum composition provided that $O(r,3)$ set exists.

Example 2.4.1. As in Example 2.1.1 we take $p = 13$, $r = 4$. $G_4 = \{1,2^3,2^6,2^9\} = \{1,8,12,5\}$. We take

$$s_1 = 2 \quad k = 3 \quad i = 3 \quad \ell = 1$$

$$s_2 = 0$$

$$s_3 = 2 \quad m = 1 \quad j = 1 \quad n = 3$$

By (2.4.5), (2.4.6) and (2.4.7), it follows that

$$ab^{-1} = 10,\ bc^{-1} = 2,\ ac^{-1} = 7.$$

We may choose $a = 1$, $b = 4$, $c = 2$ and $\lambda = 1$. Then

$$x_1 = 3,\ x_2 = 10,\ x_3 = 2$$

$$\{(at_1,bt_2)\} = \{(1,9),(8,7),(12,4),(5,6)\}$$

$$\{(at_1,ct_3)\} = \{(1,2),(8,3),(12,11),(5,10)\}$$

$$\{(bt_2,ct_3)\} = \{(4,11),(6,10),(9,2),(7,3)\}$$

$$\{K_v(\lambda,x_1,x_2,at_1,bt_2)\} = \{bt^{u+s_1+k} : b = 4,\ u = 0,1,2,3,\ s_1 = 2,\ k = 3\} =$$

$$\{6,9,7,4\}$$

$$\{K_h(\lambda,x_1,x_2,at_1,bt_2)\} = \{at^{u+m} : a = 1,\ u = 0,1,2,3,\ m = 1\} = \{8,12,5,1\}$$

$$\{K_v(\lambda,x_1,x_3,at_1,ct_3)\} = \{at^{u+i} : a = 1,\ u = 0,1,2,3,\ i = 3\} = \{5,1,8,12\}$$

$$\{K_h(\lambda,x_1,x_3,at_1,ct_3)\} = \{ct^{u+s_2+j} : c = 2,\ u = 0,1,2,3,\ s_2 = 0,\ j = 1\} =$$

$$\{3,11,10,2\}$$

$$\{K_v(\lambda,x_2,x_3,bt_2,ct_3)\} = \{ct^{u+s_3+\ell} : c = 2,\ u = 0,1,2,3,\ s_3 = 2,\ \ell = 1\} =$$

$$\{10,2,3,11\}$$

$\{K_h(\lambda,x_2,x_3,bt_2,ct_3)\} = \{bt^{u+n}: b = 4,\ u = 0,1,2,3,\ n = 3\} = \{7,4,6,9\}$.

It is clear that by Principle 1.3, three orthogonal Latin squares of order 17 can be constructed by sum composition. We state them as follows for the sake of comparison.

$L(B(3),L_1)$, $\{at_1\} = \{1,8,12,5\}$.

0	A	2	3	4	D	6	7	B	9	10	11	C	1	8	12	5
A	4	5	6	D	8	9	B	11	12	0	C	2	3	10	1	7
6	7	8	D	10	11	B	0	1	2	C	4	A	5	12	3	9
9	10	D	12	0	B	2	3	4	C	6	A	8	7	1	5	11
12	D	1	2	B	4	5	6	C	8	A	10	11	9	3	7	0
D	3	4	B	6	7	8	C	10	A	12	0	1	11	5	9	2
5	6	B	8	9	10	C	12	A	1	2	3	D	0	7	11	4
8	B	10	11	12	C	1	A	3	4	5	D	7	2	9	0	6
B	12	0	1	C	3	A	5	6	7	D	9	10	4	11	2	8
1	2	3	C	5	A	7	8	9	D	11	12	B	6	0	4	10
4	5	C	7	A	9	10	11	D	0	1	B	3	8	2	6	12
7	C	9	A	11	12	0	D	2	3	B	5	6	10	4	8	1
C	11	A	0	1	2	D	4	5	B	7	8	9	12	6	10	3
3	1	12	10	8	6	4	2	0	11	9	7	5	A	B	C	D
11	9	7	5	3	1	12	10	8	6	4	2	0	B	A	D	C
10	8	6	4	2	0	11	9	7	5	3	1	12	C	D	A	B
2	0	11	9	7	5	3	1	12	10	8	6	4	D	C	B	A

where $L_1 =$

A	B	C	D
B	A	D	C
C	D	A	B
D	C	B	A

$L(B(10),L_2)$, $\{bt_2\} = \{9,7,4,6\}$

0	1	2	3	C	5	D	B	8	A	10	11	12	9	7	4	6
10	11	12	C	1	D	B	4	A	6	7	8	9	5	3	0	2
7	8	C	10	D	B	0	A	2	3	4	5	6	1	12	9	11
4	C	6	D	B	9	A	11	12	0	1	2	3	10	8	5	7
C	2	D	B	5	A	7	8	9	10	11	12	0	6	4	1	3
11	D	B	1	A	3	4	5	6	7	8	9	C	2	0	10	12
D	B	10	A	12	0	1	2	3	4	5	C	7	11	9	6	8
B	6	A	8	9	10	11	12	0	1	C	3	D	7	5	2	4
2	A	4	5	6	7	8	9	10	C	12	D	B	3	1	11	0
A	0	1	2	3	4	5	6	C	8	D	B	11	12	10	7	9
9	10	11	12	0	1	2	C	4	D	B	7	A	8	6	3	5
6	7	8	9	10	11	C	0	D	B	3	A	5	4	2	12	1
3	4	5	6	7	C	9	D	B	12	A	1	2	0	11	8	10
12	3	7	11	2	6	10	1	5	9	0	4	8	A	B	C	D
5	9	0	4	8	12	3	7	11	2	6	10	1	C	D	A	B
1	5	9	0	4	8	12	3	7	11	2	6	10	D	C	B	A
8	12	3	7	11	2	6	10	1	5	9	0	4	B	A	D	C

where

$L_2 =$

A	B	C	D
C	D	A	B
D	C	B	A
B	A	D	C

$L(B(2), L_3)$, $\{ct_3\} = \{2,3,11,10\}$

0	1	A	B	4	5	6	7	8	9	D	C	12	2	3	11	10
2	A	B	5	6	7	8	9	10	D	C	0	1	3	4	12	11
A	B	6	7	8	9	10	11	D	C	1	2	3	4	5	0	12
B	7	8	9	10	11	12	D	C	2	3	4	A	5	6	1	0
8	9	10	11	12	0	D	C	3	4	5	A	B	6	7	2	1
10	11	12	0	1	D	C	4	5	6	A	B	9	7	8	3	2
12	0	1	2	D	C	5	6	7	A	B	10	11	8	9	4	3
1	2	3	D	C	6	7	8	A	B	11	12	0	9	10	5	4
3	4	D	C	7	8	9	A	B	12	0	1	2	10	11	6	5
5	D	C	8	9	10	A	B	0	1	2	3	4	11	12	7	6
D	C	9	10	11	A	B	1	2	3	4	5	6	12	0	8	7
C	10	11	12	A	B	2	3	4	5	6	7	D	0	1	9	8
11	12	0	A	B	3	4	5	6	7	8	D	C	1	2	10	9
4	3	2	1	0	12	11	10	9	8	7	6	5	A	B	C	D
6	5	4	3	2	1	0	12	11	10	9	8	7	D	C	B	A
9	8	7	6	5	4	3	2	1	0	12	11	10	B	A	D	C
7	6	5	4	3	2	1	0	12	11	10	9	8	C	D	A	B

where $L_3 =$

A	B	C	D
D	C	B	A
B	A	D	C
C	D	A	B

CHAPTER III

GEOMETRIC CONSTRUCTION OF GENERALIZED YOUDEN DESIGNS

3.1. Introduction

The original Youden square (YS) for v varieties was a $k \times v$ array obtained from a balanced incomplete block design BIBD (v,b,k,r,λ), with $b = v > k$ by considering blocks as columns, arranged to make each variety appear once per row. Generalizations, by Shrikhande and Agrawal allowed $b = mv$ for integer m. It was Kiefer (1958) who relaxed the restrictions $v > k$ and $b = mv$ and generalized the BIBD and YS to the balanced block design (BBD) and generalized Youden design (GYD). The basic constructive methods for BBD's and GYD's, which have been used in optimality considerations for a number of years, were listed and illustrated in Kiefer's paper (1975). Those were methods for combining LS's and known BIBD's to yield the desires structure. Ruiz and Seiden (1974) described a construction of an infinite class of GYD with $v = 4$, $b = k = 6t$, t odd, and showed that they are not D-optimal. They also constructed geometrically several families of D-optimal GYD for $v = s^2$, s a power of a prime. This part of the thesis is a generalization of Ruiz and Seiden (1974) to the case $v = s^m$, $m \geq 2$. In particular a geometrical construction of GYD for $v = 4$, $b = 6t_1$, $k = 6t_2$, t_1, t_2 odd, is performed which seems different from what has appeared in the literature and more extensively covers all nonregular cases for $v = 4$. It is

our hope that this construction of nonregular cases for $v = 4$ will stimulate further research on remaining yet unsolved problem in the design setting of two-way heteogeneity.

3.2. Definitions and Optimality of GYD.

(A). Definitions and some properties of GYD.

In the usual block design setting of one-way heterogeneity, we specify the positive integers b,v and k, and have v varieties and b blocks of size k. A design then can be thought of as a $k \times b$ array of variety labels, with blocks as columns. Let $n_{d_{ij}}$ be the number of times that variety i appears in block j in design d and let ρ = fractional part of k/v, $r_{d_i} = \Sigma_j n_{d_{ij}}$ and $\lambda_{d_{ih}} = \Sigma_j n_{d_{ij}} n_{d_{hj}}$.

Definition 3.2.1. A (v,b,k) balanced block design (BBD) is a design d with all r_{d_i} equal, all $\lambda_{d_{ih}}$ equal for $i < h$, and $|n_{d_{ij}} - k/v| < 1$ for all i,j.

Definition 3.2.2. A (v,b,k) balanced incomplete block design (BIB) is a (v,b,k) BBD with $k < v$.

A (v,b,k) BIB design is said to be symmetric if $v = b$.

In the setting of two-way heterogeneity, we write $\lambda_{d_{ih}}^{(\theta)}$ and $\rho^{(\theta)}$ with $\theta = R$ or C for the quantities λ and ρ when rows (R) or columns (C) are considered as blocks. If $\rho^{(R)}$ or $\rho^{(C)} = 0$, the design is said to be regular.

Definition 3.2.3. A (v,b,k) generalized Youden design (GYD) is a design which is a BBD when each of the rows (columns) is considered as the blocks.

In particular we have

Definition 3.2.4. A (v,k) Youden design (squares) is a GYD with $b = v$ and $k < v$.

It follows from this definition that a (v,k) Youden design is merely a symmetric BIB design with each row a permutation of the varieties. Therefore we are interested in the GYD with $k \geq v$ and $b \geq v$ which will be assumed through this part of the thesis.

There are some known properties of GYD, among others, the following two are most frequently used. For the other properties readers are referred to Ruiz and Seiden (1974).

Notation. The quotient and remainder of the division of an integer a by another b will be written $[a/b]$ and $a_{(b)}$ respectively.

For a GYD d, let $r_{d_i} = r$ for all i, $\lambda^{(R)}_{d_{ih}} = \lambda_1$, $\lambda^{(C)}_{d_{ih}} = \lambda_2$ for all i and h, $[b/v] = m_r$ and $[k/v] = n_c$.

Proposition 3.2.1. (i) $rv = kb$.

(ii) $r = m_r k + r_{(k)} = n_c b + r_{(b)}$

(iii) $vr_{(k)} = kb_{(v)}$, $br_{(k)} = rb_{(v)}$.

Proposition 3.2.2. (i) $$\lambda_1 = m_r(r + r_{(k)}) + \frac{r_{(k)}(b_{(v)} - 1)}{v - 1}$$

(ii) $$\lambda_2 = n_c(r + r_{(b)}) + \frac{r_{(b)}(k_{(v)} - 1)}{v - 1}$$

Remark 3.2.1. Notice that proposition 3.2.2 yields a necessary condition for the existence of GYD, namely

$$\frac{r_{(k)}(b_{(v)} - 1)}{v-1} \quad \text{and} \quad \frac{r_{(b)}(k_{(v)} - 1)}{v-1}$$

have to be all integers.

(B). Optimality of GYD. Let y_{ijk} denote the observation corresponding to the kth variety in the ith row and the jth column. The row, column, and variety effects are denoted by α_t, β_r, γ_c respectively. If e_{ijk} is the random error with the usual assumptions about homoscedasticity and normality, then a completely additive model is

$$y_{ijk} = \alpha_t + \beta_r + \gamma_c + e_{ijk} .$$

If we are interested only in estimation of linear combinations $c\alpha$, where c is a contrast $(\Sigma c_i = 0)$, α is the v-vector of α_t's, then the commonly used optimality criteria are usually formulated in terms of the covariance matrix V_d of the best linear estimators. They are

(a) D-optimality: minimizing the $\det V_d$.

(b) A-optimality: minimizing the $\operatorname{tr} V_d$.

(c) E-optimality: minimizing the maximum eigenvalue of V_d.

The relationship among these is well known; in the two way heterogeneity setting, D-optimality of a GYD implies A-optimality, and A-optimality implies E-optimality.

In the special setting $b = k = v$, i.e. GYD is a Latin square, Wald (1943) showed that it was D-optimal. Kiefer (1958) shows that the regular GYD is D-optimal. For the nonregular settings, the conclusions known at this time are:

(i) A GYD is always A-optimal and is therefore E-optimal.

(ii) A GYD is D-optimal unless $v = 4$.

(iii) If $v = 4$ and $b = k$ a GYD is never D-optimal.

(iv) If $v = 4$ and $\frac{b}{k}$ is sufficiently near 1, a GYD is not D-optimal.

From above known results, it follows that a nonregular GYD with $v = 4$ is a most interesting one in the consideration of optimality. Now suppose a GYD is nonregular, then $b_{(v)}$ and $k_{(v)}$ are either 1, 3 or 2. If $b_{(v)}$ (or $k_{(v)}$) were 1 or 3, by Proposition 3.2.1(iii), $r_{(k)}$ cannot be an integer. Thus $b_{(v)}$ and $k_{(v)}$ have to be 2. But then by Remark 3.2.1, $r_{(k)}$ and $r_{(b)}$ are divisible by 3. This and Proposition 3.2.1(iii) imply that k and b are both divisible by 6. Therefore the only nonregular GYD with $v = 4$ is of the form with $b = 6t_1$ and $k = 6t_2$, t_1 and t_2 odd. Since the optimality in this case has not been solved, it is felt that a new design construction is worth mentioning. Thus a geometric construction of such design is given in the next section.

3.3. Construction of GYD

By a flat we mean a (m-1)-dimensional hyperplane in $EG(m,x)$. The set of all flats in $EG(m,s)$ can be further classified into m disjoint sets as follows:

The coefficients of the following equations should range through all the elements of $GF(s)$.

$$G_m: a_1x_1 + a_2x_2 + \ldots + a_{m-1}x_{m-1} + x_m = a,$$
$$G_{m-1}: a_1x_1 + a_2x_2 + \ldots + a_{m-2}x_{m-2} + x_{m-1} = a,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$G_2: a_1x_1 + x_2 = a,$$
$$G_1: x_1 = a.$$

Note that there are s^p flats contained in G_p, $p = 1,2,3,\ldots,m$.

Let $\alpha_0,\alpha_1,\alpha_2,\ldots,\alpha_{s-1}$ be s elements of GF(s) arranged in the following order: $\alpha_0 < \alpha_1 < \alpha_2 < \ldots < \alpha_{s-1}$.

Each point in a flat can be represented by a m-tuples in such a way that the i-th component of the m-tuples is $x_i = a$, $a \in GF(s)$, $i = 1,2,3,\ldots,m$. Two points A and B on a flat are ordered as follows:

(0). $A < B$ (B follows A), if the first distinct components of A and B are $x_i = a_i$ and $x_i = b_i$ respectively, and $a_i < b_i$, $a_i,b_i \in GF(s)$.

We assume from now on that all points in a flat under consideration have been arranged according to the above ordering (0) unless otherwise specified.

Step 1. $p = 1,2,3,\ldots,m-1$.

Let ℓ_i, $i = 1,2,3,\ldots,s^{p-1}$, be pencils in G_p, and L_i be $s \times s^{m-1}$ matrix with the flats in ℓ_i as its rows. Note that the order of the flats in L_i could be arbitrary.

We define

$$T_p = \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_{s^{p-1}} \end{pmatrix} \quad \text{and} \quad \xi = \begin{pmatrix} 0_{1\times(s^{m-1}-1)} & 1 \\ I_{(s^{m-1}-1)\times(s^{m-1}-1)} & 0_{(s^{m-1}-1)\times 1} \end{pmatrix}$$

It is clear that T_p is a $s^p \times s^{m-1}$ matrix. Let

$$T_p^* = \begin{pmatrix} L_1 \\ L_2\xi^s \\ L_3\xi^{2s} \\ \vdots \\ L_{s^{p-1}}\xi^{(s^{p-1}-1)s} \end{pmatrix} \quad \text{and} \quad T_p^{**} = \begin{pmatrix} T_p^* \\ T_p^*\xi^{s^p} \\ T_p^*\xi^{2s^p} \\ \vdots \\ T_p^*\xi^{s^{m-1}-s^p} \end{pmatrix}$$

Since T_p^{**} is a $s^{m-1} \times s^{m-1}$ matrix and the point on the $(n + us)$th position of any flat in any pencil ℓ_i, where $1 \leq n \leq s$, $0 \leq u \leq s^{m-2} - 1$, is on the flat $x_m = \alpha_{n-1}$, the elements of the $(n + us)$th column of T_p^{**} form the flat $x_m = \alpha_{n-1}$.

Let

$$E = \begin{pmatrix} 0_{1\times(s-1)} & 1 \\ I_{(s-1)\times(s-1)} & 0_{(s-1)\times 1} \end{pmatrix} .$$

Then a $s^{m-1} \times s^{m-1}$ matrix η which has E as its diagonal elements and zero otherwise can be defined as follows:

$$\eta = \begin{pmatrix} E & & & 0 \\ & E & & \\ & & E & \\ & & & \ddots \\ 0 & & & & E \end{pmatrix}$$

Consider the following matrix D_p:

$$D_p = \begin{pmatrix} T_p^{**} \\ T_p^{**}\eta \\ T_p^{**}\eta^2 \\ \vdots \\ T_p^{**}\eta^{s-1} \end{pmatrix}$$

Multiplying T_p^{**} on the right by η gives a permutation of each row in which each s-tuple within the (us)th and (u+1)sth columns is permuted cyclically, $0 \leq u \leq s^{m-2} - 1$. Moreover since the (n+us)th column of T_p^{**} is the flat $X_m = \alpha_{n-1}$, each column of D_p is there-

fore a permutation of all s^m points of $EG(m,s)$.

Note that each flat in G_p as a row of T_p^{**} has been repeated s^{m-p-1} times in T_p^{**}, and thus each flat in G_p as a row of D_p has been repeated s^{m-p} times in D_p.

Step 2. $p = m$.

There are S^{m-1} pencils ℓ_i in G_m, $i = 1,2,3,\ldots,s^{m-1}$. Let L_i be $S \times S^{m-1}$ matrix with the flats in ℓ_i as its rows and ξ be defined as in Step 1.

Consider the following matrix:

$$D_m = \begin{pmatrix} L_1 \\ L_2\xi \\ L_3\xi^2 \\ \vdots \\ L_{s^{m-1}}\xi^{(s^{m-1}-1)} \end{pmatrix}$$

It follows that each column of D_m is a permutation of s^m points in $EG(m,s)$.

Step 3. Similarly as before we can classify the set of all flats in $EG(m,s)$ into m disjoint subsets in the following way.

G'_m: $a_m x_m + a_{m-1}x_{m-1} + \ldots + a_2 x_2 + x_1 = a$,

G'_{m-1}: $a_m x_m + a_{m-1}x_{m-1} + \ldots + a_3 x_3 + x_2 = a$,

. . . . . .

G'_2: $a_{m-1}x_{m-1} + x_m = a$,

G'_1: $x_m = a$.

Each point in a flat then is represented by a m-tuple in such a way that the i-th component of the m-tuples is $x_{m-i+1} = a$, $a \in GF(s)$,

$i = 1,2,\ldots,m$. Moreover two points A and B on a flat are ordered according to ordering (0).

In this step we assume that all points in a flat under consideration in EG(m,s) have been arranged in the above fashion.

For $p = 1,2,3,\ldots,m-1$, $(p = m)$, as in Step 1 (Step 2), associated with G_p' (G_m') a matrix D_p' (D_m') similar to D_p (D_m) can be constructed.

Theorem 3.3.1. There exist GYD with parameters $v = s^m$, $m \geq 2$, $b = (t_1 s + 1)s^{m-1}(s^m-1)/(s-1)$, $k = t_2 s+1)s^{m-1}(s^m-1)/(s-1)$, where $t_1, t_2 = 0,1,2,3,\ldots$. The other parameters are

$$r = (t_1 s+1)(t_2 s+1)s^{m-2}(s^m-1)^2/(s-1)^2$$

$$m_r = (t_1 s+1)(s^{m-1}-1)/(s-1) + t_1$$

$$n_c = (t_2 s+1)(s^{m-1}-1)/(s-1) + t_2$$

$$\lambda_1 = [(t_1 s+1)(s^{m-1}-1)/(s-1) + t_1](t_2 s+1)s^{m-2}(s^m-1)/(s-1)$$
$$\times [(t_1 s+1)(s^m-1)/(s-1) + 1] + (t_2 s+1)s^{m-2}(s^{m-1}-1)/(s-1).$$

$$\lambda_2 = [(t_2 s+1)(s^{m-1}-1)/(s-1) + t_2] (t_1 s+1)s^{m-2}(s^m-1)/(s-1)$$
$$\times [(t_2 s+1)(s^m-1)/(s-1) + 1] + (t_1 s+1)s^{m-2}(s^{m-1}-1)/(s-1).$$

Proof. For the sake of convenience, for a matrix M and a positive integer n, the matrix $[\overbrace{M\ M\ \ldots\ M}^{n}]$ is denoted $M^{[n]}$.

Let

$$A_{(i,t_2)} = [D_i^T]^{[(t_2s+1)s^{i-2}]}, \quad i = 2,3,\ldots,m-1,$$

$$A'_{(i,t_1)} = [(D_i')^T]^{[(t_1s+1)s^{i-2}]}, \quad i = 2,3,\ldots,m-1,$$

$$A = [[D_1^T]^{[t_2]}\,[D_m^T]^{[(t_2s+1)s^{m-2}]}\,A_{(m-1,t_2)}A_{(m-2,t_2)},\ldots,A_{(2,t_2)}]$$

and

$$A' = [[(D_1')^T]^{[t_1]}\,[D_m'^T]^{[(t_1s+1)s^{m-2}]}\,A'_{(m-1,t_1)}A'_{(m-2,t_1)},\ldots,A'_{(2,t_1)}]$$

Then the desired GYD is

$$G = \begin{bmatrix} T_1^{**} & A' \\ A^T & (L)_\beta^\alpha \end{bmatrix}$$

where $\alpha = (t_1+1)(s^{m-1}-1)/(s-1) + t_1s^{m-1}$, $\beta = (t_2+1)(s^{m-1}-1)/(s-1) + t_2s^{m-1}$ and $(L)_\beta^\alpha$ is a $\beta \times \alpha$ matrix with each entry a Latin square of order s^m.

It follows from the above construction that each flat in EG(m,s) appears $(t_1s+1)s^{m-2}$ times as columns in the upper part from row 1 to row s^{m-1} of G. Similarly each flat appears $(t_2s+1)s^{m-2}$ times as rows in the left hand part from column 1 to column s^{m-1} of G. Moreover D_i, D_i', $i = 1,2,3,\ldots,m-1,m$, are all arranged in such a way that each column is a permutation of S^m variates. Since the number of flats in EG(m,s) which contains a prescribed point (pair of points) are all the same for any two points (two paris of points) in EG(m,s), therefore G must be a GYD.

Proposition 3.3.1. There exist Latin squares of order S^m which can be split into S groups of S columns in such a way that every row in each group is a flat of $EG(m,s)$.

Proof. The desired Latin square is

$$L = \begin{array}{cccc} T_q^{**} & \eta T_q^{**} & \cdots & \eta^{s-1} T_q^{**} \\ T_q^{**}\eta & \eta T_q^{**} & & \eta^{s-1} T_q^{**}\eta \\ T_q^{**}\eta^2 & \eta T_q^{**2} & & \eta^{s-1} T_q^{**}\eta^2 \\ \vdots & \vdots & & \vdots \\ T_q^{**}\eta^{s-1} & \eta T_q^{**}\eta^{s-1} & \cdots & \eta^{s-1} T_q^{**}\eta^{s-1} \end{array}$$

where $q = 1,2,3,\ldots,m-1$.

Since the (bs)th row to $(b+1)$sth row of the T_q^{**} matrix consist of a pencil of $EG(m,s)$, $b = 0,1,2,\ldots,(s^{m-2}-1)$, it follows that L is a Latin square of order $s^m \times s^m$. Q.E.D.

Example 3.3.1. $s = 2$, $m = 3$, $t_1 = t_2 = 0$.

$v = s^m = 2^3 = 8$. $b = 28$, $k = 28$, $r = 98$, $m_r = 3$, $n_c = 3$

$\lambda_1 = \lambda_2 = 342$.

Let $0 = (0,0,0)$; $1 = (0,0,1)$, $2 = (0,1,0)$, $3 = (0,1,1)$, $4 = (1,0,0)$

$5 = (1,0,1)$, $6 = (1,1,0)$, $7 = (1,1,1)$.

G_1: $x_1 = 0$, $x_1 = 1$

G_2: $x_2 = 0$, $x_2 = 1$; $x_1 + x_2 = 0$, $x_1 + x_2 = 1$

G_3: $x_3 = 0$, $x_3 = 1$; $x_2 + x_3 = 0$, $x_2 + x_3 = 1$; $x_1 + x_2 + x_3 = 0$,

$x_1 + x_2 + x_3 = 1$; $x_1 + x_3 = 0$, $x_1 + x_3 = 1$.

Then $T_1 = \begin{matrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \end{matrix}$, $T_2 = \begin{matrix} 0 & 1 & 4 & 5 \\ 2 & 3 & 6 & 7 \\ 0 & 1 & 6 & 7 \\ 2 & 3 & 4 & 5 \end{matrix}$

$$T_1^* = \begin{matrix} 0 & 1 & 2 & 3 \\ 6 & 7 & 4 & 5 \end{matrix}, \qquad T_2^* = T_2^{**} = \begin{matrix} 0 & 1 & 4 & 5 \\ 2 & 3 & 6 & 7 \\ 6 & 7 & 0 & 1 \\ 4 & 5 & 2 & 3 \end{matrix}$$

$$T_1^{**} = \begin{matrix} 0 & 1 & 2 & 3 \\ 6 & 7 & 4 & 5 \\ 2 & 3 & 0 & 1 \\ 4 & 5 & 6 & 7 \end{matrix}, \qquad D_2 = \begin{matrix} 0 & 1 & 4 & 5 \\ 2 & 3 & 6 & 7 \\ 6 & 7 & 0 & 1 \\ 4 & 5 & 2 & 3 \\ 1 & 0 & 5 & 4 \\ 3 & 2 & 7 & 6 \\ 7 & 6 & 1 & 0 \\ 5 & 4 & 3 & 2 \end{matrix}$$

$$D_3 = \begin{matrix} 0 & 2 & 4 & 6 \\ 1 & 3 & 5 & 7 \\ 3 & 4 & 7 & 0 \\ 2 & 5 & 6 & 1 \\ 5 & 6 & 0 & 3 \\ 4 & 7 & 1 & 2 \\ 7 & 0 & 2 & 5 \\ 6 & 1 & 3 & 4 \end{matrix}$$

G_1': $x_3 = 0$, $x_3 = 1$

G_2': $x_2 = 0$, $x_2 = 1$; $x_3 + x_2 = 0$, $x_3 + x_2 = 1$,

G_3': $x_1 = 0$, $x_1 = 1$; $x_2 + x_1 = 0$, $x_2 + x_1 = 1$;

$x_3 + x_2 + x_1 = 0$, $x_3 + x_2 + x_1 = 1$;

$x_3 + x_1 = 0$, $x_3 + x_1 = 1$.

$$T_2' = \begin{matrix} 0 & 4 & 1 & 5 \\ 2 & 6 & 3 & 7 \\ 0 & 4 & 3 & 7 \\ 2 & 6 & 1 & 5 \end{matrix}, \qquad T_2'^* = T_2'^{**} = \begin{matrix} 0 & 4 & 1 & 5 \\ 2 & 6 & 3 & 7 \\ 3 & 7 & 0 & 4 \\ 1 & 5 & 2 & 6 \end{matrix}$$

$$D_2' = \begin{matrix} 0 & 4 & 1 & 5 \\ 2 & 6 & 3 & 7 \\ 3 & 7 & 0 & 4 \\ 1 & 5 & 2 & 6 \\ 4 & 0 & 5 & 1 \\ 6 & 2 & 7 & 3 \\ 7 & 3 & 4 & 0 \\ 5 & 1 & 6 & 2 \end{matrix}, \qquad D_3' = \begin{matrix} 0 & 2 & 1 & 3 \\ 4 & 6 & 5 & 7 \\ 6 & 1 & 7 & 0 \\ 2 & 5 & 3 & 4 \\ 5 & 3 & 0 & 6 \\ 1 & 7 & 4 & 2 \\ 7 & 0 & 2 & 5 \\ 3 & 4 & 6 & 1 \end{matrix}$$

$$A_{(2,0)} = [D_2^T] = \begin{matrix} 0 & 2 & 6 & 4 & 1 & 3 & 7 & 5 \\ 1 & 3 & 7 & 5 & 0 & 2 & 6 & 4 \\ 4 & 6 & 0 & 2 & 5 & 7 & 1 & 3 \\ 5 & 7 & 1 & 3 & 4 & 6 & 0 & 2 \end{matrix}$$

$$A'_{(2,0)} = D_2'^{T} = \begin{matrix} 0 & 2 & 3 & 1 & 4 & 6 & 7 & 5 \\ 4 & 6 & 7 & 5 & 0 & 2 & 3 & 1 \\ 1 & 3 & 0 & 2 & 5 & 7 & 4 & 6 \\ 5 & 7 & 4 & 6 & 1 & 3 & 0 & 2 \end{matrix}$$

$A = [[D_3^T]^{[2]} A_{(2,0)}]$, $A' = [[D_3'^T]^{[2]} [A'_{(2,0)}]]$

$D_3'^T$ $D_3'^T$ $D_2'^T$

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

$G =$

D_3

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

D_3

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

D_2

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

$(L)_3^3$

where L is a Latin square of order 8×8.

BIBLIOGRAPHY

BIBLIOGRAPHY

Agrawal, H. (1966). Some generalizations of distinct representatives with applications to statistical designs. Ann. Math. Statist. 37, pp. 525-528.

Albert, A.A. and Sandler, R. (1968). An Introduction to Finite Projective Planes. Holt, Rinehart and Winston, New York.

Bose, R.C. and Nair, K.R. (1939). Partially balanced incomplete block designs. Sankhya, Vol. 4, pp. 337-372.

Bose, R.C. and Shrikhande, S.S. (1960). On the construction of pairwise orthogonal Latin squares and falsity of a conjecture of Euler. Trans. Amer. Math. Soc. 95, pp. 191-209.

Cameron, P.J., Hall, J.I., VanLint, J.H., Springer, T.A. and van Tilborg, H.C.A. (1975). Translates of subgroups of the multiplicative group of a finite field. Nederl. Akad. Wetensch. Proc. Ser. A. 78, No. 4 and Indag. Math. 37, No. 4, pp. 285-289.

Cochran, W.G. and Cox, G.M. (1966). Experimental Designs. Wiley, New York.

Fisher, R.A. (1960). The Design of Experiments. Hafner, New York.

Gûerin, R. (1963). Aspects algebraiques du probléme de Yamamoto. C.R. Acad. Sci. Paris 256, pp. 583-586.

Gûerin, R. (1963). Sur une généralisation de la méthode de Yamamoto pour la construction de corrés latins orthogonaux. C.R. Acad. Sci. Paris 256, pp. 2097-2100.

Hall, M. (1956). An algorithm for distinct representatives. Amer. Math. Monthly 63, pp. 716-717.

Hall, M. (1967). Combinatorial Theory. Blasidell Publishing Co., Massachusetts.

Hartley, H.O. and Smith, C.A.B. (1948). The construction of Youden squares. J. Roy. Statistics Soc., Ser. B 10, pp. 262-263.

Hedayat, A. (1973). On constructing an OL(n,3) design by the method of sum composition. The Florida State University Statistics Report M284.

Hedayat, A. and Seiden, E. (1974). On the theory and application of sum composition of Latin squares and orthogonal Latin squares. Pacific Journal of Mathematics, Vol. 54, No. 2, pp. 86-113.

Horton, J.D. (1974). Sub-Latin squares and incomplete orthogonal arrays. J. Combinatorial Theory Ser. A 16, pp. 23-33.

John, P.W.M. (1971). Statistical Design and Analysis of Experiments. Macmillan, New York.

Kiefer, J. (1958). On the nonrandomized optimality and randomized nonoptimality of symmetrical designs. Ann. Math. Statist. 29, pp. 675-699.

Kiefer, J. (1959). Optimum experimental designs. J. Roy. Statist. Soc., Ser. B 21, pp. 272-319.

Kiefer, J. (1970). Optimum experimental designs. Proc. Intl. Congress Math. 3, Nice, Gauthiers-Villars, Paris, pp. 249-254.

Kiefer, J. (1971). The role of symmetry and approximation in exact deisgn optimality. Statistical Decision Theory and Related Topics, Academic Press, New York, pp. 109-118.

Kiefer, J. (1975). Balanced block designs and generalized Youden designs, I. Construction (patchwork). Ann. of Statist., Vol. 3, No. 1, pp. 109-118.

Kiefer, J. (1975). Construction and Optimality of Generalized Youden Designs. J.N. Srivastava, ed., A Survey of Statistical Design and Linear Models. North-Holland Publishing Company, pp. 333-353.

Parker, E.T. (1959). Orthogonal Latin squares. Proceedings of the National Academy of Sciences, Vol. 45, No. 6, pp. 859-862.

Ruiz, F. and Seiden, E. (1974). Some results on construction of orthogonal Latin squares by the method of sum composition. J. Combinatorial Theory Ser. A 16, pp. 230-240.

Ruiz, F. and Seiden, E. (1974). On construction of some families of generalized Youden Designs. Ann. of Statist. Vol 2, No. 3, pp. 503-519.

Seiden, E. (1950). A theorem in finite projective geometry and an application to statistics. Proc. Amer. Math. Soc., Vol. 1, pp. 282-286.

Seiden, E. (1954). On the problem of construction of orthogonal arrays. Ann. Math. Statist. 25, pp. 151-156.

Seiden, E. (1955). On the maximum number of constraints of an orthogonal array. Ann. Math. Statist. 26, pp. 132-135.

Seiden, E. (1955). Further remarks on the maximum number of constraints of an orthogonal array. Ann. Math. Statist. 26, pp. 759-763.

Seiden, E. and Zemach, R. (1966). On orthogonal arrays. Ann. Math. Statist. 37, pp. 1355-1370.

Shin, Chi-Chi (1965). A method of constructing orthogonal Latin squares (Chinese). Shunue Jinzhan. 8, pp. 98-104.

Shirkhande, S.S. (1951). Designs with two-way elimination of heterogeneity. Ann. Math. Statist. 22, pp. 235-247.

Wald, A. (1943). On the efficient design of statistical investigations. Ann. Math. Statist. 14, pp. 134-140.

Yamamoto, K. (1961). Generation principles of Latin squares. Bull. Inst. Internat. Statist. 38, pp. 73-76.