CONSTRUCTION OF SETS OF MUTUALLY ORTHOGONAL LATIN SQUARES

by

GLENN CHARLES CADEK

B.A., Wichita State University, 1973

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

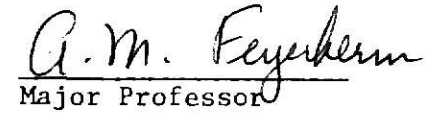
Department of Statistics

KANSAS STATE UNIVERSITY

Manhattan, Kansas

1975

Approved by:



Major Professor

TABLE OF CONTENTS

Chapter Page

1. INTRODUCTION

The interest in combinatorial problems, involving the arrangement of a finite number of objects in sets or patterns, satisfying given conditions, can be traced back at least as far as Euler [9] in 1782, who was interested in the construction of Latin and Graeco-Latin squares. However, it was not until the late 1920's and early 1930's that the importance of combinatorial problems, for the proper design of biological experiments, began to be understood, mainly through the work of Professor R. A. Fisher and his associates (Fisher [11]; Eden and Fisher [10]; Fisher and Wishart [12]; Wishart [24]; Yates [25,26]). In the late 1930's, C. R. Bose [2] made a systematic study of block designs and used Galois Fields [1] on the problem of constructing Hyper-Graeco-Latin squares.

In this report, a foundation for studying and investigating block designs is developed. The focus of concern will be with the construction and existence of mutually orthogonal Latin squares. The mathematics necessary for the construction of these designs involves Galois Field theory and finite geometries, which also comprise the groundwork for other types of block designs. One reason for starting with mutually orthogonal Latin squares (MOLS) is that they can be modified to form other types of block designs as shown by Raghavarao [22].

A Latin square of order s is defined to be an arrangement of s symbols in s^2 cells arranged in s rows and s columns, such that every symbol occurs once in each row and once in each column. This type of design is used in

THIS BOOK CONTAINS NUMEROUS PAGES WITH DIAGRAMS THAT ARE CROOKED COMPARED TO THE REST OF THE INFORMATION ON THE PAGE.

THIS IS AS RECEIVED FROM CUSTOMER.

experiments to remove the heterogeneity of experimental material in two directions and requires that the number of replications equal the number of treatments or varieties. For example, the Latin square of order 6 whose cells are occupied by the symbols A, B, C, D, E, F, can be represented:

B	D	A	E	C	F
D	A	C	B	F	E
E	F	D	A	B	C
A	C	E	F	D	B
C	B	F	D	E	A
F	E	B	C	A	D

If the symbols in the first row and first column of a Latin square are in alphabetic order or numeric order, it is said to be in "standard form", and if only the symbols of the first row are in this type of order it is said to be in "semistandard form". It is important to distinguish between these two concepts, since the standard form is useful in the randomization of Latin squares and the semistandard form is needed to study the properties of orthogonal Latin squares.

Two Latin squares are said to be orthogonal if when one is superimposed on the other, every ordered pair of symbols occurs exactly once. When two orthogonal Latin squares are superimposed, it is customary to use Latin letters for one square and Greek letters for the other square. The result is the well-known Graeco-Latin square. For convenience, sets of mutually orthogonal Latin squares of order s are referred to as MOLS of order s. A set of s-1 mutually orthogonal Latin squares of order s

forms a complete set of mutually orthogonal Latin squares. Some authors restrict the term Hyper-Graeco-Latin square to talking about superimposition of sets of MOLS which are complete sets.

When s is a prime number or the power of a prime number, a complete set of MOLS of order s can be constructed, and a method for doing this is presented in Chapter 2. According to Vajda [27] it is not known whether a complete set of MOLS exist when s is not a prime power. However, the existence of such a set has not been disproved except for special values of s.

The argument presented by Liu [15] can be used to demonstrate that there are at most s-1 Latin squares in a set of MOLS of order s. Consider $L_1, L_2, \ldots, L_r$ to be a set of MOLS of order s. Let $1_{ij}^{(1)}, 1_{ij}^{(2)}, \ldots, 1_{ij}^{(r)}$ (i,j = 0, 1, 2,...., s-1) denote the entries in the i-th row and the j-th column in $L_1, L_2, \ldots, L_n$ respectively. Notice that the orthogonality condition is not violated when the entries in the squares are renamed by permuting the symbols 0, 1, 2,...., s-1. Let us rename the entries in such a way that the first row of each of the squares reads 0, 1, 2, ..., s-1; that is,

$$1_{00}^{(1)} = 1_{00}^{(2)} = \ldots = 1_{00}^{(r)} = 0$$

$$1_{01}^{(1)} = 1_{01}^{(2)} = \ldots = 1_{01}^{(r)} = 1$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$1_{0s-1}^{(1)} = 1_{0s-1}^{(2)} = \ldots = 1_{0s-1}^{(r)} = s-1.$$

Now let us examine the entries in the second row and the first column

of the Latin squares $1_{10}^{(1)}$, $1_{10}^{(2)}$, ..., $1_{10}^{(r)}$. None of these entries can be 0. Otherwise, the condition that every square is a Latin square is violated. Also, no two of these entries can be the same. Otherwise, the condition that the set of Latin squares is an orthogonal set is violated. It follows then that there are at most s-1 Latin squares in the set L_1, L_2, ..., L_r.

It should be pointed out that there are no orthogonal Latin squares of orders 1 and 2. Trivially, there is only one Latin square of order 1. There are two Latin squares of order 2 as shown below, but they are not orthogonal.

$$L_1 = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \qquad L_2 = \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$$

Therefore, when we talk about MOLS of order s, s is understood to be greater than or equal to 3. Graeco-Latin squares exist for all orders except 6.

One purpose of this paper is to investigate the existence and construction of MOLS of order s where $s \leq 100$. Methods of construction where s is a prime or power of a prime will be discussed in Chapter 2 and Chapter 3. Chapter 3 will demonstrate the construction of equivalent Latin squares through the use of projective geometries and affine (or Euclidean) geometries. In addition, Chapter 3 will discuss the existence of complete sets of MOLS. Finally, Chapter 4 handles the case of MOLS of order s when s is not a prime or prime power.

A fairly complete and understandable presentation of Galois Fields, as given in Chapter 2, is a prime concern of this report. A full-length treatment of Galois Fields as it relates to the design of experiments is not available in book form because of the lack of textbooks dealing with

combinatorial aspects of experimental designs. Courses and research in the combinatorial theory of the design of experiments are on the increase, and the literature is available mainly in scattered papers in journals. This report will serve as an introduction to that area.

2. GALOIS FIELD THEORY AND MOLS

Basic to the construction of almost any type of experimental design is the concept of Galois Fields. A thorough knowledge of Galois Fields is necessary in order to study MOLS. In this chapter we start out in Section 2.1 with a brief study of groups, rings, and fields giving the axioms which define these concepts. In Section 2.2 the concept of a ring of polynomials is introduced. Then in 2.3 a thorough study of Galois Fields is presented giving particular emphasis to finding the multiplication and addition tables associated with a particular Galois Field. These tables are absolutely essential to the construction of complete sets of MOLS of order s, where s is a prime or a prime power, as is discussed in Section 2.4

2.1 Axioms for Groups, Rings, and Fields

A group consists of a set of elements a, b, c,... which have a single-valued binary operation, say addition denoted by +, such that the following four *axioms* are satisfied.

I. (Closure property)

For any two elements a and b of the group, there exists a unique element s belonging to the group defined by

$$a + b = s.$$

II. (Associativity property)

$$a + (b + c) = (a + b) + c$$

for all a, b, c in the group.

III. (Identity property)

There exists a unique element 0 belonging to the group with the property that

$$c + 0 = c$$

for any element c of the group.

IV. (Inverse property)

For any element a of the group, there exists a unique element a* such that

$$a + a^* = 0.$$

This element a* will be denoted by -a. By b - a we shall mean b + a* or b + (-a).

If in addition to these axioms, the following axiom also holds true, then the group is called a commutative group or an Abelian group.

V. (Commutative property)

$$a + b = b + a$$

for all a and b in the group.

A nonempty set of elements with two single-valued binary operations, say addition - denoted by + and multiplication - denoted by $\cdot$ or juxtaposition of elements, constitutes a ring if addition forms an Abelian group and multiplication satisfies the following axioms:

VI. (Closure property)

For any two elements a and b of the ring, there exists a unique element r belonging to the ring defined by

$$a \cdot b = r.$$

VII. (Associativity property)

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

for all a, b, c in the ring.

VIII. (Distributive property)

For any elements a, b, c in the ring

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

A ring satisfying the following axiom is called a commutative ring.

IX. (Commutative property)

$$ab = ba$$

for all a and b in the ring.

A commutative ring that satisfies axioms X. and XI. is said to be a field.

X. (Identity property)

There exists a unique element $1 \neq 0$ belonging to the field with the property that

$$a \cdot 1 = a$$

for any element a of the field.

XI. (Inverse property)

For any element $a \neq 0$ of the field, there exists a unique element a^{-1} such that

$$aa^{-1} = 1.$$

The systems of all rational numbers, all real numbers, and all complex numbers provide examples of fields.

Next we look at the concept of a ring of polynomials. Polynomials are used to represent the elements of a Galois Field, and an understanding of addition and multiplication is necessary in building a Galois Field.

2.2 The Ring of Polynomials F[x].

Let F be a field. Then according to Maxfield [18] expressions like

$$(2.2.1) \qquad a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

where $a_i \in F$ for $i = 0, 1, 2, \ldots, n$ and $n \geq 0$ is an integer, forms a ring F[x] under the operations of + and $\cdot$ defined by

$$(2.2.2) \qquad \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

(2.2.3) and $$\sum_{i=0}^{m} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j = \sum_{k=0}^{m+n} c_k x^k,$$

where $$c_k = \sum_{i+j=k} a_i b_j.$$

The degree of a particular polynomial is the maximum i for which $a_i \neq 0$.

Polynomials over a field do not form a field since nonzero polynomials of positive degree do not have multiplicative inverses, that is, they fail to satisfy axiom XI. This results from the fact that any two nonzero polynomials when multiplied together, result in a product having degree greater than or equal to one, but the multiplicative identity polynomial is 1 and has degree 0.

2.3 The Galois Field $GF(p^n)$.

The mathematical systems of interest to a statistician designing experiments are fields containing only a finite number of elements. Such systems are called Galois Fields. First we will talk about modular arithmetic, the simplest example of a Galois Field. Then the general case of a Galois Field will be presented and a procedure for constructing addition and multiplication tables in this Field is given.

2.3.1 The Galois Field GF(p)

The element a is said to be congruent to b modulus p if a - b is divisible by p. This is notated by $a \equiv b \pmod{p}$; p is the modulus of congruence and b is called the residue. For a given positive integer p, a modular arithmetic is obtained by using only the integers 0, 1, 2, ..., p-1 and defining addition and multiplication by letting the

sum a + b and the product ab be the remainder after division by p.

For example, if p = 6 then the addition and multiplication tables are:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Notice from the multiplication table that there does not exist an element which when multiplied by 3 gives 1; that is, 3 has no multiplicative inverse. Modular arithmetic mod p is a commutative ring with mulitplicative identity element; if p is a prime then arithmetic mod p forms a field.

The field of classes of residues mod p, where p is any positive prime integer gives the simplest example of a Galois Field. Consider all integers congruent to one another mod p belonging to the same class, and let the class to which the integer a belongs be denoted by (a). Then (a) = (b) if and only if $a \equiv b \pmod{p}$. So there exists only p different classes (0), (1), (2), ..., (p-1). These are the residue classes (mod p) with addition and multiplication of these classes defined by

(2.3.1.1) $$(a) + (b) = (a + b)$$

(2.3.1.2) $$(a) \cdot (b) = (ab).$$

This type of Galois Field is denoted GF(p).

For instance, if p = 5 the five different classes are (0), (1), (2), (3), (4). Examples of addition and multiplication of these classes are

$$(1) + (2) = (3) \qquad (2) + (4) = (6) = (1)$$

$$(1) \cdot (2) = (2) \qquad (3) \cdot (4) = (12) = (2).$$

For residue classes, the integer a is a representative of the class (a). The standard representative of the class (a) is the only non-negative integer less than p which is a representative of (a). The elements of GF(5) are (0), (1), (2), (3), and (4), but these classes will be denoted by their standard representatives 0, 1, 2, 3, and 4.

The addition table and multiplication table of GF(p) are used in working with the coefficients of the polynomials that are elements of the general type of Galois Field. These tables are also used to construct complete sets of MOLS of order s when s is a prime.

The concept of modular arithmetic or GF(p) where elements of the field are sets of non-negative integers can be extended to the general case where the elements of the field are polynomials, and this is our next topic.

2.3.2 The Galois Field $GF(p^n)$

A polynomial f(x) of positive degree is irreducible in F[x] if it has no factorization

$$f(x) = g(x)h(x) \tag{2.3.2.1}$$

with g(x) and h(x) in F[x] of positive degrees. If $f(x) = g(x)h(x) \in F[x]$,

then f(x) is reducible over F[x].

The irreducibility of a polynomial depends on the field it is defined over. For example, the polynomial $x^2 + 1$ is irreducible over the real numbers, but is reducible over GF(5) as

$$(x + 2)(x + 3) = x^2 + 5x + 6 = x^2 + 1$$

since $5 \equiv 0 \pmod 5$ and $6 \equiv 1 \pmod 5$.

Let f(x) be an irreducible polynomial of F[x], then two polynomials p(x) and q(x) are congruent modulo f(x) if p(x) - q(x) is divisible by f(x) and this is written

(2.3.2.2) $$p(x) \equiv q(x) \pmod{f(x)}.$$

For example, if F is GF(7) and

$$p(x) = 3x^2 + 6x + 4 \qquad q(x) = x^2 + 4x + 4,$$

then $$p(x) \equiv q(x) \pmod{(x + 1)},$$

since $$p(x) - q(x) = 2x^2 + 2x \text{ is divisible by } x + 1.$$

For a given f(x), the class of all polynomials congruent to p(x) mod f(x) may be denoted by [p(x)]. Addition and multiplication of these classes may be defined as

(2.3.2.3) $$[p(x)] + [q(x)] = [p(x) + q(x)]$$

(2.3.2.4) $$[p(x)] \cdot [q(x)] = [p(x)q(x)].$$

When f(x) is an irreducible polynomial, then the residue classes

(mod f(x)) form a field. The polynomial p(x) is a representative of the class [p(x)]. The standard representative of [p(x)] is the only polynomial which is representative of p(x) and has degree smaller than the degree of f(x).

The most general Galois Field, denoted by $GF(p^n)$ contains p^n elements, where p is a positive prime number and n any positive integer. The prime is called the characteristic of the field. In order to construct the elements of this field, let f(x) be an irreducible polynomial over GF(p) in x of degree n with coefficients belonging to GF(p) and let P(x) be any polynomial in x with integral coefficients. Then P(x) can be written as

$$P(x) = p(x) + p \cdot r(x) + f(x) \cdot s(x), \tag{2.3.2.5}$$

where $p(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_2x^2 + a_1x + a_o$ and the coefficients a_i $(i = 0, 1, \ldots, n-1)$ belong to GF(p). Raghavarao [22] states that this relationship may be written as

$$P(x) \equiv p(x) \bmod\{p, F(x)\}. \tag{2.3.2.6}$$

Exactly what equation 2.3.2.5 means and how it is used will become more clear when construction of the multiplication table for $GF(p^n)$ is discussed.

The functions P(x) that satisfy this relation when p(x), p, and f(x) are kept fixed form a residue class. If p and f(x) are kept constant, but p(x) is varied, then p^n residue classes may be formed since each coefficient in p(x) may take on the p values of GF(p). The residue classes defined by p(x) form the Galois Field. The function f(x) is called the minimum function for generating the elements of $GF(p^n)$. The candidates for an irreducible polynomial f(x) for $GF(p^n)$ are all polynomials of the form

$$(2.3.2.7) \qquad f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

where $a_i = 0, 1, 2, \ldots, p-1 \quad i = 0, 1, 2, \ldots, n$ except that $a_n \neq 0$.

For an example of such a field consider $p = 3$ and $n = 2$ so that we have $GF(3^2)$. All possible elements for this field are $p(x) = a_1 x + a_0$ where $a_i = 0, 1, 2 \quad (i = 0, 1)$. Hence $p(x)$ can be

$$0x + 0 = 0$$

$$0x + 1 = 1$$

$$0x + 2 = 2$$

$$1x + 0 = x$$

$$1x + 1 = x + 1$$

$$1x + 2 = x + 2$$

$$2x + 0 = 2x$$

$$2x + 1 = 2x + 1$$

$$2x + 2 = 2x + 2 \ .$$

The candidates for an irreducible polynomial $f(x)$ for $GF(3^2)$ are all polynomials of the form

$$f(x) = a_2 x^2 + a_1 x + a_0$$

where $a_2 = 1$ or 2 but $a_2 \neq 0$ and $a_i = 0, 1, 2 \qquad i = 0, 1$. The possible alternatives for $f(x)$ are:

$1x^2 + 0x + 0 = x^2 = x \cdot x$

$1x^2 + 0x + 1 = x^2 + 1$ irreducible

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

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

$1x^2 + 1x + 1 = x^2 + x + 1 = (x + 2)(x + 2)$

$1x^2 + 1x + 2 = x^2 + x + 2$ irreducible

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

$1x^2 + 2x + 1 = x^2 + 2x + 1 = (x + 1)(x + 1)$

$1x^2 + 2x + 2 = x^2 + 2x + 2$ irreducible

$2x^2 + 0x + 0 = 2x^2 = 2x \cdot x$

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

$2x^2 + 0x + 2 = 2x^2 + 2$ irreducible

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

$2x^2 + 1x + 1 = 2x^2 + x + 1$ irreducible

$2x^2 + 1x + 2 = 2x^2 + x + 2 = (2x + 2)(x + 1)$

$2x^2 + 2x + 0 = 2x^2 + 2x = (2x + 2)x$

$2x^2 + 2x + 1 = 2x^2 + 2x + 1$ irreducible

$2x^2 + 2x + 2 = 2x^2 + 2x + 2 = (2x + 1)(x + 2)$

The polynomial is irreducible if it can not be factored into elements of the Galois Field. Inspection of some polynomials reveals that they can be factored by 2 or x. The remaining reducible polynomials can be factored by considering a systematic examination of products of pairs of the remaining field elements $x + 1$, $x + 2$, $2x + 1$, and $2x + 2$. $2x$ need not be considered since $2x = x \cdot 2$.

Notice that one of x, x + 1, x + 2 is a factor for each polynomial that is reducible. If a polynomial is reducible then there exists an integer d which is a member of GF(p) such that x + d is a factor of this polynomial, otherwise the polynomial is irreducible.

In order to construct the addition table for $GF(3^2)$, one must perform normal algebraic operations on the field elements and use modular arithmetic to reduce coefficients outside the field back into the field. This leads to the following addition table

x	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	1	2	0	x+1	x+2	x	2x+1	2x+2	2x
2	2	0	1	x+2	x	x+1	2x+2	2x	2x+1
x	x	x+1	x+2	2x	2x+1	2x+2	0	1	2
x+1	x+1	x+2	x	2x+1	2x+2	2x	1	2	0
x+2	x+2	x	x+1	2x+2	2x	2x+1	2	0	1
2x	2x	2x+1	2x+2	0	1	2	x	x+1	x+2
2x+1	2x+1	2x+2	2x	1	2	0	x+1	x+2	x
2x+2	2x+2	2x	2x+1	2	0	1	x+2	x	x+1

It is possible for all the entries in this table or any addition or multiplication table for $GF(p^n)$ to be represented by some set of nonnegative integers. How this is accomplished will become clear later when the concepts additive form and multiplicative form are defined.

In order to define multiplication in $GF(p^n)$ so that this operation satisfies the properties of a field, every non-zero element α of $GF(p^n)$ must satisfy the equation

(2.3.2.8) $$y^{p^n-1} = 1$$

which assures that all of the p^n-1 non-zero elements are covered in the multiplication cycle.

We shall define α to be a primitive mark of $GF(p^n)$ if α is root of $y^{p^n-1} - 1 = 0$ such that $p^n - 1$ is the smallest positive integer for which $\alpha^{p^n-1} = 1$. For simplicity's sake, it is customary to choose the primitive mark $\alpha = x$.

Reduction of polynomials not in $GF(p^n)$ with powers larger than $n - 1$ can be accomplished by selecting one of the irreducible polynomials and setting it equal to zero and then solving for x^n in order to establish multiplicative relationships. To solve for x^n, add a polynomial to both sides of the equation which, when using modular arithmetic on the coefficients, allows the left hand side of the equation to reduce to x^n.

For example in $GF(3^2)$, the possible multiplicative relationships are:

$$\begin{array}{lll} x^2 + 1 = 0 & x^2 + x + 2 = 0 & x^2 + 2x + 2 = 0 \\ \underline{\quad + 2 = 2} & \underline{\quad + 2x + 1 = 2x + 1} & \underline{\quad + x + 1 = x + 1} \\ x^2 = 2 & x^2 = 2x + 1 & x^2 = x + 1 \end{array}$$

$$\begin{array}{lll} 2x^2 + 2 = 0 & 2x^2 + x + 1 = 0 & 2x^2 + 2x + 1 = 0 \\ \underline{\quad + x^2 = x^2} & \underline{\quad + x^2 = x^2} & \underline{\quad + x^2 = x^2} \\ 2 = x^2 & x + 1 = x^2 & 2x + 1 = x^2 \end{array}$$

Choosing the irreducible polynomial $f(x) = x^2 + x + 2 = 0$ so that $x^2 = 2x + 1$ and choosing the primitive mark equal to x provides the following relations;

$$0$$

$$1 = y^8 = x(x + 1) = x^2 + x = (2x + 1) + x = 1$$

$$2 = y^4 = x(2x + 2) = 2x^2 + 2x = 2(2x + 1) + 2x$$

$$= 4x + 2 + 2x = 6x + 2 = 2$$

$$x = y^1$$

$$x+1 = y^7 = x(x + 2) = x^2 + 2x = (2x + 1) + 2x$$

$$4x + 1 = x + 1$$

$$x+2 = y^6 = x \cdot 2x = 2x^2 = 2(2x + 1) = 4x + 2 = x + 2$$

$$2x = y^5 = x \cdot 2 = 2x$$

$$2x+1 = y^2 = x^2 = 2x + 1$$

$$2x+2 = y^3 = y \cdot y^2 = x(2x + 1) = 2x^2 + x = 2(2x + 1) + x$$

$$= 4x + 2 + x = 5x + 2 = 2x + 2$$

Choosing the irreducible polynomial $f(x) = x^2 + 2x + 2 = 0$ so that $x^2 = x + 1$ and selecting the primitive mark equal to x yields the following relations

$$0$$

$$1 = y^8$$

$$2 = y^4$$

$$x = y^1$$

$$x+1 = y^2$$

$$x+2 = y^7$$

$$2x = y^5$$

$$2x+1 = y^3$$

$$2x+2 = y^6$$

Another possibility is the choice of irreducible polynomial $f(x) = x^2 + 1$

so that $x^2 = 2$. Choice of the primitive mark being x causes the multiplicative cycle to close before all non-zero elements are covered in the field. The following computations show that the field elements $x + 1$, $x + 2$, $2x + 1$, and $2x + 2$ are not represented by this multiplicative relationship when x is the primitive mark.

0

$1 = y^4 = x \cdot 2x = 2x^2 = 2(2) = 4 \equiv 1 \pmod 3$

$2 = y^2$

$x = y^1 = y^5 = 1 \cdot x = x$(primitive mark)

$x+1$

$x+2$

$2x = y^3 = x \cdot 2 = 2x$

$2x+1$

$2x+2$

However, choosing the primitive mark to be $x + 1$ allows all non-zero elements to be covered when using the multiplicative relationship $x^2 = 2$. This is demonstrated by the following results.

0

$1 = y^8$

$2 = y^4$

$x = y^6$

$x+1 = y^1$(primitive mark)

$x+2 = y^7$

$2x = y^2$

$2x+1 = y^3$

$2x+2 = y^5$

Only irreducible polynomials that are factors of the cyclotomic polynomial (to be defined below) will always assure that all non-zero elements in the field are covered by the multiplicative cycle when x is the primitive mark. Consider the equation $x^t - 1 = 0$. A root of this equation is of <u>order r</u> if r is the smallest positive integer for which $\alpha^r - 1 = 0$. We say that α is a primitive root of the equation $x^t - 1 = 0$ if is of order t. The <u>cyclotomic polynomial of order t</u> is the polynomial c(x) such that c(x) = 0 is the equation which has for its roots, all primitive roots of $x^t - 1 = 0$. Hence the factors of c(x) that are irreducible polynomials, have as their roots all elements α_i of the field over which the polynomials are defined. These $\alpha_i = x$ satisfy the definition of a primitive mark if we are working in $GF(p^n)$ and $t = p^n - 1$.

In order to obtain the cyclotomic polynomial, we must remove from $x^t - 1$ all factors corresponding to non-primitive roots. If t is a prime number, then the cyclotomic polynomial of order t is given by

$$(2.3.2.9) \qquad x^{t-1} + x^{t-2} + x^{t-3} + \ldots + x + 1 \ .$$

For example, if t = 7, the cyclotomic polynomial of order 7 is

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

When t is not a prime number, then the decomposition of t is

$$t = p_1^{c_1} \ p_2^{c_2} \ \ldots \ p_k^{c_k}$$

and the cyclotomic polynomial as given by Bose[3] is

$$(2.3.2.10) \qquad c(x) = \frac{(x^t - 1)\Pi((x^{t/p_i p_j} - 1)\Pi(x^{t/p_i p_j p_k p_l} - 1) \ldots}{\Pi(x^{t/p_i} - 1)\Pi(x^{t/p_i p_j p_k} - 1) \ldots} .$$

The degree of the cyclotomic polynomial of order t is

$$(2.3.2.11) \qquad \phi(t) = t(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots . (1 - \frac{1}{p_k})$$

where ϕ is the Euler function giving the number of positive integers less than t and relatively prime to it.

For example, if $t = 60 = 2^2 \cdot 3 \cdot 5$, then

$$c(x) = \frac{(x^{60} - 1)(x^{60/2 \cdot 3} - 1)(x^{60/2 \cdot 5} - 1)(x^{60/3 \cdot 5} - 1)}{(x^{60/2} - 1)(x^{60/3} - 1)(x^{60/5} - 1)(x^{60/2 \cdot 3 \cdot 5} - 1)}$$

$$= \frac{(x^{60} - 1)(x^{10} - 1)(x^6 - 1)(x^4 - 1)}{(x^{30} - 1)(x^{20} - 1)(x^{12} - 1)(x^2 - 1)} .$$

When $t = p^n - 1$ and the cyclotomic polynomial is of order $p^n - 1$ and belongs to the ring GF(p)[x] and f(x) is an irreducible factor of the cyclotomic polynomial over GF(p), then f(x) is often called a <u>minimum function</u> for the field $GF(p^n)$. There are $\frac{1}{n} \phi (p^n - 1)$ distinct minimum functions any one of which may be chosen for f(x). The advantage of choosing f(x) to be a minimum polynomial, rather than one of the other irreducible polynomials, is that the class [x] is a primitive mark of $GF(p^n)$. This also assures us that the multiplicative cycle will cover all non-zero field elements exactly once before repeating.

For the case $p^n = 5^2$, the ordinary cyclotomic polynomial of order 24 is

$$\frac{(x^{24} - 1)(x^4 - 1)}{(x^{12} - 1)(x^8 - 1)} = x^8 - x^4 + 1$$

hence the corresponding cyclotomic polynomial of GF(5)[x] is

$$x^8 + 4x^4 + 1$$

where the integers are now standard representatives of classes of residues moduluo 5. This can be factored as

$$(x^2 + 2x + 3)(x^2 + x + 2)(x^2 + 4x + 2)(x^2 + 3x + 3).$$

The cyclotomic polynomial of order 8, used to find minimum functions for $GF(3^2)$ is

$$c(x) = \frac{x^8 - 1}{x^4 - 1} = x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$$

Let $f_1(x) = x^2 + x + 2$ be a minimum function and $f_2(x) = x^2 + 2x + 2$ be another possible choice. Taking classes modulo $f_1(x)$ and modulo $f_2(x)$, we have

mod $f_1(x)$	mod $f_2(x)$
$[0] = [0]$	$[0] = [0]$
$[1] = [1]$	$[1] = [1]$
$[x] = [x]$	$[x] = [x]$
$[x^2] = [2x + 1]$	$[x^2] = [x + 1]$
$[x^3] = [2x + 2]$	$[x^3] = [2x + 1]$
$[x^4] = [2]$	$[x^4] = [2]$
$[x^5] = [2x]$	$[x^5] = [2x]$
$[x^6] = [x + 2]$	$[x^6] = [2x + 2]$
$[x^7] = [x + 1]$	$[x^7] = [x + 2]$

Two Galois Fields with the same number of elements are isomorphic, i.e. structurally identical. This means it is possible to make a one-to-one correspondence between their elements in such a way that the sum of two elements, corresponds to the sum of the corresponding elements, and the same holds for the product of two elements. Hence, irregardless of choice of minimum function, the resulting fields will be isomorphic.

To illustrate this, let the above residue classes with respect to $f_1(x)$ be denoted by $[a_1x + a_0]$ and the residue classes with respect to $f_2(x)$ be denoted by $\{a_1x + a_0\}$ where a_0, $a_1 = 0, 1, 2$. Then the field of residue classes $[a_1x + a_0]$ is isomorphic to the field of residue classes $\{a_1x + a_0\}$. This is shown by the correspondence

$$
\begin{aligned}
[0] &\rightarrow \{0\} \\
[1] &\rightarrow \{1\} \\
[x] &\rightarrow \{x\} \\
[2x+1] &\rightarrow \{x+1\} \\
[2x+2] &\rightarrow \{2x+1\} \\
[2] &\rightarrow \{2\} \\
[2x] &\rightarrow \{2x\} \\
[x+2] &\rightarrow \{2x+2\} \\
[x+1] &\rightarrow \{x+2\} \quad .
\end{aligned}
$$

Consider the elements $[2x + 2]$ and $[x + 1]$ of the first field. Their sum is $[0]$ and their product is $[2x + 1]$. The elements corresponding to $[2x + 2]$ and $[x + 1]$ are $\{2x + 1\}$ and $\{x + 2\}$. Their sum is $\{0\}$ and their product is $\{x + 1\}$. Notice that the sum $[0]$ corresponds to the sum $\{0\}$ and the product $[2x + 1]$ corresponds to the product $\{x + 1\}$. Similar

results hold when using other pairs of elements.

The addition table previously constructed for $GF(3^2)$ remains unchanged regardless of the choice of minimum function. If $f_1(x) = x^2 + x + 2$ is the minimum function for $GF(3^2)$, then the multiplication table is:

·	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	2x+1	1	x+1	x+2	2x+2	2
x+1	0	x+1	2x+2	1	x+2	2x	2	x	2x+1
x+2	0	x+2	2x+1	x+1	2x	2	2x+2	1	x
2x	0	2x	x	x+2	2	2x+2	2x+1	x+1	1
2x+1	0	2x+1	x+2	2x+2	x	1	x+1	2	2x
2x+2	0	2x+2	x+1	2	2x+1	x	1	2x	x+2

If $f_2(x) = x^2 + 2x + 2$ is the minimum function for $GF(3^2)$, the multiplication table is:

·	0	1	2	x	x+1	x+2	2x	x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	x+1	2x+1	1	2x+2	2	x+2
x+1	0	x+1	2x+2	2x+1	2	x	x+2	2x	1
x+2	0	x+2	2x+1	1	x	2x+2	2	x+1	2x

·	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2x	0	2x	x	2x+2	x+2	2	x+1	1	2x+1
2x+1	0	2x+1	x+2	2	2x	x+1	1	2x+2	x
2x+2	0	2x+2	x+1	x+2	1	2x	2x+1	x	2

Because of the isomorphism between any two sets of field elements due to different minimum functions, only one multiplication table is needed since no new information is contained in other tables. The isomorphism property also allows one to choose any minimum function for multiplication table construction.

In the general case when f(x) is a minimum function, Bose [3] states that each non-zero element of the Galois Field GF(p^n) can be expressed in three different ways, first as a power of the primitive element [x], i.e., as

$$[x]^i, \qquad i = 0, 1, 2, \ldots, p^n - 2,$$

which is called the multiplicative form; and second, as the class

$$[a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0],$$

where $a_o, a_1, \ldots, a_{n-1}$ are all elements of GF(p) (not all zero) which is called the additive form. The third form is the alpha form where

$$\alpha_0 = 0 \quad \text{and} \quad \alpha_i = x^{i-1} \quad \text{for } i = 1, 2, \ldots, p^n - 1.$$

When f(x) and p are given, it is often convenient to drop the bracket and write the elements as x^i or $a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0$.

Continuing the example of $GF(3^2)$ when $f(x) = x^2 + x + 2$, the nine elements may be written as:

Alpha Form	Multiplicative Form	Additive Form
α_0	0	0
α_1	1	1
α_2	x	x
α_3	x^2	2x+1
α_4	x^3	2x+2
α_5	x^4	2
α_6	x^5	2x
α_7	x^6	x+2
α_8	x^7	x+1

When adding or subtracting use the additive form, remember that the coefficients add (mod 3). To multiply or divide, use the multiplicative form remembering that $x^8 = 1$. Thus

$$\alpha_3 + \alpha_8 = (2x + 1) + (X + 1) = 2 = \alpha_5;$$

$$\alpha_6 \cdot \alpha_8 = x^5 \cdot x^7 = x^{12} = x^8 \cdot x^4 = x^4 = \alpha_5;$$

$$\frac{\alpha_3}{\alpha_7} = \frac{x^2}{x^6} = \frac{x^{10}}{x^6} = x^4 = \alpha_5 .$$

There are two ways of determining the additive form that corresponds to a given multiplicative form. The easier method is to set the minimum function equal to zero and solve for x^n. For example, $x^2 + x + 2 = 0$ implies $x^2 = 2x + 1$. Then use the recursive relationship $x^s = x \cdot x^{s-1}$ where s takes on the values of $n + 1$ to $p^n - 1$ in order to build up the correspondences. We always start with $\alpha_0 = 0$ then use $\alpha_i = x^i$ $\quad i = 0, 1, 2, \ldots, n - 1$ to cover the first n α_i's.

Another approach for determining x^s where $n + 1 \leq s \leq p^n - 1$ is to first divide x^s by the minimum function f(x) which provides some remainder, say h(x). If h(x) is one of the additive forms then we are finished, but if h(x) is not an additive form, then use mod p arithmetic to reduce h(x) to one of the additive forms. Essentially we are making use of the earlier stated relationship $P(x) \equiv p(x) \bmod\{p, f(x)\}$ which means

$$P(x) = p(x) + p \cdot r(x) + f(x) \cdot s(x),$$

wher $P(x) = x^s$, $f(x) = f(x)$, and $h(x) = p(x) + p \cdot r(x)$. The division of P(x) by f(x) reduces a polynomial of degree larger than $n - 1$ back down to a polynomial of degree $n - 1$ or smaller and division by p or

modular arithmetic finishes the reduction so that the final element is a member of $GF(p^n)$. It is this type of relationship that assures the closure properties of the field.

In order to construct the multiplication table, all possible pairs of additive forms can be multiplied and then reduced either by setting the minimum function equal to zero and using the resulting relationship with recursive calculations or by dividing the product by the minimum function and using modular arithmetic on the remainder. If correspondence has already been established between multiplicative forms and additive forms, then multiplication can be accomplished by using adding exponents mod p.

The entries in the addition table and multiplication table may be the additive forms, the multiplicative forms, the α_i notation or the subscripts only from the α_i that is i = 0, 1, 2, ..., $p^n - 1$.

GF(2)

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

GF(3)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$GF(2^2)$

$\alpha_0 = 0 \quad \alpha_1 = 1 \quad \alpha_2 = x \quad \alpha_3 = x^2 = x + 1$

+	α_0	α_1	α_2	α_3
α_0	α_0	α_1	α_2	α_3
α_1	α_1	α_0	α_3	α_2
α_2	α_2	α_3	α_0	α_1
α_3	α_3	α_2	α_1	α_0

·	α_0	α_1	α_2	α_3
α_0	α_0	α_0	α_0	α_0
α_1	α_0	α_1	α_2	α_3
α_2	α_0	α_2	α_3	α_1
α_3	α_0	α_3	α_1	α_2

In GF(2^3) using the minimum function $x^3 + x^2 + 1$ which implies $x^3 = x^2 + 1$, then

$$\alpha_0 = 0 \quad \alpha_1 = 1 \quad \alpha_2 = x \quad \alpha_3 = x^2 \quad \alpha_4 = x^3 = x^2 + 1$$

$$\alpha_5 = x^4 = x^2 + x + 1 \quad \alpha_6 = x^5 = x + 1 \quad \alpha_7 = x^6 = x^2 + x$$

+	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7
α_0	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7
α_1	α_1	α_0	α_6	α_4	α_3	α_7	α_2	α_5
α_2	α_2	α_6	α_0	α_7	α_5	α_4	α_1	α_3
α_3	α_3	α_4	α_7	α_0	α_1	α_6	α_5	α_2
α_4	α_4	α_3	α_5	α_1	α_0	α_2	α_7	α_6
α_5	α_5	α_7	α_4	α_6	α_2	α_0	α_3	α_1
α_6	α_6	α_2	α_1	α_5	α_7	α_3	α_0	α_4
α_7	α_7	α_5	α_3	α_2	α_6	α_1	α_4	α_0

$\cdot$	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7
α_0	α_0	α_0	α_0	α_0	α_0	α_0	α_0	α_0
α_1	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7
α_2	α_0	α_2	α_3	α_4	α_5	α_6	α_7	α_1
α_3	α_0	α_3	α_4	α_5	α_6	α_7	α_1	α_2
α_4	α_0	α_4	α_5	α_6	α_7	α_1	α_2	α_3
α_5	α_0	α_5	α_6	α_7	α_1	α_2	α_3	α_4
α_6	α_0	α_6	α_7	α_1	α_2	α_3	α_4	α_5
α_7	α_0	α_7	α_1	α_2	α_3	α_4	α_5	α_6

Notice pattern in multiplication table - this makes for easy construction.

Since factorization of a cyclotomic polynomial is not always easy, the following table provides help by listing possible minimum functions necessary for constructing Galois Fields up to $GF(3^3)$.

GF	Minimum Function
2^2	$x^2 + x + 1$
2^3	$x^3 + x^2 + 1$ or $x^3 + x + 1$
3^2	$x^2 + x + 2$ or $x^2 + 2x + 2$
2^4	$x^4 + x^3 + 1$ or $x^4 + x + 1$
5^2	$x^2 + 2x + 3$ or $x^2 + x + 2$ or $x^2 + 4x + 2$ or $x^2 + 3x + 3$
3^3	$x^3 + 2x + 1$ or $x^3 + 2x^2 + 1$ or $x^3 + x^2 + 2x + 1$ or $x^3 + 2x^2 + x + 1$

In $GF(2^4)$ using the minimum function $x^4 + x + 1$ so that $x^4 = x + 1$, then

$$\alpha_0 = 0 \quad \alpha_1 = 1 \quad \alpha_2 = x \quad \alpha_3 = x^2 \quad \alpha_4 = x^3 \quad \alpha_5 = x^4 = x + 1$$

$$\alpha_6 = x^5 = x^2 + x \quad \alpha_7 = x^6 = x^3 + x^2 \quad \alpha_8 = x^7 = x^3 + x + 1$$

$$\alpha_9 = x^8 = x^2 + 1 \quad \alpha_{10} = x^9 = x^3 + x \quad \alpha_{11} = x^{10} = x^2 + x + 1$$

$$\alpha_{12} = x^{11} = x^3 + x^2 + x \quad \alpha_{13} = x^{12} = x^3 + x^2 + x + 1$$

$$\alpha_{14} = x^{13} = x^3 + x^2 + 1 \quad \alpha_{15} = x^{14} = x^3 + 1$$

There are a few useful references on Galois Fields. Volume 12 of the Bulletin of the American Mathematical Society for 1905 gives, on pages 22 to 38, listings of correspondences between multiplicative forms and additive forms for Galois Fields where $p^n \leq 169$. Volume 16 of the same journal gives listings on pages 188 to 206 for $p^n < 1000$.

A method of constructing irreducible polynomials by automatic computation is discussed in volume 14 of Mathematics of Computation for 1960 on pages 99 to 103.

2.4 Construction of Complete Sets of MOLS

A Galois Field of order $s = p^n$ where p is a positive prime integer and n is a positive integer will be used to construct a complet set of s - 1 MOLS of order s. For this we need the addition and multiplication tables for $GF(p^n)$.

Let x be a primitive root of GF(s) and let the elements be chosen as $\alpha_0 = 0$, $\alpha_1 = 1$, $\alpha_2 = x$, ..., $\alpha_{s-1} = x^{s-2}$. If in the (i,j)the cell of the t-th s x s square we put the number u determined by

$$\alpha_u = \alpha_i \alpha_t + \alpha_j \qquad t = 1, 2, \ldots, s-1; \quad i,j = 0, 1, 2, \ldots s-1, \tag{2.4.1}$$

then we get a Latin square L_t. The s - 1 squares $L_1, L_2, \ldots, L_{s-1}$

form a complete set of mutually orthogonal Latin squares.

Raghavarao [22] uses the following argument to verify that L_t is a Latin square, and Latin squares L_t and L_w $(t \neq w)$ are orthogonal. In L_t in the j-th column (j = 0, 1, ..., s - 1) each of the s distinct elements of GF(s) occurs exactly once. In fact, when i varies from 0, 1, ..., s - 1, $\alpha_i\alpha_t$ will take each value of GF(s), and so $\alpha_i\alpha_t + \alpha_j$ will take each value of GF(s). In the same manner it can be seen that each element of GF(s) will occur exactly once in the i-th row (i = 0, 1, ..., s - 1). Now consider two Latin squares L_t and L_w as well as their (i,j)th cells. Suppose the element in L_t is $\alpha_i\alpha_t + \alpha_j = \alpha_x$ and in L_w it is $\alpha_i\alpha_w + \alpha_j = \alpha_y$. Given α_x, α_y, α_t, and α_w and the fact that these elements belong to a field then we can solve these equations for α_i and α_j:

$$\alpha_i = \frac{\alpha_y - \alpha_x}{\alpha_w - \alpha_t} \qquad \alpha_j = \frac{\alpha_x\alpha_w - \alpha_t\alpha_y}{\alpha_w - \alpha_t},$$

and the solution is unique. Since these are unique, the ordered pair (α_x, α_y) will occur on the superimposition of L_t on L_w in the (i,j)th cell as determined by these solutions. Thus every ordered pair occurs exactly once.

The special case of n = 1 so that s = p is a prime number allows us to identify α_i with the residue class (i), mod p. Then the number u to be put in the cell (i,j) of L_t is given by

$$u = it + j,$$

where i, t, j, u are standard representatives of residue classes mod p. The addition and multiplication tables of GF(p) are very helpful in determining u.

For example, if s = 5, then the four mutually orthogonal Latin squares of order 5 obtained by this method are:

L_1

$u = i + j$

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

L_2

$u = 2i + j$

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

L_3

$u = 3i + j$

0	1	2	3	4
3	4	0	1	2
1	2	3	4	0
4	0	1	2	3
2	3	4	0	1

L_4

$u = 4i + j$

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

Notice that square L_1 is the addition table for GF(5); it can be seen by examining the formula $\alpha_u = \alpha_i\alpha_t + \alpha_j$ that square L_1 resulting from any $GF(p^n)$ will always be the addition table since $\alpha_u = \alpha_i + \alpha_j$ for all i and j values. In order to construct the squares L_2, ... L_{s-1} when $s = p^1$, it is only necessary to use the $u = it + j$ relationship

for finding the values of the first column in each square. If the first entry in each row is known, the remaining entries in that row can be filled in by counting in modular arithmetic mod p.

Using this last method of construction, the two MOLS of order 3 are:

L_1

0	1	2
1	2	0
2	0	1

L_2

0	1	2
2	0	1
1	2	0

The six MOLS of order 7 are:

L_1

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

L_2

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

L_3

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

L_4

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

L_5

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

L_6

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

Making use of the equation $\alpha_u = \alpha_i\alpha_t + \alpha_j$, the three MOLS of order 4 are given below with the equation of each square given at the top

L_1

$\alpha_u = \alpha_i\alpha_1 + \alpha_j$

0	1	2	3
1	0	2	3
2	3	0	1
3	2	1	0

L_2

$\alpha_u = \alpha_i\alpha_2 + \alpha_j$

0	1	2	3
2	3	0	1
3	2	1	0
1	0	3	2

L_3

$\alpha_u = \alpha_i\alpha_3 + \alpha_j$

0	1	2	3
3	2	1	0
1	0	3	2
2	3	0	1

In this example, notice that L_1 is the addition table for $GF(2^2)$ if we replace α_0 by 0, α_1 by 1, α_2 by 2, and α_3 by 3. Notice also that if we fix the first row in each Latin square, the second square can be formed from the first Latin square by putting the second row of the first square as the last row of the second square and moving all but the first row, up one row. If we use this same type of cyclic permutation on the second row, i.e. fix the first row of the second square, drop the second row to

the last row and move all other rows up one row, then the third Latin square is formed.

This cyclic permutation is true in general for MOLS obtained by $\alpha_u = \alpha_i\alpha_t + \alpha_j$ if $s = p^n$ where $n < 1$ and $\alpha_0 = 0$, $\alpha_1 = 1$, $\alpha_2 = 2$, ..., $\alpha_i = x^{i-1}$, ..., $\alpha_{s-1} = x^{s-2}$. To prove this, let the element in the cell (i,j) of L_t be the number u given by

$$(2.4.2) \qquad \alpha_u = \alpha_i\alpha_t + \alpha_j, \quad 0 \le u \le s-1; \quad 1 \le t \le s-2, \quad 2 \le i \le s-1.$$

The element in the cell (i-1,j) of L_{t+1} is the number u' given by

$$\alpha_{u'} = \alpha_{i-1}\alpha_{t+1} + \alpha_j, \quad 0 \le u' \le s-1; \; 1 \le t \le s-2, \quad 2 \le i \le s-1.$$

Then

$$\begin{aligned} \alpha_u &= \alpha_i\alpha_t + \alpha_j \\ &= x^{i-1}x^{t-1} + \alpha_j \qquad \text{since } \alpha_i = x^{i-1} \\ &= x^{i-2}x^{t} + \alpha_j \\ &= \alpha_{i-1}\alpha_{t+1} + \alpha_j \qquad \text{since } \alpha_i = x^{i-1} \\ &= \alpha_{u'}; \end{aligned}$$

or $u = u'$. So the cell $(i-1,j)$ of L_{t+1} contains the same number as the cell (i,j) of L_t. Again, the element in the cell (1,j) of L_t is the number v given by

$$\alpha_v = \alpha_1\alpha_t + \alpha_j = x^{t-1} + \alpha_j;$$

and the number in the cell (s-1,j) of L_{t+1}, $1 \leq t \leq s-2$, is the number v' given by

$$\alpha_{v'} = \alpha_{s-1}\alpha_{t+1} + \alpha_j = x^{s+t-2} + \alpha_j$$

$$= x^{t-1}x^{s-1} + \alpha_j$$

$$= x^{t-1} + \alpha_j \quad \text{since } x^{s-1} = 1.$$

Hence the cell (s-1,j) of L_{t+1} contains the same number as the cell (1,j) of L_t. Our conclusion is that for $1 \leq t \leq s-2$, the rows 1, 2, ..., s-1 of L_t are identical with the rows s-1, 1, ..., s-2 of L_{t+1}, the first or so-called zero-th row being fixed in both squares. Also notice that square L_1 is always the addition table for $GF(p^n)$.

For construction of the 7 MOLS of order 8 it is sufficient to display L_1 or the addition table for $GF(2^3)$. The rows of L_2 can be obtained by keeping the row 0 unchanged and applying a cyclic permutation to the rows 1, 2, ..., 7 of the previous square L_1. In the same fashion, the successive squares L_3, L_4, ..., L_7 can be determined. The first Latin square L_1 is given below

L_1

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

The first Latin square L_1 of the 8 MOLS of order 9 is

0	1	2	3	4	5	6	7	8
1	5	8	4	6	0	3	2	7
2	8	6	1	5	7	0	4	3
3	4	1	7	2	6	8	0	5
4	6	5	2	8	3	7	1	0
5	0	7	6	3	1	4	8	2
6	3	0	8	7	4	2	5	1
7	2	4	0	1	8	5	3	6
8	7	3	5	0	2	1	6	4

The other squares can be obtained from L_1 as described before.

3. PROJECTIVE GEOMETRY, AFFINE GEOMETRY, AND THE EXISTENCE OF COMPLETE SETS OF MOLS

In the previous chapter construction of complete sets of MOLS of order s where s is a prime or a prime power was accomplihsed by using Galois Fields. These same designs can also be constructed by using projective geometries or affine geometries. Partially for the sake of completeness in the study of construction techniques, we will study these additional methods of arriving at the designs previously covered. By doing so, we will gain an important corollary about the existence or nonexistence of complete sets of MOLS of order s where s is a prime or a prime power.

3.1 Projective Geometry

Bruck and Ryser [6] state that a projective plane geometry Π is a mathematical system composed of undefined elements called points and undefined sets of point called lines, subject to the following three postulates:

(1) Two distinct points are contained in a unique line.

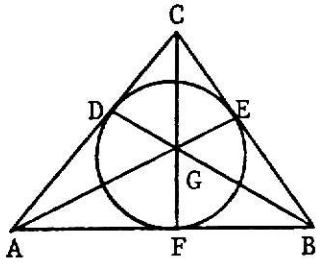
(2) Two distinct lines contain a unique common point.

(3) Each line contains at least three points.

The projective plane Π if finite if it consists of a finite number of points. If Π is finite, then there exists a positive integer $s \geq 2$ such that each line of Π contains exactly s+1 distinct points, and each point is contained in exactly s+1 distinct lines. Moreover, the finite

projective plane is said to be of order s and has exactly $s^2 + s + 1$ distinct points and $s^2 + s + 1$ distinct lines. Some authors say that a line is incident with two points and one point is incident with each of two lines, rather than saying that a line contains two points and each of two lines intersect at one point. It will sometimes be convenient to use the term incident or incidence relation and the reader may substitute the words contains or intersects whichever is appropriate.

The simplest finite plane is that with s = 2. In this system there are 3 lines through each point, 3 points on each line, 7 points, and 7 lines in the plane. It is illustrated below



The points are A, B, C, D, E, F, and G and the lines are ADC, AGE, AFB, CGF, CEB, DGB, and DEF. The last three points are not connected by a straight line, but straightness is not a meaningful concept in a finite plane; a line is only defined as a subset of points.

The finite projective geometry $PG(m,p^n)$ consists of the points $(x_o, x_1, \ldots, x_m)$ wherw $x_0, x_1, \ldots, x_m$ are elements of $GF(p^n)$ and are not all simultaneously zero. It is understood that the point $(y_0, y_1, \ldots, y_m)$ is the same as $(x_0, x_1, \ldots, x_m)$ if and only if there exists a nonzero element θ of $GF(p^n)$ such that $y_i = \theta x_i$ for i = 0, 1, ..., m. Of interest to us is the special case where m = 2 which is a finite projective plane $PG(2,p^n)$. The figure displayed above is an illustration of PG(2,2).

In $PG(2,p^n)$ an ordered triplet (x,y,z) where $x, y, z \in GF(p^n)$ and not all x, y, z being zero defines a point. To avoid using more than one name for a given point since any scalar multiple of a point is just another name, a standard form should be adopted. The coordinates of a point can be taken in a standard form by adopting the convention that the last non-zero coordinate is unity. There are $s^2 + s + 1$ distinct points in $PG(2,p^n)$ where $s = p^n$ is the number of elements in $GF(p^n)$. The s^2 number of points are of the form $(x,y,1)$ where x and y are any of the s field elements of $GF(p^n)$. All points of the form $(x,1,0)$ where x is any field element comprise the next s points. Finally, the point $(1,0,0)$ belongs to every $PG(2,p^n)$ since any point $(x,0,0)$ where x is a non-zero field element is another labeling for $(1,0,0)$.

A linear homogeneous equation $ax + by + cz = 0$, where a, b, c (not all zero) belong to the field, defines a line. The equations $a_1x + b_1y + c_1z = 0$ and $a_2x + b_2y + c_2z = 0$ define the same line if and only if there exists a non-zero element θ of the field such that

$$(3.1.1) \qquad a_2 = \theta a_1, \quad b_2 = \theta b_1, \quad \text{and} \quad c_2 = \theta c_1.$$

The point (x_0,y_0,z_0) is said to be <u>incident</u> with the line $ax + by + cz = 0$ if and only if the relation

$$(3.1.2) \qquad ax_0 + by_0 + cz_0 = 0$$

holds.

As an example, let us look at $PG(2,2^2)$. This finite projective plane has $s = 2^2$, $s^2 + s + 1 = 21$ points and 21 lines, each line being incident with $s + 1 = 5$ points and each point being incident with 5 lines. The ele-

ments of $GF(2^2)$ have been taken as linear polynomials in t (rather than in x) but otherwise follow the same rules of composition as before. The four elements are

$$\alpha_0 = 0, \quad \alpha_1 = 1, \quad \alpha_2 = t, \quad \alpha_3 = t^2 = t + 1.$$

Another useful relation is $t^3 = 1$.

The following table gives the equations of the 21 lines and the coordinates incident with them. A possible convention for the standard form of a line is requiring that the first non-zero coefficient is one. The benefit of such a convention is an aid in a systematic and exhaustive search for all possible distinct lines.

Table 3.1

Points and Lines of $PG(2,2^2)$

Equation of Line	Coordinates of Incident Points				
$x = 0$	$(0,0,1)$	$(0,1,1)$	$(0,t,1)$	$(0,t^2,1)$	$(0,1,0)$
$x + z = 0$	$(1,0,1)$	$(1,1,1)$	$(1,t,1)$	$(1,t^2,1)$	$(0,1,0)$
$x + tz = 0$	$(t,0,1)$	$(t,1,1)$	$(t,t,1)$	$(t,t^2,1)$	$(0,1,0)$
$x + t^2z = 0$	$(t^2,0,1)$	$(t^2,1,1)$	$(t^2,t,1)$	$(t^2,t^2,1)$	$(0,1,0)$
$y = 0$	$(0,0,1)$	$(1,0,1)$	$(t,0,1)$	$(t^2,0,1)$	$(1,0,0)$
$y + z = 0$	$(0,1,1)$	$(1,1,1)$	$(t,1,1)$	$(t^2,1,1)$	$(1,0,0)$
$y + tz = 0$	$(0,t,1)$	$(1,t,1)$	$(t,t,1)$	$(t^2,t,1)$	$(1,0,0)$
$y + t^2z = 0$	$(0,t^2,1)$	$(1,t^2,1)$	$(t,t^2,1)$	$(t^2,t^2,1)$	$(1,0,0)$
$x + y = 0$	$(0,0,1)$	$(1,1,1)$	$(t,t,1)$	$(t^2,t^2,1)$	$(1,1,0)$
$x + y + z = 0$	$(0,1,1)$	$(1,0,1)$	$(t,t^2,1)$	$(t^2,t,1)$	$(1,1,0)$
$x + y + tz = 0$	$(0,t,1)$	$(1,t^2,1)$	$(t,0,1)$	$(t^2,1,1)$	$(1,1,0)$
$x + y + t^2z = 0$	$(0,t^2,1)$	$(1,t,1)$	$(t,1,1)$	$(t^2,0,1)$	$(1,1,0)$
$x + ty = 0$	$(0,0,1)$	$(1,t^2,1)$	$(t,1,1)$	$(t^2,t,1)$	$(t,1,0)$
$x + ty + z = 0$	$(0,t^2,1)$	$(1,0,1)$	$(t,t,1)$	$(t^2,1,1)$	$(t,1,0)$
$x + ty + tz = 0$	$(0,1,1)$	$(1,t,1)$	$(t,0,1)$	$(t^2,t^2,1)$	$(t,1,0)$
$x + ty + t^2z = 0$	$(0,t,1)$	$(1,1,1)$	$(t,t^2,1)$	$(t^2,0,1)$	$(t,1,0)$
$x + t^2y = 0$	$(0,0,1)$	$(1,t,1)$	$(t,t^2,1)$	$(t^2,1,1)$	$(t^2,1,0)$
$x + t^2y + z = 0$	$(0,t,1)$	$(1,0,1)$	$(t,1,1)$	$(t^2,t^2,1)$	$(t^2,1,0)$
$x + t^2y + tz = 0$	$(0,t^2,1)$	$(1,1,1)$	$(t,0,1)$	$(t^2,t,1)$	$(t^2,1,0)$
$x + t^2y + t^2z = 0$	$(0,1,1)$	$(1,t^2,1)$	$(t,t,1)$	$(t^2,0,1)$	$(t^2,1,0)$
$z = 0$	$(0,1,0)$	$(1,0,0)$	$(1,1,0)$	$(t,1,0)$	$(t^2,1,0)$

The 16 of the 21 points in $PG(2,2^2)$, using standard form are

$(0,0,1)$	$(0,1,1)$	$(0,t,1)$	$(0,t^2,1)$
$(1,0,1)$	$(1,1,1)$	$(1,t,1)$	$(1,t^2,1)$
$(t,0,1)$	$(t,1,1)$	$(t,t,1)$	$(t,t^2,1)$
$(t^2,0,1)$	$(t^2,1,1)$	$(t^2,t,1)$	$(t^2,t^2,1)$

for all points of the form $(x,y,1)$ where x and $y \in GF(2^2)$. The next 4 points are $(0,1,0)$, $(1,1,0)$, $(t,1,0)$, and $(t^2,1,0)$ where all points are of the form $(x,1,0)$, $x \in GF(2^2)$. The last point is $(1,0,0)$. Those points incident with line $y = 0$ can easily be found by inspection - just choose all those points out of the 21 standard points which have 0 for the second coordinate. There are $(0,0,1)$, $(1,0,1)$, $(t,0,1)$, $(t^2,0,1)$, and $(1,0,0)$.

For a more difficult line examine $x + t^2y + tz = 0$. Since all solution points can be of standard form, then it must be that the second coordinate is 1 and the last coordinate is 0, or the last coordinate is 1 and the first coordinate can be 0, 1, t, or t^2. In the first case put $y = 1$ and $z = 0$ in the equation $x + t^2y + tz = 0$ and it changes to $x + t^2 = 0$. Checking the addition table given below it is evident that $x = t^2$. Thus the point $(t^2,1,0)$ is incident with this line. In the second case $z = 1$ and suppose we let $x = 0$, then $x + t^2y + tz = 0$ becomes $t^2y + t = 0$ which is $t^2y = t$ if we add to to both sides of the equation (see addition table) and examining the multiplication table it can be seen the $y = t^2$ in order for $t^2y = t$. Hence the point $(0,t^2,1)$ is incident with the line $x + t^2y + tz = 0$. The remaining points for this line can be found by continuing in a similar manner by changing x from 0 to 1, t, and t^2 and finding y. This type of systematic search can be used to determine all points incident to a given line.

Addition and Multiplication Tables for $GF(2^2)$

(Primitive mark t is such that $t^2 = t + 1$)

+	0	1	t	t+1
0	0	1	t	t+1
1	1	0	t+1	t
t	t	t+1	0	1
t+1	t+1	t	1	0

·	0	1	t	t^2
0	0	0	0	0
1	0	1	t	t^2
t	0	t	t^2	1
t^2	0	t^2	1	t

The spaces, or geometries, so far considered have been called projective because of their analogy to continuous projective geometry. An analogue of a continuous Euclidean plane can be constructed by omitting, from a finite projective plane, one line and all the points on it. There will then be s^2 points and $s^2 + s$ points left, with a line through any pair of points, and s points on every line. The Euclidean plane derived from PG(2,s) in this way is denoted EG(2,s) and is called a finite affine plane or Euclidean geometry. Geometries of this type are our next topic.

3.2 Finite Affine Planes

Next let us consider a class of objects called points, a class of objects called lines, and a relation incidence such that a point and a line may or may not be incident. Two lines will be defined to be parallel if there is no point with which both are incident. This set of points and lines is then said to form a finite affine plane if the following axioms are satisfied:

(1) There is exactly one line which is incident with each of two distinct points.

(2) Given a point P not incident with the line m there is just one line incident with P and parallel to m.

(3) There exists at least three points not incident with the same line.

(4) There is at least one line, and the number of points incident with this line is finite.

Affine planes are called Euclidean planes by some authors.

The property of parallelism mentioned above is transitive. That is, if l_1, l_2, l_3 are distinct lines such that l_1 and l_2 are parallel and l_2 and l_3 are parallel then l_1 and l_3 are parallel. To prove this, suppose that lines l_1 and l_3 are not parallel and so are incident with at least one point P. Since l_1 and l_2 are parallel, P is not incident with l_2. Axiom (2) is contradicted since there are two distinct lines incident with P and parallel to l_2.

This transitivity property allows the set of lines to be divided into subsets called <u>parallel pencils</u>, such that any two distinct lines belonging to the same parallel pencil are parallel, whereas any two lines belonging to different parallel pencils are non-parallel and have a point of intersection. There is exactly one line in any given parallel pencil which is incident with a given point P.

The affine plane based on the Galois Field $GF(p^n)$ is denoted by $EG(2,p^n)$ and consists of the points (x,y) where x and y are elements of $GF(p^n)$. If $s = p^n \geq 2$ then the number of points (x,y) is s^2 since each of x and y can take s values indepently; the number s is defined to be the order of the plane. It can be shown that each line is incident with exactly s points

and each point is incident with exactly s + 1 lines. The total number of lines is $s^2 + s$ which can be divided into s + 1 parallel pencils, each consisting of s mutually parallel lines.

Any equation ax + by + c = 0 where a, b, c belong to the field $GF(p^n)$ and $(a,b) \neq (0,0)$ defines a line. The equations

$$(3.2.1) \qquad a_1x + b_1y + c_1 = 0 \quad \text{and} \quad a_2x + b_2y + c_2 = 0$$

define the same line if and only if there exists a non-zero element θ of the field $GF(p^n)$ such that

$$(3.2.2) \qquad a_2 = \theta a_1, \quad b_2 = \theta b_1, \quad c_2 = \theta c_1.$$

The point (x_0,y_0) is defined to be incident with the line ax + by + c = 0 if and only if

$$(3.2.3) \qquad ax_0 + by_0 + c = 0.$$

The lines

$$(3.2.4) \qquad a_1x + b_1y + c_1 = 0, \quad a_2x + b_2y + c_2 = 0$$

are defined to be parallel if there exists a non-zero element θ of the field such that

$$(3.2.5) \qquad a_2 = \theta a_1, \quad b_2 = \theta b_1, \quad c_2 \neq \theta c_1.$$

To divide the lines into parallel pencils and in order to systematically enumerate all lines, it is convenient to express the equation of each line in a standard form. The standard form is obtained by considering equations of the form

$$y + \delta = 0$$

which constitutes one pencil where δ takes on the s different values in $GF(p^n)$ and equations of the form

$$x + \beta y + \gamma = 0$$

In this last equation for each fixed β, a parellel pencil of s lines is constructed as γ takes on the s different values belonging to the field. For the different values of β, we get s parallel pencils and hence altogether s + 1 parellel pencils, each containing s lines.

For a concrete example we look at $EG(2,2^2)$. This finite affine plane has $s = 2^2$, $s^2 = 16$ points, $s^2 + s = 20$ lines, each line being incident with s = 4 points, and each point being incident with s + 1 = 5 lines. The following table gives the equations of the 20 lines and the coordinates of the points incident with them. Lines belonging to the same parallel pencil appear in the same group. The elements of $GF(2^2)$ have been taken as linear polynomials in t (rather than in x) as in Table 3.1

Table 3.2

Points and Lines of $EG(2,2^2)$

Pencil	Equation of Line		Coordinates of Incident Points			
(X)	$x = 0$	line 0	$(0,0)$	$(0,1)$	$(0,t)$	$(0,t^2)$
	$x + 1 = 0$	line 1	$(1,0)$	$(1,1)$	$(1,t)$	$(1,t^2)$
	$x + t = 0$	line 2	$(t,0)$	$(t,1)$	(t,t)	(t,t^2)
	$x + t^2 = 0$	line 3	$(t^2,0)$	$(t^2,1)$	(t^2,t)	(t^2,t^2)
(Y)	$y = 0$	line 0	$(0,0)$	$(1,0)$	$(t,0)$	$(t^2,0)$
	$y + 1 = 0$	line 1	$(0,1)$	$(1,1)$	$(t,1)$	$(t^2,1)$
	$y + t = 0$	line 2	$(0,t)$	$(1,t)$	(t,t)	(t^2,t)
	$y + t^2 = 0$	line 3	$(0,t^2)$	$(1,t^2)$	(t,t^2)	(t^2,t^2)
(V_1)	$x + y = 0$	line 0	$(0,0)$	$(1,1)$	(t,t)	(t^2,t^2)
	$x + y + 1 = 0$	line 1	$(0,1)$	$(1,0)$	(t,t^2)	(t^2,t)
	$x + Y + t = 0$	line 2	$(0,t)$	$(1,t^2)$	$(t,0)$	$(t^2,1)$
	$x + y + t^2 = 0$	line 3	$(0,t^2)$	$(1,t)$	$(t,1)$	$(t^2,0)$
(V_2)	$x + ty = 0$	line 0	$(0,0)$	$(1,t^2)$	$(t,1)$	(t^2,t)
	$x + ty + 1 = 0$	line 1	$(0,t^2)$	$(1,0)$	(t,t)	$(t^2,1)$
	$x + ty + t = 0$	line 2	$(0,1)$	$(1,t)$	$(t,0)$	(t^2,t^2)
	$x + ty + t^2 = 0$	line 3	$(0,t)$	$(1,1)$	(t,t^2)	$(t^2,0)$
(V_3)	$x + t^2y = 0$	line 0	$(0,0)$	$(1,t)$	(t,t^2)	$(t^2,1)$
	$x + t^2y + 1 = 0$	line 1	$(0,t)$	$(1,0)$	$(t,1)$	(t^2,t^2)
	$x + t^2y + t = 0$	line 2	$(0,t^2)$	$(1,1)$	$(t,0)$	(t^2,t)
	$x + t^2y + t^2 = 0$	line 3	$(0,1)$	$(1,t^2)$	(t,t)	$(t^2,0)$

The 16 points in $EG(2,2^2)$ are

$(0,0)$	$(0,1)$	$(0,t)$	$(0,t^2)$
$(1,0)$	$(1,1)$	$(1,t)$	$(1,t^2)$
$(t,0)$	$(t,1)$	(t,t)	(t,t^2)
$(t^2,0)$	$(t^2,1)$	(t^2,t)	(t^2,t^2)

Those points incident with $y + t^2 = 0$ can be found by adding t^2 to both sides of the equation and noticing that the resulting equation $y = t^2$ implies that we take all points with second coordinate being t^2. These points are $(0,t^2)$, $(1,t^2)$, (t,t^2), and (t^2,t^2).

To find those points incident with line $x + t^2y + t = 0$, let $x = 0, 1, t, t^2$ and solve to find y. For example, if $x = t$, then $x + t^2y + t = 0$ becomes $t + t^2y + t = t^2y = 0$ since $t + t = 0$. Examination of the multiplication table for $GF(2^2)$ shows that $t^2y = 0$ if $y = 0$. Hence the point $(t,0)$ is incident with the line $x + t^2y + t = 0$. The procedure of letting x be all the elements of $GF(2^2)$ and solving the particular linear equation to find corresponding y values can be used to locate all points incident with a given line.

3.3 The Correspondence Between $PG(2,p^n)$ and $EG(2,p^n)$

The finite affine plane can be extended to a finite projective plane in the following manner. To each pencil of parallel lines, assign a new point incident with each line of the pencil and call it the vertex of the pencil. These new points are called points at inifinity and the line which is incident with all the points at infinity and with no others is called the line at infinity. The original points and lines of the affine plane are often called finite points and finite lines to distinguish them from the points at infinity and the line at infinity. It can be shown that the

extended plane so obtained satisfies the axioms of a finite projective plane.

Conversely, it can be proved that if we start from a finite projective plane, we can obtain from it a finite affine plane by deleting one line and all the points on it.

The correspondence between points and lines of $EG(2,p^n)$ and $PG(2,p^n)$ can be carried out analytically and is shown in the following table from Bose[3].

Table 3.3

	$EG(2,p^n)$	$PG(2,p^n)$
1.	Point (x,y)	Point $(x,y,1) = (\theta x,\theta y,\theta)$, $\theta \neq 0$
	———	Point $(x,y,0) = (\theta x,\theta y,0)$, $\theta \neq 0$
2.	Line $ax + by + c = 0$ $(a,b) \neq (0,0)$	Line $ax + by + cz = 0$
	———	Line $z = 0$

Thus the point (x,y) of $EG(2,p^n)$ can be identified with the point $(x,y,1)$ or $(\theta x,\theta y,\theta)$ of $PG(2,p^n)$, $\theta \neq 0$. Conversely, if (x_1,y_1,z_1) is any point of $PG(2,p^n)$ such that $z_1 \neq 0$, then set $x_1 = \theta x$, $y_1 = \theta y$, $z_1 = \theta$ so that it corresponds to the point $(\frac{x_1}{z_1},\frac{y_1}{z_1})$ of $EG(2,p^n)$. Thus there is a one-to-one correspondence between points of $EG(2,p^n)$ and those of $PG(2,p^n)$ for which the last coordinate is different from zero.

Likewise the line $ax + by + c = 0$ of $EG(2,p^n)$ can be made to correspond to the line $ax + by + cz = 0$ of $PG(2,p^n)$, $(a,b) \neq (0,0)$. There is only one line in $PG(2,p^n)$, namely $z = 0$, for which the coefficients of x and y simultaneously vanish. Thus there is a one-to-one correspondence between line of

$EG(2,p^n)$ and lines of $PG(2,p^n)$ other than $z = 0$. If (x_0,y_0) is incident with $ax + by + c$ in $EG(2,p^n)$, then the corresponding point $(x_0,y_0,1)$ is incident with the corresponding line $ax + by + cz = 0$ in $PG(2,p^n)$. Thus the relation of incidence is invariant with respect to the correspondence considered.

If we now identify the corresponding points and lines of $EG(2,p^n)$ and $PG(2,p^n)$, then $EG(2,p^n)$ may be considered as embedded in $PG(2,p^n)$. The additional points of $PG(2,p^n)$ are the $p^n + 1$ points incident with $z = 0$ which may be considered as the line at infinity. If the lines $a_1x + b_1y + c_1 = 0$ and $a_2x + b_2y + c_2 = 0$ of $EG(2,p^n)$ are parallel, then there is no point of $EG(2,p^n)$ with which they are both incident so that $a_2 = \theta a_1$, $b_2 = \theta b_1$, $\theta \neq 0$. However, the lines $a_1x + b_1y + c_1z = 0$ and $a_2x + b_2y + c_2z = 0$ of the extended plane are incident with the common point $(-b_1,a_1,0) = (-b_2,a_2,0)$ which lies on the line at infinity $z = 0$.

Comparing Table 3.1 giving the points and lines of $PG(2,2^2)$ with the Table 3.2 giving the points and lines of $EG(2,2^2)$, the first twenty lines of $PG(2,2^2)$ correspond to the lines of $EG(2,2^2)$. Thus, for example the line $x + ty + z = 0$ of $PG(2,2^2)$ corresponds to the line $x + ty + 1 = 0$ of $EG(2,2^2)$. The first four points on any of these lines correspond to the four points of the corresponding line. Thus the first four points of $x + ty + z = 0$ are $(0,t^2,1)$, $(1,0,1)$, $(t,t,1)$, $(t^2,1,1)$. They correspond to the points $(0,t^2)$, $(1,0)$, (t,t), and $(t^2,1)$ of the line $x + ty + 1 = 0$. The twenty first line $z = 0$ of $PG(2,2^2)$ which does not correspond to any line of $EG(2,2^2)$ is the line at infinity. The fifth point on each of the first twenty lines of $PG(2,2^2)$ has a zero z-coordinate and is a point at infinity which does not correspond to any point of $EG(2,2^2)$. Notice that

the lines in $PG(2,2^2)$ which correspond to the lines of the same parallel pencil in $EG(2,2^2)$ have the same point at infinity. For example, the lines $x + ty = 0$, $x + ty + 1 = 0$, $x + ty + t = 0$, and $x + ty + t^2 = 0$ of $EG(2,2^2)$ constitute a parallel pencil. The corresponding lines $x + ty = 0$, $x + ty + z = 0$, $x + ty + tz = 0$, and $x + ty + t^2z = 0$ of $PG(2,2^2)$ have the common point at infinity $(t,1,0)$.

3.4 Equivalence of $EG(2,p^n)$ and Complete Sets of MOLS

Given $EG(2,p^n)$ we can construct the $p^n - 1$ MOLS of order p^n. For example, consider $EG(2,2^2)$ and let the 5 parallel pencils be denoted (X), (Y), (V_1), (V_2), (V_3). For each pencil, assign the numbers 0, 1, 2, 3 to the 4 lines. Any point of $EG(2.2^2)$ is uniquely determined as the intersection of a line of the pencil (X), say the i-th line, and a line of the pencil (Y), say the j-th line. It is possible to establish a one-to-one correspondence between any point P belonging to $EG(2,2^2)$ and the cells of a 4×4 square, the point of intersection of the i-th line of (X) and the j-th line of (Y) corresponding to the cell (i,j) where $i,j = 0, 1, 2, 3$. Through the point P, there passes a unique line of the pencil (V_t). Put the number of this line in the cell (i,j) of a 4×4 square; when this is done for each cell, the result is a Latin square L_t. This is seen to be so since the cells of the row i correspond to points on the i-th line of pencil (X). If two cells (i,j_1), (i,j_2); $j_1 \neq j_2$ contain the same number u, this would mean that the u-th line of the pencil (V_t) intersects the i-th line at the pencil (X) in two points which is a contradiction since two distinct nonparallel lines are incident with just one point. Thus the cells

of the i-th row contain all the numbers 0, 1, 2, 3 exactly once. In the same way, we can show the corresponding property for the columns. From the pencils (V_1), (V_2), and (V_3) the 3 Latin squares L_1, L_2, and L_3 can be obtained.

To show that any two of these squares are orthogonal, we must show that when the square L_t is superimposed on the square L_w, there is a unique cell which will contain the number u of L_t and the number u' of L_w. This is in fact the cell which corresponds to the point of intersection of the u-th line of (V_t) and the u'-th line of (V_w). In the above construction and argument, if 3, 4, and 5 are replaced by s - 1, $s = p^n$, and s + 1 respectively, then we have demonstrated that starting from a finite affine plane of order s, we can construct a complete set of MOLS of order s. The MOLS of order 4 obtained by using this method on the pencils and lines of Table 3.2 are the transpositions of the MOLS obtained by using Galois Fields in section 2.4.

Conversely, given a set of s - 1 mutually orthogonal Latin squares of order s, we can construct EG(2,s). Suppose the Latin squares are superimposed on one another and the symbols occupying the cells are taken to be 0, 1, 2, ..., s - 1. Then each cell contains exactly one symbol from each of the s - 1 Latin squares. The s^2 cells (i,j) where i,j = 0, 1, 2, ..., s - 1 may be made to correspond to s^2 points. A set of s cells, the members of which lie in the same row, same column, or are occupied by the same symbol of one of the Latin squares L_t, is made to correspond with a line. The s lines corresponding to the rows form then pencil (X); the s lines corresponding to the columns form the pencil (Y); and the s lines, one correspon-

ding to each of the different symbols of L_t will be taken to form the pencil (V_t); t = 1, 2, ..., s - 1. Thus we have $s^2 + s$ lines divided into s + 1 pencils.

To see where a certain line comes from for $EG(2,2^2)$, we examine L_1 and choose those cells which are all occupied by 1.

L_1

	0	1	t	t^2
0	0	[1]	2	3
1	[1]	2	3	0
t	2	3	0	[1]
t^2	3	0	[1]	2

The coordinates for these cells using elements from $GF(2^2)$ are (0,1), (1,0), (t,t^2), and (t^2,t). Looking at Table 3.2, it can be seen that in pencil (V_1) these are the points incident to line 1.

With the type of correspondence described above, it is possible to show that the axioms for the finite affine plane are satisfied. Since EG(2,n) can be extended to PG(2,n) by adding points at infinity and the line at infinity, it is also possible to to use PG(2,n) to derive MOLS by using the EG(2,n) embedded in it.

3.5 Existence and Nonexistence of Complete Sets of MOLS

Since EG(2,s) is embedded in PG(2,s) and EG(2,s) is equivalent to a complete set of MOLS, then the existence of a complete set of MOLS of order s is equivalent to the existence of PG(2,s).

Due to the results of Bruck and Ryser [6] and Raghavarao [22], the condition for the nonexistence of PG(2,s) is specified in the following

corollary:

Corollary 3.5.1 if $s \equiv 1 \pmod 4$ or $s \equiv 2 \pmod 4$ and the square free part of s contains a prime congruent to 3(mod 4), then there does not exist PG(2,s).

If the number s can be factored as a^2b where b cannot be factored as the square of any integer larger than one, then b is the square free part of s.

From the corollary we can see that PG(2,s) does not exist for s = 6, 14, 21, 22, 33, 38, 42, 46, 54, 57, 66, 69, 70, 74, 77, 78, 86, 93, 94, etc.

The following two theorems given by Raghavarao [22] indicate conditions when it is possible to build up a complete set of MOLS when only part of the set has been formed.

Theorem 3.5.1 Any set of s - 2 MOLS of order s can be extended to a complete set of s - 1 MOLS.

Theorem 3.5.2 If $s \neq 4$, any set of s - 3 MOLS of order s can be uniquely extended to a complete set of s - 1 MOLS.

One method of finding the remaining Latin squares needed to comprise a complete set is to use the corresponding $EG(2,p^n)$ or $PG(2,p^n)$ and locate a parallel pencil which does not have a corresponding Latin square, and then construct that square.

Raghavarao [22] using finite geometries as a means of building orthogonal arrays, balanced incomplete block designs, and in dealing with confounding problems in factorial experiments.

The important thing we gain from finite geometries is the knowledge of conditions determining when a complete set of MOLS does not exist.

4. CONSTRUCTION OF MOLS OF ORDER S WHEN S IS NOT A PRIME OR A PRIME POWER

In Chapter 1 we showed that the maximum number of MOLS of order s is s - 1. For s a prime or a prime power, this maximum number can be achieved using the construction techniques of Chapter 2 and Chapter 3. MOLS can be constructed when s is not a prime or a prime power. In this chapter, we shall look at the problem of constructing MOLS when s can be written as a product of prime powers, i.e.

$$s = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}.$$

Since any value of s can be written in this manner, we are in effect studying the situation where s is not a prime or a prime power.

4.1 The Lower Bound for the Number of MOLS and the MacNeish-Mann Theorem

Let the prime decomposition of a composite number s be $p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ and define

$$n(s) = \min (p_1^{e_1}, p_2^{e_2}, \ldots, p_m^{e_m}) - 1 . \tag{4.1.1}$$

MacNeish [16] and Mann [17] showed that a set of n(s) MOLS of order s can always be constructed. If N(s) denotes the maximum possible number of MOLS of order s, then the MacNeish-Mann theorem states that

$$N(s) \geq n(s) . \tag{4.1.2}$$

By means of the method of construction described below, it is possible to

always construct n(s) MOLS of order s. If 2^1 is the minimum of the prime powers of decomposition of s, then n(s) = 1 and this method provides no orthogonal mates to the original Latin square. MacNeish conjectured that the upper bound of the N(s) is n(s) so that N(s) = n(s). This same conjecture was made by Euler [9] in 1782, and became known as Euler's conjecture. However, Parker [20] used a balanced incomplete block design to show that it was possible to have N(s) > n(s). From results of Bruck [7], an upper bound of N(s) is given by

$$N(s) < (s - 1) - (2s)^{1/4} \tag{4.1.3}$$

whenever N(s) < s - 1, i.e. when s is not a prime or a prime power.

Actual construction by the MacNeish-Mann theorem of n(s) MOLS of orders, where $s = p_1^{e}1, p_2^{e}2, \ldots, p_m^{e}m$ requires us to form the system of s elements

$$\gamma_j = [g_1^{(j)}, g_2^{(j)}, \ldots, g_m^{(j)}] \tag{4.1.4}$$

where 0, $g_i^{(1)} = 1, g_i^{(2)}, \ldots, g_i^{(p_i^{e}i - 1)}$ are the elements of $GF(p_i^{e}i)$ for every i = 1,...., m. Define addition and multiplication in the usual component-wise nature as

$$\gamma_1 + \gamma_2 = (g_1^{(1)}, g_2^{(1)}, \ldots, g_m^{(1)}) + (g_1^{(2)}, g_2^{(2)}, \ldots, g_m^{(2)}) \tag{4.1.5}$$

$$= (g_1^{(1)} + g_1^{(2)}, g_2^{(1)} + g_2^{(2)}, \ldots, g_m^{(1)} + g_m^{(2)}) \tag{4.1.6}$$

and

$$\gamma_1 \gamma_2 = (g_1^{(1)} g_1^{(2)}, g_2^{(1)} g_2^{(2)}, \ldots, g_m^{(1)} g_m^{(2)}) \tag{4.1.7}$$

where the operations in each component are defined as in corresponding Galois Fields. This system does not form a field since (0,1,....,1) does not have a multiplicative inverse, however, all points that have no zero among their coordinates possess inverses.

If γ_j is defined as in (4.1.4) and $0 < j \leq n(s)$, then γ_j's possess inverses, as does $\gamma_j - \gamma_i$ if $i \neq j$. The next step is to number the points γ in such a way that $\gamma_0 = (0,0,....,0)$ and the next n(s) elements are given by (4.1.4) where $0 < j \leq n(s)$. If in each cell (i,j) of an s x s square, where (i,j) is the intersection of row i + 1 and column j + 1 (since rows and columns are numbered from 0 to s - 1), we put the number u determined by

$$(4.1.8) \quad \gamma_u = \gamma_t\gamma_i + \gamma_j \quad t = 1,2,....,n(s) \quad i,j = 0,1,....,s-1 \ ,$$

we get a Latin square L_t. The n(s) Latin squares form a set of mutually orthoganal Latin squares. The pattern of choosing $\gamma_1,...., \gamma_{n(s)}$ as specified earlier is that this allows γ_u to take on all possible values in the system for some fixed t and i with j = 0, 1,...., s - 1 or for some fixed t and j with i = 0, 1,...., s - 1. This property of all elements appearing only once in a given row or column is necessary for the construction of the Latin square design and might not be possible if γ_t were allowed to have no multiplicative inverse. The choice of which elements correspond to $\gamma_{n(s)+1},...., \gamma_{s-1}$ is left to the person constructing the design. While different individuals will make different choices for labeling this last set of elements, this will not alter the orthogonality of the resulting Latin squares and all results will be equivalent up to an isomorphism.

Illustration of this method will now be given in the case where s = 15. Thus n(15) = 2 and $\gamma_0 = (0,0)$, $\gamma_1 = (1,1)$, and $\gamma_2 = (2,2)$. The values for the first coordinate come from GF(3) and the values for the second coordi-

nate come from GF(5). Let the remaining elements be given by $\gamma_3 = (0,1)$, $\gamma_4 = (0,2)$, $\gamma_5 = (0,3)$, $\gamma_6 = (0,4)$, $\gamma_7 = (1,0)$, $\gamma_8 = (1,2)$, $\gamma_9 = (1,3)$, $\gamma_{10} = (1,4)$, $\gamma_{11} = (2,0)$, $\gamma_{12} = (2,1)$, $\gamma_{13} = (2,3)$, and $\gamma_{14} = (2,4)$. The addition and multiplication tables for this system are given in Table 4.1. To find the entry that belongs in cell (2,11) of the addition table we add $\gamma_2 + \gamma_{11} = (2,2) + (2,0) = (1,2) = \gamma_8$. The entry that belongs to cell (5,2) of the multiplication table is $\gamma_5 \cdot \gamma_2 = (0,3) \cdot (2,2) = (0,1) = \gamma_3$.

The resulting Latin squares are found in Table 4.1.2.

Table 4.1.1 Addition and Multiplication Tables for (x,y)

Where x ε GF(3) and y ε GF(5)

+	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8	γ_9	γ_{10}	γ_{11}	γ_{12}	γ_{13}	γ_{14}
γ_0	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8	γ_9	γ_{10}	γ_{11}	γ_{12}	γ_{13}	γ_{14}
γ_1	γ_1	γ_2	γ_5	γ_8	γ_9	γ_{10}	γ_7	γ_{12}	γ_{13}	γ_{14}	γ_{11}	γ_3	γ_4	γ_6	γ_0
γ_2	γ_2	γ_5	γ_{10}	γ_{13}	γ_{14}	γ_{11}	γ_{12}	γ_4	γ_6	γ_0	γ_3	γ_8	γ_9	γ_7	γ_1
γ_3	γ_3	γ_8	γ_{13}	γ_4	γ_5	γ_6	γ_0	γ_1	γ_9	γ_{10}	γ_7	γ_{12}	γ_2	γ_{14}	γ_{11}
γ_4	γ_4	γ_9	γ_{14}	γ_5	γ_6	γ_0	γ_3	γ_8	γ_{10}	γ_7	γ_1	γ_2	γ_{13}	γ_{11}	γ_{12}
γ_5	γ_5	γ_{10}	γ_{11}	γ_6	γ_0	γ_3	γ_4	γ_9	γ_7	γ_1	γ_8	γ_{13}	γ_{14}	γ_{12}	γ_2
γ_6	γ_6	γ_7	γ_{12}	γ_0	γ_3	γ_4	γ_5	γ_{10}	γ_1	γ_8	γ_9	γ_{14}	γ_{11}	γ_2	γ_{13}
γ_7	γ_7	γ_{12}	γ_4	γ_1	γ_8	γ_9	γ_{10}	γ_{11}	γ_2	γ_{13}	γ_{14}	γ_0	γ_3	γ_5	γ_6
γ_8	γ_8	γ_{13}	γ_6	γ_9	γ_{10}	γ_7	γ_1	γ_2	γ_{14}	γ_{11}	γ_{12}	γ_4	γ_5	γ_0	γ_3
γ_9	γ_9	γ_{14}	γ_0	γ_{10}	γ_7	γ_1	γ_8	γ_{13}	γ_{11}	γ_{12}	γ_2	γ_5	γ_6	γ_3	γ_4
γ_{10}	γ_{10}	γ_{11}	γ_3	γ_7	γ_1	γ_8	γ_9	γ_{14}	γ_{12}	γ_2	γ_{13}	γ_6	γ_0	γ_4	γ_5
γ_{11}	γ_{11}	γ_3	γ_8	γ_{12}	γ_2	γ_{13}	γ_{14}	γ_0	γ_4	γ_5	γ_6	γ_7	γ_1	γ_9	γ_{10}
γ_{12}	γ_{12}	γ_4	γ_9	γ_2	γ_{13}	γ_{14}	γ_{11}	γ_3	γ_5	γ_6	γ_0	γ_1	γ_8	γ_{10}	γ_7
γ_{13}	γ_{13}	γ_6	γ_7	γ_{14}	γ_{11}	γ_{12}	γ_2	γ_5	γ_0	γ_3	γ_4	γ_9	γ_{10}	γ_1	γ_8
γ_{14}	γ_{14}	γ_0	γ_1	γ_{11}	γ_{12}	γ_2	γ_{13}	γ_6	γ_3	γ_4	γ_5	γ_{10}	γ_7	γ_8	γ_9

$\cdot$	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8	γ_9	γ_{10}	γ_{11}	γ_{12}	γ_{13}	γ_{14}
γ_0	γ_0	γ_0	γ_0	γ_0	γ_0	γ_0	γ_0	γ_0	γ_0	γ_0	γ_0	γ_0	γ_0	γ_0	γ_0
γ_1	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8	γ_9	γ_{10}	γ_{11}	γ_{12}	γ_{13}	γ_{14}
γ_2	γ_0	γ_2	γ_{10}	γ_4	γ_6	γ_3	γ_5	γ_{11}	γ_{14}	γ_{12}	γ_{13}	γ_7	γ_8	γ_1	γ_9
γ_3	γ_0	γ_3	γ_4	γ_3	γ_4	γ_5	γ_6	γ_0	γ_4	γ_5	γ_6	γ_0	γ_3	γ_5	γ_6
γ_4	γ_0	γ_4	γ_6	γ_4	γ_6	γ_3	γ_5	γ_0	γ_6	γ_3	γ_5	γ_0	γ_4	γ_3	γ_5
γ_5	γ_0	γ_5	γ_3	γ_5	γ_3	γ_6	γ_4	γ_0	γ_3	γ_6	γ_4	γ_0	γ_5	γ_6	γ_4
γ_6	γ_0	γ_6	γ_5	γ_6	γ_5	γ_4	γ_3	γ_0	γ_5	γ_4	γ_3	γ_0	γ_6	γ_4	γ_3
γ_7	γ_0	γ_7	γ_{11}	γ_0	γ_0	γ_0	γ_0	γ_7	γ_7	γ_7	γ_7	γ_{11}	γ_{11}	γ_{11}	γ_{11}
γ_8	γ_0	γ_8	γ_{14}	γ_4	γ_6	γ_3	γ_5	γ_7	γ_{10}	γ_1	γ_9	γ_{11}	γ_2	γ_{12}	γ_{13}
γ_9	γ_0	γ_9	γ_{12}	γ_5	γ_3	γ_6	γ_4	γ_7	γ_1	γ_{10}	γ_8	γ_{11}	γ_{13}	γ_{14}	γ_2
γ_{10}	γ_0	γ_{10}	γ_{13}	γ_6	γ_5	γ_4	γ_3	γ_7	γ_9	γ_8	γ_1	γ_{11}	γ_{14}	γ_2	γ_{12}
γ_{11}	γ_0	γ_{11}	γ_7	γ_0	γ_0	γ_0	γ_0	γ_{11}	γ_{11}	γ_{11}	γ_{11}	γ_7	γ_7	γ_7	γ_7
γ_{12}	γ_0	γ_{12}	γ_8	γ_3	γ_4	γ_5	γ_6	γ_{11}	γ_2	γ_{13}	γ_{14}	γ_7	γ_1	γ_9	γ_{10}
γ_{13}	γ_0	γ_{13}	γ_1	γ_5	γ_3	γ_6	γ_4	γ_{11}	γ_{12}	γ_{14}	γ_2	γ_7	γ_9	γ_{10}	γ_8
γ_{14}	γ_0	γ_{14}	γ_9	γ_6	γ_5	γ_4	γ_3	γ_{11}	γ_{13}	γ_2	γ_{12}	γ_7	γ_{10}	γ_8	γ_1

Table 4.1.2. The 2 MOLS of Order 15 as Obtained by MacNeish-Mann Procedure

L_1

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	5	8	9	10	7	12	13	14	11	3	4	6	0
2	5	10	13	14	11	12	4	6	0	3	8	9	7	1
3	8	13	4	5	6	0	1	9	10	7	12	2	14	11
4	9	14	5	6	0	3	8	10	7	1	2	13	11	12
5	10	11	6	0	3	4	9	7	1	8	13	14	12	2
6	7	12	0	3	4	5	10	1	8	9	14	11	2	13
7	12	4	1	8	9	10	11	2	13	14	0	13	5	6
8	13	6	9	10	7	1	2	14	11	12	4	5	0	3
9	14	0	10	7	1	8	13	11	12	2	5	6	3	4
10	11	3	7	1	8	9	14	12	2	13	6	0	4	5
11	3	8	12	2	13	14	0	4	5	6	7	1	9	10
12	4	9	2	13	14	11	3	5	6	0	1	8	10	7
13	6	7	14	11	12	2	5	0	3	4	9	10	1	8
14	0	1	11	12	2	13	6	3	4	5	10	7	8	9

L_2

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	5	10	13	14	11	12	4	6	0	3	8	9	7	1
10	11	13	7	1	8	9	14	12	2	13	6	0	4	5
4	9	14	5	6	0	3	8	10	7	1	2	13	11	12
6	7	12	0	3	4	5	10	1	8	9	14	11	2	13
3	8	13	4	5	6	0	1	9	10	7	12	2	14	11
5	10	11	6	0	3	4	9	7	1	8	13	14	12	2
11	3	8	12	2	13	14	0	4	5	6	7	1	9	10
14	0	1	11	12	2	13	6	3	4	5	10	7	8	9
12	4	9	2	13	14	11	3	5	6	0	1	8	10	7
13	6	7	14	11	12	2	5	0	3	4	9	10	11	8
7	12	4	1	8	9	10	11	2	13	14	0	3	5	6
8	13	6	9	10	7	1	2	14	11	12	4	5	0	3
1	2	5	8	9	10	7	12	13	14	11	3	4	6	0
9	14	0	10	7	1	8	13	11	12	2	5	6	3	4

Notice that square L_1 is the addition table for our system of ordered pairs. It can be seen by examining the formula $\gamma_u = \gamma_i\gamma_t + \gamma_j$ that L_1 will always be the addition table because $\gamma_u = \gamma_i\gamma_t + \gamma_j = \gamma_i + \gamma_j$ for all i and j values since $\gamma_t = (1,1,\ldots,1)$. In order to construct the Latin squares $L_2,\ldots, L_{n(s)}$ it is only necessary to use the $u = it + j$ relationship for finding the values of the first column in each square. If the first entry in each row is known, the remaining entries in that row are the same as in the row from L_1 with that first entry. In other words to construct the Latin square L_t, $2 \leq t \leq n(s)$, find the row or column in the multiplication table corresponding to γ_t and use the subscripts of these elements to establish the ordering of the symbols 0, 1, ..., s - 1 in the first column of your square. Now permute the rows of square L_1 so that their leading entry corresponds with the ordering of your column and you have formed the Latin square L_t.

Looking back at the addition and multiplication tables of the previous example and then at the Latin squares, one can see the relationship described above.

For another example, take the case where s = 20 and hence n(s) = 3. The first component of the order pair comes from $GF(2^2)$ and is either 0, 1, x, or x + 1. Elements of GF(5) comprise the values of the second component. Let the γ_j be given as

$$\gamma_0 = (0,0) \quad \gamma_1 = (1,1) \quad \gamma_2 = (x,2) \quad \gamma_3 = (x+1,3) \quad \gamma_4 = (0,1)$$

$$\gamma_5 = (0,2) \quad \gamma_6 = (0,3) \quad \gamma_7 = (0,4) \quad \gamma_8 = (1,0) \quad \gamma_9 = (1,2)$$

$\gamma_{10} = (1,3)$ $\gamma_{11} = (1,4)$ $\gamma_{12} = (x,0)$ $\gamma_{13} = (x,1)$ $\gamma_{14} = (x,3)$

$\gamma_{15} = (x,4)$ $\gamma_{16} = (x+1,0)$ $\gamma_{17} = (x+1,1)$ $\gamma_{18} = (x+1,2)$ $\gamma_{19} = (x+1,4)$.

The addition table and necessary portion of the multiplication table are given in Table 4.1.3. Resulting mutually orthogonal Latin Squares are given in table 4.1.4.

Table 4.1.3 Addition Table and Multiplication Relationship for (x,y) Where x ε GF(2^2) and y ε GF(5)

+	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8	γ_9	γ_{10}	γ_{11}	γ_{12}	γ_{13}	γ_{14}	γ_{15}	γ_{16}	γ_{17}	γ_{18}	γ_{19}
γ_0	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8	γ_9	γ_{10}	γ_{11}	γ_{12}	γ_{13}	γ_{14}	γ_{15}	γ_{16}	γ_{17}	γ_{18}	γ_{19}
γ_1	γ_1	γ_5	γ_3	γ_{15}	γ_9	γ_{10}	γ_{11}	γ_8	γ_4	γ_6	γ_7	γ_0	γ_{17}	γ_{18}	γ_{19}	γ_{16}	γ_{13}	γ_2	γ_{14}	γ_{12}
γ_2	γ_2	γ_3	γ_7	γ_8	γ_{14}	γ_{15}	γ_{12}	γ_{13}	γ_{18}	γ_{19}	γ_{16}	γ_{17}	γ_5	γ_6	γ_0	γ_4	γ_9	γ_{10}	γ_{11}	γ_1
γ_3	γ_3	γ_{15}	γ_8	γ_4	γ_{19}	γ_{16}	γ_{17}	γ_{18}	γ_{14}	γ_{12}	γ_{13}	γ_2	γ_{10}	γ_{11}	γ_1	γ_9	γ_6	γ_7	γ_0	γ_5
γ_4	γ_4	γ_9	γ_{14}	γ_{19}	γ_5	γ_6	γ_7	γ_0	γ_1	γ_{10}	γ_{11}	γ_8	γ_{13}	γ_2	γ_{15}	γ_{12}	γ_{17}	γ_{18}	γ_3	γ_{16}
γ_5	γ_5	γ_{10}	γ_{15}	γ_{16}	γ_6	γ_7	γ_0	γ_4	γ_9	γ_{11}	γ_8	γ_1	γ_2	γ_{14}	γ_{12}	γ_{13}	γ_{18}	γ_3	γ_{19}	γ_{17}
γ_6	γ_6	γ_{11}	γ_{12}	γ_{17}	γ_7	γ_0	γ_4	γ_5	γ_{10}	γ_8	γ_1	γ_9	γ_{14}	γ_{15}	γ_{13}	γ_2	γ_3	γ_{19}	γ_{16}	γ_{18}
γ_7	γ_7	γ_8	γ_{13}	γ_{18}	γ_0	γ_4	γ_5	γ_6	γ_{11}	γ_1	γ_9	γ_{10}	γ_{15}	γ_{12}	γ_2	γ_{14}	γ_{19}	γ_{16}	γ_{17}	γ_3
γ_8	γ_8	γ_4	γ_{18}	γ_{14}	γ_1	γ_9	γ_{10}	γ_{11}	γ_0	γ_5	γ_6	γ_7	γ_{16}	γ_{17}	γ_3	γ_{19}	γ_{12}	γ_{13}	γ_2	γ_{15}
γ_9	γ_9	γ_6	γ_{19}	γ_{12}	γ_{10}	γ_{11}	γ_8	γ_1	γ_5	γ_7	γ_0	γ_4	γ_{18}	γ_3	γ_{16}	γ_{17}	γ_2	γ_{14}	γ_{15}	γ_{13}
γ_{10}	γ_{10}	γ_7	γ_{16}	γ_{13}	γ_{11}	γ_8	γ_1	γ_9	γ_6	γ_0	γ_4	γ_5	γ_3	γ_{19}	γ_{17}	γ_{18}	γ_{14}	γ_{15}	γ_{12}	γ_2
γ_{11}	γ_{11}	γ_0	γ_{17}	γ_2	γ_8	γ_1	γ_9	γ_{10}	γ_7	γ_4	γ_5	γ_6	γ_{19}	γ_{16}	γ_{18}	γ_3	γ_{15}	γ_{12}	γ_{13}	γ_{14}
γ_{12}	γ_{12}	γ_{17}	γ_5	γ_{10}	γ_{13}	γ_2	γ_{14}	γ_{15}	γ_{16}	γ_{18}	γ_3	γ_{19}	γ_0	γ_4	γ_6	γ_7	γ_8	γ_1	γ_9	γ_{11}
γ_{13}	γ_{13}	γ_{18}	γ_6	γ_{11}	γ_2	γ_{14}	γ_{15}	γ_{12}	γ_{17}	γ_3	γ_{19}	γ_{16}	γ_4	γ_5	γ_7	γ_0	γ_1	γ_9	γ_{10}	γ_8
γ_{14}	γ_{14}	γ_{19}	γ_0	γ_1	γ_{15}	γ_{12}	γ_{13}	γ_2	γ_3	γ_{16}	γ_{17}	γ_{18}	γ_6	γ_7	γ_4	γ_5	γ_{10}	γ_{11}	γ_8	γ_9
γ_{15}	γ_{15}	γ_{16}	γ_4	γ_9	γ_{12}	γ_{13}	γ_2	γ_{14}	γ_{19}	γ_{17}	γ_{18}	γ_3	γ_7	γ_0	γ_5	γ_6	γ_{11}	γ_8	γ_1	γ_{10}
γ_{16}	γ_{16}	γ_{13}	γ_9	γ_6	γ_{17}	γ_{18}	γ_3	γ_{19}	γ_{12}	γ_2	γ_{14}	γ_{15}	γ_8	γ_1	γ_{10}	γ_{11}	γ_0	γ_4	γ_5	γ_7
γ_{17}	γ_{17}	γ_2	γ_{10}	γ_7	γ_{18}	γ_3	γ_{19}	γ_{16}	γ_{13}	γ_{14}	γ_{15}	γ_{12}	γ_1	γ_9	γ_{11}	γ_8	γ_4	γ_5	γ_6	γ_0
γ_{18}	γ_{18}	γ_{14}	γ_{11}	γ_0	γ_3	γ_{19}	γ_{16}	γ_{17}	γ_2	γ_{15}	γ_{12}	γ_{13}	γ_9	γ_{10}	γ_8	γ_1	γ_5	γ_6	γ_7	γ_4
γ_{19}	γ_{19}	γ_{12}	γ_1	γ_5	γ_{16}	γ_{17}	γ_{18}	γ_3	γ_{15}	γ_{13}	γ_2	γ_{14}	γ_{11}	γ_8	γ_9	γ_{10}	γ_7	γ_0	γ_4	γ_6

$\cdot$	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8	γ_9	γ_{10}	γ_{11}	γ_{12}	γ_{13}	γ_{14}	γ_{15}	γ_{16}	γ_{17}	γ_{18}	γ_{19}
γ_1	γ_0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8	γ_9	γ_{10}	γ_{11}	γ_{12}	γ_{13}	γ_{14}	γ_{15}	γ_{16}	γ_{17}	γ_{18}	γ_{19}
γ_2	γ_0	γ_2	γ_{19}	γ_1	γ_5	γ_7	γ_4	γ_6	γ_{12}	γ_{15}	γ_{13}	γ_{14}	γ_{16}	γ_{18}	γ_{17}	γ_3	γ_8	γ_9	γ_{11}	γ_{10}
γ_3	γ_0	γ_3	γ_1	γ_{15}	γ_6	γ_4	γ_7	γ_5	γ_{16}	γ_{17}	γ_{19}	γ_{18}	γ_8	γ_{10}	γ_{11}	γ_9	γ_{12}	γ_{14}	γ_{13}	γ_2

Table 4.1.4. The 3 MOLS of Order 20 as Obtained

By MacNeish-Mann Procedure

L_1

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	5	3	15	9	10	11	8	4	6	7	0	17	18	19	16	13	2	14	12
2	3	7	8	14	15	12	13	18	19	16	17	5	6	0	4	9	10	11	1
3	15	8	4	19	16	17	18	14	12	13	2	10	11	1	9	6	7	0	5
4	9	14	19	5	6	7	0	1	10	11	8	13	2	15	12	17	18	3	16
5	10	15	16	6	7	0	4	9	11	8	1	2	14	12	13	18	3	19	17
6	11	12	17	7	0	4	5	10	8	1	9	14	15	13	2	3	19	16	18
7	8	13	18	0	4	5	6	11	1	9	10	15	12	2	14	19	16	17	3
8	4	18	14	1	9	10	11	0	5	6	7	16	17	3	19	12	13	2	15
9	6	19	12	10	11	8	1	5	7	0	4	18	3	16	17	2	14	15	13
10	7	16	13	11	8	1	9	6	0	4	5	3	19	17	18	14	15	12	2
11	0	17	2	8	1	9	10	7	4	5	6	19	16	18	3	15	12	13	14
12	17	5	10	13	2	14	15	16	18	3	19	0	4	6	7	8	1	9	11
13	18	6	11	2	14	15	12	17	3	19	16	4	5	7	0	1	9	10	8
14	19	0	1	15	12	13	2	3	16	17	18	6	7	4	5	10	11	8	9
15	16	4	9	12	13	2	14	19	17	18	3	7	0	5	6	11	8	1	10
16	13	9	6	17	18	3	19	12	2	14	15	8	1	10	11	0	4	5	7
17	2	10	7	18	3	19	16	13	14	15	12	1	9	11	8	4	5	6	0
18	14	11	0	3	19	16	17	2	15	12	13	9	10	8	1	5	6	7	4
19	12	1	5	16	17	18	3	15	13	2	14	11	8	9	10	7	0	4	6

L_2

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	3	7	8	14	15	12	13	18	19	16	17	5	6	0	4	9	10	11	1
19	12	1	5	16	17	18	3	15	13	2	14	11	8	9	10	7	0	4	6
1	5	3	15	9	10	11	8	4	6	7	0	17	18	19	16	13	2	14	12
5	10	15	16	6	7	0	4	9	11	8	1	2	14	12	13	18	3	19	17
7	8	13	18	0	4	5	6	11	1	9	10	15	12	2	14	19	16	17	3
4	9	14	19	5	6	7	0	1	10	11	8	13	2	15	12	17	18	3	16
6	11	12	17	7	0	4	5	10	8	1	9	14	15	13	2	3	19	16	18
12	17	5	10	13	2	14	15	16	18	3	19	0	4	6	7	8	1	9	11
15	16	4	9	12	13	2	14	19	17	18	3	7	0	5	6	11	8	1	10
13	18	6	11	2	14	15	12	17	3	19	16	4	5	7	0	1	9	10	8
14	19	0	1	15	12	13	2	3	16	17	18	6	7	4	5	10	11	8	9
16	13	9	6	17	18	3	19	12	2	14	15	8	1	10	11	0	4	5	7
18	14	11	0	3	19	16	17	2	15	12	13	9	10	8	1	5	6	7	4
17	2	10	7	18	3	19	16	13	14	15	12	1	9	11	8	4	5	6	0
3	15	8	4	19	16	17	18	14	12	13	2	10	11	1	9	6	7	0	5
8	4	18	14	1	9	10	11	0	5	6	7	16	17	3	19	12	13	2	15
9	6	19	12	10	11	8	1	5	7	0	4	18	3	16	17	2	14	15	13
11	0	17	2	8	1	9	10	7	4	5	6	19	16	18	3	15	12	13	14
10	7	16	13	11	8	1	9	6	0	4	5	3	19	17	18	14	15	12	?

L_3

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
3	15	8	4	19	16	17	18	14	12	13	2	10	11	1	9	6	7	0	6
1	5	3	15	9	10	11	8	4	6	7	0	17	18	19	16	13	2	14	12
15	16	4	9	12	13	2	14	19	17	18	3	7	0	5	6	11	8	1	10
6	11	12	17	7	0	4	5	10	8	1	9	14	15	13	2	3	19	16	18
4	9	14	19	5	6	7	0	1	10	11	8	13	2	15	12	17	18	3	16
7	8	13	18	0	4	5	6	11	1	9	10	15	12	2	14	19	16	17	3
5	10	15	16	6	7	0	4	9	11	8	1	2	14	12	13	18	3	19	17
16	13	9	6	17	18	3	19	12	2	14	15	8	1	10	11	0	4	5	7
17	2	10	7	18	3	19	16	13	14	15	12	1	9	11	8	4	5	6	0
19	12	1	5	16	17	18	3	15	13	2	14	11	8	9	10	7	0	4	6
18	14	11	0	3	19	16	17	2	15	12	13	9	10	8	1	5	6	7	4
8	4	18	14	1	9	10	11	0	5	6	7	16	17	3	19	12	13	2	15
10	7	16	13	11	8	1	9	6	0	4	5	3	19	17	18	14	15	12	2
11	0	17	2	8	1	9	10	7	4	5	6	19	16	18	3	15	12	13	14
9	6	19	12	10	11	8	1	5	7	0	4	18	3	16	17	2	14	15	13
12	17	5	10	13	2	14	15	16	18	3	19	0	4	6	7	8	1	9	11
14	19	0	1	15	12	13	2	3	16	17	18	6	7	4	5	10	11	8	9
13	18	6	11	2	14	15	12	17	3	19	16	4	5	7	0	1	9	10	8
2	3	7	8	14	15	12	13	18	19	16	17	5	6	0	4	9	10	11	1

4.2 Other Methods for Constructing MOLS of Non-Prime Power Orders

When s is not a prime power, a set of n(s) MOLS of order s can always be constructed using the method described in Section 4.1. In many cases, however, there exist special procedures which can be used to increase the number of MOLS from n(s) to some number $N(s) \geq n(s)$. It is not known in general what the maximum value of N(s) can be when s is not a prime power. However, in several cases N(s) is much greater than n(s).

In this section we will study briefly several procedures of construction which allow us to achieve an $N(s) > n(s)$. These procedures include construction of MOLS from block designs and group divisible designs; the method of differences; and finally special methods such as computer search procedures. Each of these procedures will be surveyed to give the reader a chance to see how $N(s) > n(s)$ can be achieved. For a more detailed study of any one of the methods, the reader is referred to the references contained in each section.

4.2.1 Construction of MOLS from Block Designs

Pairwise balanced designs, balanced incomplete block designs, and group divisible designs can be used to construct some sets of MOLS and to establish values for N(s). An arrangement of v objects (called treatments) in b blocks is a pairwise balanced design of index λ and type $(v; k_1, k_2, \ldots, k_m)$ if each block contains k_1, k_2,..., or k_m treatments which are all distinct ($k_i \leq v$, $k_i \neq k_j$) and every pair of distinct treatments occurs in exactly λ blocks of the design. It can be shown that for a pairwise balanced design of sets of size $k_i (i = 1, 2, \ldots, m)$, then

$$(4.2.1) \qquad b = \sum_{i=1}^{m} b_i, \qquad \lambda v(v-1) = \sum_{i=1}^{m} b_i k_i (k_i - 1).$$

To illustrate this definition, suppose we have four treatments 1, 2, 3, and 4 in eleven blocks $B_1, B_2, \ldots, B_{11}$ to form a pairwise balanced design of index 4 and type (4; 2,3,4):

B_1: 1,2 B_2: 1,3 B_3: 1,4 B_4: 2,3 B_5: 2,4 B_6: 3,4

B_7: 1,2,3 B_8: 1,2,4 B_9: 1,3,4 B_{10}: 2,3,4 B_{11}: 1,2,3,4.

In this case $v = 4$, $b = 11$, $b_1 = 6$, $k_1 = 2$, $b_2 = 4$, $k_2 = 3$, $b_3 = 1$, $k_3 = 4$, and $\lambda = 4$.

When $\lambda = 1$ we have a pairwise balanced design of index unity. Consider a pairwise balanced design D of index unity and type $(v; k_1, k_2, \ldots, k_m)$. The subdesign D_i formed by the blocks of size k_i is called the i-th equiblock component of D, $i = 1, 2, \ldots, m$. A subset of vlocks belonging to any equi-block component D_i is of type I if every treatment occurs in the subset exactly k_i times. Also a subset of blocks belonging to D_i is of type II if every treatment occurs in the subset exactly once. For example, a pairwise balanced design of index unity (i.e., $\lambda = 1$) and $v = 5$, $b = 6$, $b_1 = 4$, $k_1 = 2$, $b_2 = 2$, and $k_2 = 3$ is

First equiblock
- B_1: 1,4
- B_2: 1,5
- B_3: 3,4
- B_4: 3,5

Second equiblock
- B_5: 1,2,3
- B_6: 2,4,5

Treatment 2 does not occur in equiblock 1 so it cannot be of type I or type II. In the second equiblock all treatments do not occur exactly $k_2 = 3$ times and hence is not of type I; also, since all treatments do not occur exactly once, it is not of type II.

A component D_i is said to be <u>separable</u> if the blocks can be divided into subsets of type I or type II (both types may occur at the same time) and design D is defined to be separable if each equiblock component is separable. In the following pairwise design where $\lambda = 1$, $b = 3$, $b = 4$. $b_1 = 3$, $k_1 = 1$, $b_2 = 1$, and $k_2 = 3$, the first equiblock is of type I and type II and so is separable.

B_1: 1 $\quad$ B_2: 2 $\quad$ B_3: 3 $\quad$ B_4: 1,2,3

Equiblocks $D_1, D_2, \ldots, D_\ell (\ell<m)$ are said to be clear if the $\sum_{i=1}^{\ell} b_i$ blocks comprising $D_1, D_2, \ldots, D_\ell$ are disjoint. For example, the first two equiblocks in the next pairwise balanced design where $\lambda = 1$, $v = 6$, $b = 15$, $b_1 = 2$, $k_1 = 1$, $b_2 = 12$, $k_2 = 2$, $b_3 = 1$, $k_3 = 3$ are clear.

B_1: 1,2,5	B_4: 1,3	B_7: 2,3	B_{10}: 3,4	B_{13}: 4,5
B_2: 3	B_5: 1,4	B_8: 2,4	B_{11}: 3,5	B_{14}: 4,6
B_3: 6	B_6: 1,6	B_9: 2,6	B_{12}: 3,6	B_{15}: 5,6

A <u>balanced incomplete block</u> (BIB) <u>design</u> with parameters v, b, r, k, λ is an arrangement of v treatments into b blocks such that (1) each block contains $k < v$ different treatments, (2) each treatment occurs in r different blocks, and (3) each pair of treatments occurs together in exactly λ blocks. For a BIB design with these parameters, the equations

(4.2.2) $\lambda(v - 1) = r(k - 1)$ and $bk = vr$, $b \geq v$

are necessary but not sufficient for the existence of a BIB design. Specifically, $v = b = 22$, $r = k = 7$, $\lambda = 2$ satisfy these equations, but there is no design with these parameters. If $v = b$, then $k = r$ and in such a case the BIB design is said to be symmetric. The following is a BIB with $v = b = 7$, $k = r = 3$, $\lambda = 1$. It is also of type I as every treatment occurs exactly $k = 3$ times.

B_1: 1,2,5	B_4: 2,4,7	B_7: 5,6,7
B_2: 3,4,5	B_5: 1,4,6	
B_3: 1,3,7	B_6: 2,3,6	

Since $v = b$ and $k = r$, this is a symmetrical BIB.

A BIB design is <u>resolvable</u> if the sets of the blocks can be divided into sets, such that the blocks of a given set contain each treatment exactly once. When $\lambda = 1$ the BIB design is a pairwise balanced design of index unity and type $(v;k)$. Such a design is denoted by BIB$(v;k)$. The following BIB design where $v = 9$, $b = 12$, $r = 4$, $k = 3$, and $\lambda = 1$ is resolvable since the blocks in each set contain each treatment exactly once.

Set 1
- B_1: 1,2,3
- B_2: 4,6,8
- B_3: 5,7,9

Set 2
- B_4: 1,4,5
- B_5: 2,6,9
- B_6: 3,7,8

$$\text{Set 3} \quad \begin{cases} B_7: 1,6,7 \\ B_8: 2,5,8 \\ B_9: 3,4,9 \end{cases}$$

$$\text{Set 4} \quad \begin{cases} B_{10}: 1,8,9 \\ B_{11}: 2,4,7 \\ B_{12}: 3,5,6 \end{cases}$$

Bose, Shrikhande, and Parker [4] established the following main theorem relating MOLS and a pairwise balanced design of index unity.

Theorem 4.2.1 Let D be a pairwise balanced design $(v; k_1, k_2, \ldots, k_m)$ of index unity in which the equiblock components $D_1, D_2, \ldots, D_\ell$ ($\ell < m$) are a clear set. Let there be $q_i - 1$ MOLS of order k_i and let

$$q = \min(q_1 + 1, q_2 + 1, \ldots, q_\ell + 1, q_{\ell+1}, \ldots, q_m) \tag{4.2.3}$$

Then there exist at least $q - 2$ MOLS of order v.

Several corollaries which follow from this theorem allow a lower bound to be found for N(s). These corollaries given by Raghavarao [22] are:

Corollary 4.2.1 The existence of a BIB(v;k) implies that

$$N(v - 3) \geq \min[N(k), N(k-1), 1 + N(k-2)] - 1.$$

Corollary 4.2.2 The existence of a resolvable BIB(v;k) implies that

$$N(v + x) \geq \min[N(k), N(k+1), 1 + N(x)] - 1 \text{ if } 1 < x \leq r-2.$$

Corollary 4.2.3 The existence of a resolvable BIB(v;k) implies that

$$N(v+r-1) \geq \min[1 + N(k), N(k+1), 1 + N(r-1)] - 1.$$

Corollary 4.2.4 If s and s + 1 are both primes, then

$$N(s^m + 1) \geq s - 2.$$

Corollary 4.2.5 If $x \leq 10$

$$N(73 - x) \geq 5.$$

Corollary 4.2.6 If $x \leq 10$

$$N(81 - x) \geq 5.$$

Corollary 4.2.7 The existence of a BIB(v;k) with sets of type I implies that

$$N(v+r) \geq \min[N(k+1), 1 + N(r)] - 1.$$

Actually corollary 4.2.5 and corollary 4.2.6 are special cases of more general corollaries that Bose [3] develops from the following theorem

Theorem 4.2.2 If there exists a BIB(v;k), for which we can find a set of x treatments, no three of which occur in the same block, then

$$N(v-x) \geq \min[N(k), N(k-1), N(k-2)] - 1.$$

One corollary resulting from this states that if $s = p^n$ is a prime power,

$$N(s^2+s+1) \geq \min[N(s+1), s-1, N(s-1)] - 1$$

where $x \leq s + 1$ when p is odd, and $x \leq s + 2$ when $p = 2$. Setting $s = 8$ produces corollary 4.2.5. Bose also derives another corollary from the theorem which says that if $s = p^n$ is a prime power,

$$N(s^2-x) \geq \min[s-1, N(s-1), N(s-2)], \quad x \leq s+1.$$

When $s = 9$ we obtain corollary 4.2.6.

A result from Raghavarao [22] which provides useful corollaries in obtaining a value for N(s) is the next theorem.

Theorem 4.2.3 Let there exist a separable pairwise balanced design $(v;k_1, k_2, \ldots, k_m)$ of index unity and suppose that there exist $q_i - 1$ MOLS of order k_i. If

$$q = \min(q_1, q_2, \ldots, q_m)$$

then there are at least $q - 1$ MOLS of order v.

Some of the corollaries that follow from this theorem will now be stated.

Corollary 4.2.8 The existence of a symmetrical BIB(v;k) implies that

$$N(v) \geq N(k).$$

Corollary 4.2.9 If s is a prime or a prime power, then

$$N(s^2+s+1) \geq N(s+1).$$

Corollary 4.2.10 If s is a prime or a prime power, then

$$N(s^2-1) \geq N(s-1).$$

By working with the main theorem of Bose, Shrikhande, and Parker mentioned earlier, Murthy [19] obtained two new series of pairwise balanced designs of index unity and showed that $N(90) \geq 4$ and $N(94) \geq 5$ and improved the lower bound of N(s) for other $s > 100$. Construction of the N(s) MOLS

from these corollaries and methods involves construction of the corresponding pairwise balanced design or BIB and then modifying it in some particular fashion.

Group divisible designs constitute another method for constructing MOLS and stating lower bounds for N(s). An arrangement of v treatments in b blocks each containing k distinct treatments is said to be a group divisible design (GD) if the treatments can be divided into ℓ groups of m treatments each, so that any two treatments belonging to the same group occur together in λ_1 blocks, and any two treatments from different groups occur together in λ_2 blocks. Such a design is denoted by $GD(v;k,m;\lambda_1\lambda_2)$ and it can be shown that

$$v = \ell m, \quad bk = vr, \quad \lambda_1(m-1) + \lambda_2 m(1-1) = r(k-1),$$

where r is the number of replications, that is, the number of times each treatment occurs in the design.

In the following example we have a GD(14;4,2;0,1). There are 14 treatments in 7 blocks each containing 4 distinct treatments. Furthermore there are 7 groups of 2 treatments each such that any two treatments belonging to the same group occur together in 0 blocks, and any two treatments from different groups occur in 1 block.

The groups are:

G_1: 1,2 G_3: 5,6 G_5: 9,10 G_7: 13,14

G_2: 3,4 G_4: 7,8 G_6: 11,12

The blocks are:

B_1: 2,3,5,9	B_8: 1,4,6,10
B_2: 4,5,7,11	B_9: 3,6,8,12
B_3: 6,7,9,13	B_{10}: 5,8,10,14
B_4: 1,8,9,11	B_{11}: 2,7,10,12
B_5: 3,10,11,13	B_{12}: 4,9,12,14
B_6: 1,5,12,13	B_{13}: 2,6,11,14
B_7: 1,3,7,14	B_{14}: 2,4,8,13

Two more corollaries resulting from the main theorem of Bose, Shrikhande, and Parker which provide lower bounds for N(s) are:

Corollary 4.2.11 The existence of a GD(v;k,n;0,1) implies that

$$N(v-1) \geq \min[N(k), N(k-1), 1 + N(n), 1 + N(n-1)] - 1.$$

Corollary 4.2.12 The existence of a resolvable GD(v;k,n;0,1) with r replications imples that

$$N(v+x) \geq \min[N(k), N(k+1), 1 + N(n), 1 + N(x)] - 1 \text{ if } 1 < x < r.$$

Using group divisible designs, Bose, Shrikhande, and Parker [4] establish the following theorem, which with proper selection of parameters allows one to deduce that $N(82) \geq 4$, $N(95) \geq 6$, and $N(60) \geq 3$.

Theorem 4.2.4 If $k \leq N(m) + 1$, then

$$N(km+x) \geq \min[N(k), N(k+1), 1 + N(m), 1 + N(x)] - 1 \text{ if } 1 < x < m.$$

Construction of the number of MOLS asserted by thes corollaries or theorem is accomplished by means of using the group divisible design corresponding to the theorem or corollaries.

One problem of using block designs or group divisible designs to determine N(s) is that this presupposes a knowledge of the existence of a particular block design for certain values of the parameters. This, however, is not usually a problem since existence of block designs is tabled for many cases in Cochran and Cox [8], Hall [13], and Raghavarao [22] and many other sources. Most of the time a suitable block design can be found to handle the problem. But for those times when such a block design does not exist or is not known to exist, one alternative which can be used in certain cases for finding N(s) and constructing the MOLS is the method of differences. This is our next topic.

4.2.2 Method of Difference

Some sets of MOLS can be constructed by a technique called the method of differences. This technique presupposes an understanding of orthogonal arrays, which is a generalization of orthogonal Latin squares. Since orthogonal arrays are beyond the scope of this paper, the interested reader is referred to Raghavarao [22], Bose [3], or Hall [13] for their development and use in the method of differences.

However, an understanding of the method of differences is not necessary in order to be able to apply the theorems resulting from this method which state lower bounds for N(s) in certain cases. Some of these theorems follow.

Theorem 4.2.5 If m is odd, there exist at least two MOLS of order $3m + 1$. In particular, if $m = 4t + 3$, then $N(12t + 10) \geq 2$.

Theorem 4.2.6 $N(14) \geq 2$.

Theorem 4.2.7 $N(18) \geq 2$.

Theorem 4.2.8 $N(26) \geq 2$.

4.2.3 Other Methods of Construction of MOLS

Computer search procedures comprise another method of constructing MOLS. Johnson, Dulmage, and Mendelsohn [14] introduced the notion of an orthomorphism. This is a transformation which when applied to the addition table of an abelian group yields a square which is orthogonal to the original square. The theory of orthomorphisms leads to an algorithm for the computation of orthogonal Latin squares, which can be programmed on a digital computer. Using this method 5 MOLS of order 12 were constructed. It is indicated that for large s, this method is not practical.

Other computer investigations of orthogonal Latin squares include the work of Bose, Chakravarti, and Knuth [5] and Parker [21].

It is not known in general what the maximum value of N(s) can be when s is not a prime power. The problem of finding a complete set of MOLS for s not a prime power is still open.

The methods discussed in this last section will undoubtedly be used to extend the existing lower bounds of N(s) for certain values of s. Perhaps a new method of constructing MOLS will be discovered which will allow a

unified theory of obtaining the true upper bound of N(s) for all s. Or if this is not possible, then a demonstration or proof of why it is not possible.

5. SUMMARY

In this report we have developed Galois Field theory and looked at its relationship to projective geometries and affine geometries by means of investigating construction of MOLS of order s when s is a prime power. Construction by Galois Fields was generalized one step further to the method of construction associated with the MacNeish-Mann theorem in order to handle cases when s is not a prime power.

This material on Galois Fields and MOLS provides a good background for working with experimental designs and lays a foundation for constructing balanced incomplete block designs and partially balanced incomplete block designs. With these techniques it is even easier for the statistician to create or derive his own experimental design or alter it to fit the problem at hand.

Besides the aesthetic appeal of certain combinatorial problems related to MOLS, scheduling problems subject to time and space constraints can be solved by using an ordering from an appropriate set of MOLS.

The section surveying miscellaneous methods for constructing MOLS presents terminology of the other main types of block designs.

We are now in the position of having covered all the construction techniques needed to reach the maximum number of MOLS of order s when $s \leq 100$. These construction techniques also produce the optimal number of MOLS of order s for most cases when $s > 100$. In way of summary, let us

look at construction of MOLS when $s \leq 100$. For s a prime or a prime power, complete sets of s - 1 MOLS can be constructed using Galois Fields, finite projective planes, or finite Euclidean planes. When s is not a prime or a prime power, the MacNeish-Mann theorem allows construction of n(s) MOLS of order s. Using special techniques, we can sometimes find N(s) > n(s) MOLS of order s. Table 5.1 summarizes the cases where s is not a prime or a prime power, giving n(s) and the greatest lower bound of N(s) known so far, along with the construction technique needed to achieve this N(s) value. Thus the reader should now have a thorough knowledge of construction techniques of MOLS of order s, where $s \leq 100$.

Table 5.1

s	n(s)	N(s)≥	Method of Construction
6	1	1	Eulerian number
10	1	2	Theorem 4.2.5 (m=3)
12	2	5	Johnson, Dumlage, and Mencelsohn [14]
14	1	2	Theorem 4.2.6
15	2	2	MacNeish-Mann theorem
18	1	2	Theorem 4.2.7
20	3	3	MacNeish-Mann theorem
21	2	4	Corollary 4.2.9 (s=4)
22	1	2	Theorem 4.2.5 (m=7)
24	2	3	Corollary 4.2.10 (s=5)
26	1	2	Theorem 4.2.8
28	3	3	MacNeish-Mann theorem
30	1	2	Corollary 4.2.3 (v=21,k=3,r=10)
33	2	3	Corollary 4.2.7 (v=25,r=8,k=4)
34	1	2	Theorem 4.2.5 (m=11)
35	4	4	MacNeish-Mann theorem
36	3	3	MacNeish-Mann theorem
38	1	2	Corollary 4.2.1 (v=41,k=5)
39	2	3	Corollary 4.2.11 on GD(40;5,8;0,1)
40	4	4	MacNeish-Mann theorem
42	1	2	Corollary 4.2.1 (v=45,k=5)
44	3	3	MacNeish-Mann theorem
45	4	4	MacNeish-Mann theorem
46	1	3	Shih [23]
48	2	2	MacNeish-Mann theorem

s	n(s)	N(s)$\geq$	Method of Construction
50	1	5	Corollary 4.2.4 (s=7,m=2)
51	2	2	MacNeish-Mann theorem
52	3	3	MacNeish-Mann theorem
54	1	4	Corollary 4.2.2 (v=49,k=7,x=5)
55	4	4	MacNeish-Mann theorem
56	6	6	MacNeish-Mann theorem
57	2	7	Corollary 4.2.8 (v=57,k=8)
58	1	2	Theorem 4.2.5 (m=19)
60	2	3	Theorem 4.2.4 (k=7,m=8,x=4)
62	1	2	Corollary 4.2.1 (v=65,k=5)
63	6	6	MacNeish-Mann theorem
65	4	7	Corollary 4.2.7 (v=57,r=8,k=8)
66	1	5	Corollary 4.2.5 (x=7)
68	3	5	Corollary 4.2.5 (x=5)
69	2	5	Corollary 4.2.5 (x=4)
70	1	6	Corollary 4.2.1 (v=73,k=9)
72	7	7	MacNeish-Mann theorem
74	1	5	Corollary 4.2.6 (x=7)
75	2	5	Corollary 4.2.6 (x=6)
76	3	5	Corollary 4.2.6 (x=5)
77	6	6	MacNeish-Mann theorem
78	1	6	Corollary 4.2.1 (v=81,k=9)
80	4	7	Corollary 4.2.10 (s=8)
82	1	4	Theorem 4.2.4 (k=7,m=11,x=5)
84	2	5	Corollary 4.2.12 on GD(77;7,11;0,1)(x=7)
85	4	5	Corollary 4.2.12 on GD(77;7,11;0,1)(x=8)

s	n(s)	N(s)≥	Method of Construction
86	1	5	Corollary 4.2.12 on GD(77;7,11;0,1)(x=9)
87	2	2	MacNeish-Mann theorem
88	7	7	MacNeish-Mann theorem
90	1	4	Murthy [19]
91	6	6	MacNeish-Mann theorem
92	3	5	Corollary 4.2.12 on GD(91;7,13;0,1)(x=1)
93	2	3	Shih [23]
94	1	5	Murthy [19]
95	4	6	Theorem 4.2.4 (k=8,m=11,x=7)
96	2	6	Corollary 4.2.12 on GD(88;8,11;0,1)(x=8)
98	1	5	Corollary 4.2.12 on GD(91;7,13;0,1)(x=7)
99	8	8	MacNeish-Mann theorem
100	3	5	Corollary 4.2.12 on GD(91;7,13;0,1)(x=9)

ACKNOWLEDGEMENTS

The writer wishes to express his sincere appreciation to Dr. J.W. Evans for his helpful suggestions in directing the writing of this report. I am also indebted to Dr. A. M. Feyerherm for his supervision of this paper and to Rosemary Kelly for typing the manuscript.

REFERENCES

[1] Bose, R. C. (1938), "On the application of the properties of Galois Fields to the problem of construction of hyper-Graeco-Latin squares", Sankhya, 3: Part 4, 323-338.

[2] Bose, R. C. (1939), "On the construction of balanced incomplete block designs", Annals of Eugenics, 9: 353-399.

[3] Bose, R. C. (1950), The Design of Experiments, Mimeographed Lecture Notes, University of North Carolina.

[4] Bose, R. C., Shrikhande, S. S., and Parker, E. T. (1960), "Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture", Canadian Journal of Mathematics, 12: 189-203.

[5] Bose, R. C., Chakravarti, I. M., and Knuth, D. E. (1961), "On methods of constructing sets of mutually orthogonal Latin squares using a computer - II", Technometrics, 3: 111-118.

[6] Bruck R. H. and Ryser, H. J. (1949), "The nonexistence of certain finite projective planes", Canadian Journal of Mathematics, 1: 88-93.

[7] Bruck, R. H. (1963), "Finite nets II", Pacific Journal of Mathematics, 13: 421-457.

[8] Cochran, W. G. and Cox, G. M. (1950), Experimental Designs, Wiley, New York.

[9] Euler, L. (1782), "Recherches sur une nouvelle espece de quarres magiques", Verh. Genootsch. der Wet Vlissingen, 9: 85-232.

[10] Eden T. and Fisher, R. A. (1929), "Studies in crop variation. VI. Experiments on the response to potash and nitrogen", Journal of Agricultural Science, 19: Part 2, 201-213.

[11] Fisher, R. A. (1926), "The arrangement of field experiments", Journal of the Ministry of Agriculture, 33: 503-513.

[12] Fisher, R. A. and Wishart, J. (1930), "The arrangement of field experiments and the statistical reduction of the results", Imperial Bureau of Soil Science, Technical Communication, Number 10.

[13] Hall, M. H. Jr. (1967), Combinatorial Theory, Blaisdell, Waltham, Massachusetts.

[14] Johnson, D. M., Dulmage, A. L., and Mendelsohn, N. S. (1961), "Orthomorphisms of Abelian groups and orthogonal Latin squares", Canadian Journal of Mathematics, 13: 356-372.

[15] Liu, C. L. (1968), Introduction to Combinatorial Mathematics, McGraw-Hill, New York.

[16] MacNeish, H. F. (1922), "Euler squares", Annals of Mathematics, 23: 221-227.

[17] Mann, H. B. (1942), "The construction of orthogonal Latin squares", Annals of Mathematical Statistics, 13: 418-423.

[18] Maxfield, J. E. and Maxfield, M. W. (1971), Abstract Algebra and Solution by Radicals, W. B. Saunders Company, Philadelphia, Pennsylvania.

[19] Murthy, J. S. (1965), "On the construction of mutually orthogonal Latin squares of non-prime power orders", Journal of the Indian Society of Agricultural Statistics, 17: 224-229.

[20] Parker, E. T. (1958), "Construction of some sets of pairwise orthogonal Latin squares", American Mathematical Society Notices, 5: 815 (abstract).

[21] Parker, E. T. (1963), "Computer investigations of orthogonal Latin squares of order 10", Proceedings of the Symposium in Applied Mathematics, 15: 73-81.

[22] Raghavarao, D. (1971), Construction and Combinatorial Problems in Design of Experiments, Wiley, New York.

[23] Shih, C. -C. (1965), "A method of constructing the orthogonal Latin squares", Shuxue Jinzhan, 8: 98-104.

[24] Wishart, J. (1931), "The analysis of variance illustrated in its application to a complex agricultural experiment on sugar beet", Archiv Fur Pflanzenbau, 5: 561.

[25] Yates, F. (1933a), "The formation of Latin squares for use in field experiments", Empire Journal of Experimental Agriculture, 1: Number 3, 235-244.

[26] Yates, F. (1933b), "The priniciples of orthogonality and confounding in replicated experiments", Journal of Agricultural Science, 33: Part 1, 108-145.

[27] Vajda, S. (1967), The Mathematics of Experimental Design: Incomplete Block Designs and Latin Squares, Griffin's Statistical Monographs and courses, Number 23, Hafner, New York.

CONSTRUCTION OF SETS OF MUTUALLY ORTHOGONAL LATIN SQUARES

by

GLENN CHARLES CADEK

B.A., Wichita State University, 1973

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Statistics

KANSAS STATE UNIVERSITY

Manhattan, Kansas

1975

ABSTRACT

In this report, a foundation for studying and investigating block designs is developed. The focus of concern is the construction and existence of mutually orthogonal Latin squares. The mathematics necessary for the construction of these designs involves Galois Fields and finite geometries, which also comprise the groundwork for other types of block designs. One reason for starting with mutually orthogonal Latin squares (MOLS) is that they can be modified from other types of block designs.

These same designs are also constructed by using projective geometries. Partially for the sake of completeness in the study of construction techniques, these additional methods are covered. By doing so, we gain an important corollary about the existence or nonexistence of complete sets of MOLS of order s where s is a prime or a prime power.

Construction of MOLS of order s when s is not a prime is demonstrated by the technique associated with the MacNeish-Mann theorem. This technique is actually a generalization of the procedure using Galois Fields. Other methods of construction which, in special cases, allow an increase in the number of MOLS obtained by the MacNeish-Mann procedure are surveyed.

This material on Galois Fields and MOLS provides a good background for working with experimental designs and lays a foundation for construc-

ting balanced incomplete block designs and partially balanced incomplete block designs. With these techniques it is even easier for the statistician to create or derive his own experimental design or alter it to fit the problem at hand.