UNIVERSITY OF NAIROBI

College of Biological and Physical Sciences

School of Mathematics

ON THE RELATIONSHIPS BETWEEN LATIN SQUARES, FINITE GEOMETRIES & BALANCED INCOMPLETE BLOCK DESIGNS (BIBDs)

by

Andrew W. Nyamu

A PROJECT SUBMITTED TO THE SCHOOL OF MATHEMATICS IN PARTIAL FULFILLMENT FOR THE DEGREE OF MASTER OF SCIENCE IN STATISTICS

June 2016

Declaration

This project is my original work and has not been presented for the award of a degree in any other University.

Signature: ..... Date: .....

Andrew W. Nyamu

(I56/75598/2014)

This project has been submitted with my approval as University supervisor.

Signature: ..... Date: .....

Prof. Moses M. Manene

School of Mathematics

Abstract

In this project, we have reviewed the methods of constructing Balanced Incomplete Block Designs (BIBDs) by means of Mutually Orthogonal Latin squares (MOLS) of prime powers order arising from Finite Geometries and Finite Fields. This project finds that the existence of an Affine plane of prime powers order implies the existence of a set of Mutually Orthogonal Latin squares (MOLS) of the same order, a treatment square of side equal to the prime powers order, a set of bijective maps defined on the key Latin square into the treatment space and a transformation defined on the set of bijective maps that generates new sets of bijective maps that are the mappings of the remaining MOLS into the treatment square.

Key Words: *Balanced Incomplete Block Designs (BIBDs); Bijective map; Treatment space; Latin Squares; Orthogonal Latin Squares; Mutually Orthogonal Latin Squares (MOLS); Geometries - Projective & Euclidean (Affine); Finite (Galois) Fields*

Acknowledgments

Though this project is the authors personal work, it would not have been completed without the academic, spiritual, or moral support from many individuals.

First and foremost, I want to thank God the creator; Jesus Christ the saviour; and Holy Spirit the companion & comforter, for allowing me to live in this world, blessing me with knowledge, and guiding me throughout my MSc candidature.

Next, I would like to express my heartfelt thanks to my supervisor Prof. Moses Manene, who has been a critical reviewer of my work, very meticulous, diligent, the first filter for all my forays into this project. I am motivated by your passion for research and academic excellence. Thanks for your keen interest in seeing me through this project.

The support of two very important people in my life, my father, David N. Nyamu, and mother, Alice W. Nyamu, cannot be overstated. Thank you for bearing with me when I decided to pursue a second MSc. You had your reservations but see! I've done it by God's help.

I want to thank my (many) dear siblings & friends for all the support you have given me at one time or another.

Dedication

I wish dedicate this project to my parents,
Mr. David N. Nyamu & Mrs. Alice W. Nyamu

Contents

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

Chapter 1

Introduction

Scientific research is a process of guided learning where knowledge is obtained by conducting experimens. An experiment is a set of observations made under conditions deliberately arranged by the observer. The three basic principles of experimental designs are:

1. **Replication:** more than one observation is taken for each combination of treatment factors.

2. **Blocking:** is the use of blocking factors to divide the experimental units into sets (blocks) in a manner that captures the variability introduced by blocking

3. **Randomisation:** combinations of treatment factors are allocated to experimental units in a manner that minimises bias.

To realise these principles, the experimenter makes use of such tools as combinatorial theory, the theory of algebraic structures and number theory.

Combinatorial design theory concerns itself with the arrangements of elements of a finite set into subsets in a manner that satisfies certain "balance" properties. Experimental Designs have had various applications in recreational mathematics, tournament scheduling, lotteries, mathematical biology, algorithm design & analysis, group testing & cryptography (see Stinson (2004)).

According to Arshaduzzaman (2014), the development of Latin squares started with Euler in 1779. Arthur Cayley extended the work of Euler between 1877 and 1890 and proved that the multiplication table of a group is a special Latin square. The development somewhat stalled until 1930 when the ideas of quasi-groups and loops began to be developed in group theory. These also played an important role in the foundations of finite geometries, and R. A. Fisher began using them together with other combinatorial structures in the design of statistical experiments.

1.1 Problem Statement

In this project, we study the relationships between Latin squares and finite geometries and the resulting BIBDs.

1.2 Objectives

The main objective of the study is to establish the relationships between Latin squares, finite geometries and BIBDs more intuitively. The specific objectives are:

1. Prove that the existence of an Affine Geometry is equivalent to the existence of a Projective Geometry.

2. Prove that the existence of an Affine Geometry is equivalent to the existence of $s-1$ mutually orthogonal Latin squares (MOLS) of prime-powers order s.

3. Develop a more intuitive description of constructing BIBDs from the $s-1$ MOLS.

1.3 Significance of the study

In the Design of Experiments, many fundamental questions seek to establish the existence or non-existence of a specified type of design (see Stinson (2004)). In this study, we are relating the methods of constructing BIBDs using mutually orthogonal Latin squares and Finite Geometries by looking at possible relationships in the parameters of the resulting BIBDs. This might provide insights that unify these methods, leading to a possible simplification of the computations that are involved in coming up with designs.

1.4 General Outline of the Project

Chapter 2 will provide important definitions, theorems and properties of designs that will give us a common vocabulary as we progress. Chapter 3 will be concerned with constructions of BIBDs using multiple methods. Chapter 4 will summarise the properties of the constructions, mainly by looking at their parameters, and try relating the methods of construction via these parameters. Chapter 5 will discuss the challenges encountered, & areas for further work.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 2

Preliminaries

We shall provide important definitions, theorems and corollaries that will lay our foundation for the work ahead. The theorems and corollaries are stated without proof or citation since these have become common literature in most books on Experimental Designs.

2.1 General Definitions and Theorems

The excellent book by Stinson (2004) provides the following definitions and theorems.

Definition 2.1. (Design; Repeated Blocks; Simple Design) *A Design is a pair* $(X, \mathcal{A})$ *with*

a) X*: a set of elements called points, and*

b) $\mathcal{A}$*: is a multiset on non-empty sets of* X *called blocks.*

Further, repeated blocks arise when two blocks in a design are identical, and a simple design is one which has no repeated blocks.

Definition 2.2. (Balanced Incomplete Block Design (BIBD)) *Let* ν*,* k*, and* λ *be positive integers such that* $\nu > k \geq 2$*. A* (ν, k, λ)*-BIBD is a design* $(X, \mathcal{A})$ *such that*

1. $|X| = \nu$,

2. *each block has exactly k points, and*

3. *every pair of distinct points is contained in exactly λ blocks (balance property)*

A BIBD is an incomplete block design because $k < \nu$, and hence all blocks are incomplete blocks.

Theorem 2.3. *In a (ν, k, λ)-BIBD, every point occurs in exactly*

$$r = \frac{\lambda(\nu - 1)}{(k - 1)}$$

blocks.

Theorem 2.4. *A (ν, k, λ)-BIBD, has exactly*

$$b = \frac{\nu r}{k} = \frac{\lambda\nu(\nu - 1)}{k(k - 1)}$$

blocks.

Corollary 2.5. *If a (ν, k, λ)-BIBD exists, then*

$$\lambda(\nu - 1) \equiv 0 \pmod{(k - 1)}, \text{ and}$$
$$\lambda\nu(\nu - 1) \equiv 0 \pmod{(k(k - 1))}$$

The above corollary trivially follows from theorems (2.3) and (2.4) and is useful as a quick check for the existence of a BIBD. A more general use of corollary (2.5) is to determine necessary conditions for families of BIBDs with fixed values of k and λ.

Definition 2.6. (Incidence Matrix) *Let $(X, \mathcal{A})$ be a design where $X = \{x_1, \ldots, x_\nu\}$ and $\mathcal{A} = \{A_1, \ldots, A_b\}$. The incidence matrix of the design $(X, \mathcal{A})$ is the 0-1 matrix $M_{\nu \times b}$ defined by the rule*

$$m_{i,j} = \begin{cases} 1 & if x_i \in A_j \\ 0 & otherwise \end{cases}$$

Theorem 2.7. *Let $M_{\nu\times b}$ be an incidence matrix and $2 \leq k < \nu$. Then $M_{\nu\times b}$ is the incidence matrix of a (ν, b, r, k, λ)-BIBD iff*

$$MM^T = \lambda J_\nu + (r-\lambda)I_\nu, \quad \textit{and,}$$
$$\boldsymbol{u_\nu} M = k\boldsymbol{u_b}$$

where $\boldsymbol{u_\nu}$ and $\boldsymbol{u_b}$ are unit vectors.

Theorem 2.8. *The 0-1 matrix $M_{\nu\times b}$ is an incidence matrix of a regular pairwise balanced design having 'ν' points and 'b' blocks iff*

$$(\exists r, \lambda \in \mathbb{N}^+ | MM^T = \lambda J_\nu + (r-\lambda)I_\nu)$$

Definition 2.9. (Dual) *Suppose that $(X, \mathcal{A})$ is a design with $|X| = \nu$ and $|\mathcal{A}| = b$ and $M_{\nu\times b}$ the incidence matrix of $(X, \mathcal{A})$. The design having incidence matrix M^T is the dual design of $(X, \mathcal{A})$.*

Definition 2.10. (Isomorphism) *Suppose that $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ are two designs with $|X| = |Y|$. Then the two designs $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ are isomorphic if there exists a bijection $\alpha : X \to Y$ such that*

$$[\{\alpha(x) | x \in A\} | A \in \mathcal{A}] = \mathcal{B}.$$

The bijection α is an isomorphism.

Isomorphisms of designs in terms of incidence matrices can be described in the theorem below:

Theorem 2.11. *Suppose $M_{\nu\times b} = (m_{i,j})$ and $N_{\nu\times b} = (n_{i,j})$ are incidence matrices. Then the two designs are isomorphic iff there exists a permutation γ of $\{1, \ldots, \nu\}$ and a permutation β of $\{1, \ldots, b\}$ such that*

$$m_{i,j} = n_{\gamma(i),\beta(j)} \qquad \forall\, (1 \leq i \leq \nu, 1 \leq j \leq b).$$

We also have the definitions below which can be found in any common literature concerning algebraic structures:

Definition 2.12. (Latin Square): *A Latin square of order 'k' is an arrangement of 'k' symbols in a k×k square so that every symbol appears once and once only in each row and each column.*

Example 2.13. *Below is an example of a Latin square.*

α	β	θ	γ
β	θ	γ	α
θ	γ	α	β
γ	α	β	θ

Arising from $\mathcal{S} = \{\gamma, \alpha, \beta, \theta\}$ and $k = 4 = |\mathcal{S}|$

Definition 2.14. (Orthogonal Latin Squares): *Two Latin squares of the same order, both defined as in definition 2.12 above, are said to be orthogonal if when superimposed, each element of the first square appears with each element of the second square once and once only.*

Definition 2.15. (Mutually Orthogonal Latin Squares): *If $L_1, \ldots, L_r$ are all Latin squares of the same order, defined as in definition 2.12 above, such that L_i is orthogonal to L_j for all $i \neq j$, then the set $(L_1, \ldots, L_r)$ is said to be a set of mutually orthogonal Latin squares of the same order.*

Example 2.16. *Below is an example of two mutually orthogonal Latin squares.*

A	B	C
B	C	A
C	A	B

A	B	C
C	A	B
B	C	A

Arising from $\mathcal{S} = \{A, B, C\}$ and $k = 3 = |\mathcal{S}|$

Bose (1938) gave a method to construct a set of mutually orthogonal Latin squares based on finite fields (GF_s). Arshaduzzaman (2014) summarises the method as below:

Let $GF(s) = x_0, \ldots, x_{s-1}$ be a finite field of order $s = p^m$, with $x_0 = 0$ and $x_1 = 1$. Let $L_1 = (a_{ij}^1)$ be the Latin square of order s that is the addition table of $GF(s)$. Then

$$a_{ij}^1 = x_i + x_j \qquad \text{for} \quad 0 \leq i, j \leq s-1$$

This is generalised in the proposition below:

Proposition 2.17. *Define the squares $L_k = (a_{ij}^k)$, for $1 \leq k \leq s-1$, by*

$$a_{ij}^k = x_k \cdot x_i + x_j \qquad \textit{for} \quad 0 \leq i, j \leq s-1$$

then L_k is a Latin square of order s for $1 \leq k \leq s-1$ based on $GF(s)$.

The proof that the Latin squares obtained above are mutually orthogonal is also given in the same paper by Arshaduzzaman (2014) and in many other sources since it is common literature in Experimental Designs.

Definition 2.18. (Field): *Is an algebraic structure, $(\mathcal{F}, +, \cdot)$, formed by a set $\mathcal{F}$ together with two binary operations $(+, \cdot)$, addition and multiplication defined on the set $\mathcal{F}$ by prescription of the following axioms $\forall \alpha, \beta, \gamma \in \mathcal{F}$:*

i) Associative property:
$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ *and*
$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

ii) Commutative property:
$\alpha + \beta = \beta + \alpha$ *and*
$\alpha \cdot \beta = \beta \cdot \alpha$

iii) Identity element:
$\exists! 0 \in \mathcal{F} | \alpha + 0 = 0 + \alpha = \alpha, \forall \alpha \in \mathcal{F}$ *and*
$\exists! 1 \in \mathcal{F} | \alpha \cdot 1 = 1 \cdot \alpha = \alpha, \forall \alpha \in \mathcal{F}$

iv) Distributive property of multiplication over addition:
$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \beta) = \alpha \cdot \beta + \alpha \cdot \beta$

v) Inverse element:

$\forall \alpha \in \mathcal{F}, \exists!(-\alpha) \in \mathcal{F} | \alpha + (-\alpha) = (-\alpha) + \alpha = 0$ *and*

$\forall (\alpha \neq 0) \in \mathcal{F}, \exists!(\alpha^{-1}) \in \mathcal{F} | \alpha \cdot (\alpha^{-1}) = (\alpha^{-1}) \cdot \alpha = 1$

Definition 2.19. (Galois field): *An algebraic structure satisfying all the properties of the field in definition* (2.18) *above, but with* $\mathcal{F}$ *being a finite set of elements. It is denoted* GF_p *where* $p = |\mathcal{F}|$.

Definition 2.20. (Commutative Ring): *A set of elements together with the binary operations* $(+, \cdot)$ *of a field that satisfy all the properties of a field except multiplicative identity.*

In the construction of experimental designs using geometries, the points are usually taken to represent treatments whereas the lines and higher $m-$flats represent blocks. We now lay out some basic definitions and theorems of the finite geometries as found in Vanpoucke (2012).

Definition 2.21. (Finite Incidence Structure/Finite Geometry): $\mathcal{P} = (P, B, I)$ *is a finite set of points* P*, a finite set of lines* B*, and a relation* I *between the points and the lines, called the* **incidence relation.**.

Definition 2.22. (Finite Projective Plane): *Is a finite incidence structure such that the following properties hold.*

I. Two different points are incident with one line.

II. Two different lines are incident with one point (i.e. they intersect).

III. There exists at least four different points such that no three of them are incident with one line.

Definition 2.23. *For a finite projective plane* $\mathcal{P}$*, there is a positive integer* s*, such that any line of* $\mathcal{P}$ *has exactly* $s + 1$ *points. The* **order** *of* $\mathcal{P}$ *is* s.

Projective planes are denoted $PG(p, s)$, whenever it is constructed from a finite field of order s (i.e. $GF(s)$) and p is the highest dimension of the subspace. Vanpoucke

(2012) also noted that the theorem of Desargues is only valid in $PG(2, n)$ and thus such a finite projective plane is a **Desarguesian** plane.

Theorem 2.24. *On any line, there are $s + 1$ points, where $2 \leq s$.*

Theorem 2.25. *Through any point, there passes $s + 1$ lines.*

Theorem 2.26. *The total number of points in the geometry is $s^2 + s + 1$.*

Theorem 2.27. *The total number of lines in the geometry is $s^2 + s + 1$.*

2.2 Literature Review

Arshaduzzaman (2014) summarised the work of Bose (1938) by presenting a paper that dealt with Latin squares, orthogonal Latin squares, mutually orthogonal Latin squares and the close connections between Latin squares and finite geometries. He also provided a historical background of Latin squares. In the paper, he showed that the table for a finite group $(G, +)$ of order n is a Latin square of order n based on G and that with Latin squares, permuting the rows among themselves (or columns) results in a new Latin square of the same order (hence the set of MOLS - Mutually Orthogonal Latin Squares). He noted that Latin squares were useful in designing statistical experiments because they showed how to arrange factors and experimental units in a manner that minimised errors without making the experiment too large. He also empirically showed that there existed Latin squares that could not be derived from group tables.

Tang (2009) discussed Latin squares and their transversals, Mutually Orthogonal Latin Squares (MOLS) and Latin subsquares and their applications in coding messages, and game playing. He also noted that Latin squares were a "relatively unknown aspect of mathematics". He also introduces the Kronecker Product method of constructing MOLS in addition to the Finite (Galois) Field method.

Pachamuthu (2011) studied the construction of 2^2 and 3^2 Mutually Orthogonal Latin Squares by using Galois Field theory.

Bose (1938) discussed the Graeco-Latin square which is just a pair of two orthogonal Latin squares superimposed on one another, with one having Greek symbols. He also referred to the superposition of $p-1$ mutually orthogonal squares of size p as a completely orthogonalised or Hyper-Graeco-Latin square. In his paper, he sought to prove the surmise that it is possible to construct a Hyper-Graeco-Latin square for every value of p, which is a prime or prime power using the properties of Galois Fields.

Vanpoucke (2012) studied Latin squares, Sudoku Latin squares, mutually orthogonal Latin squares and mutually orthogonal Sudoku Latin squares, their properties and generalizations. In his thesis, he also discussed the important connection between Latin squares and projective planes especially when it came to mutually orthogonal Latin squares (MOLS). He proved the conjecture that there are $(p-2)!$ distinct sets of $(p-1)MOLS(p)$, for prime p, describing $PG(2,p)$ and extended his results to prime powers of p.

Chapter 3

Constructions

Here, we shall state some propositions and theorems and give the corresponding proofs (and examples where necessary) for the purpose of completeness. A good Abstract Algebra book like Fraleigh (2002) and Beachy and Blair (2005) would offer a more complete treatment of finite fields.

3.1 MOLS and Finite Fields

In Chapter 2, we already defined what Latin squares and orthogonal Latin squares are. We now consider the proposition below

Proposition 3.1. *For any s, the largest size of a set of $s \times s$ MOLS is $s - 1$.*

Proof. Suppose we have a set of $L_1, \ldots, L_{s-1}$ MOLS. An automorphism of any of the Latin squares in the set remains orthogonal to the rest of the Latin squares in the set. Take out any pair of orthogonal Latin squares from the set and consider the symbol

in the cell in the second row, and first column as shown below (i.e. cell (2, 1)):

$$\begin{bmatrix} 1 & 2 & \dots & s \\ \alpha & - & \dots & \\ \vdots & & & \\ - & - & \dots & - \end{bmatrix}, \begin{bmatrix} 1 & 2 & \dots & s \\ \beta & - & \dots & \\ \vdots & & & \\ - & - & \dots & - \end{bmatrix}.$$

Now, α and β are both different from 1 (properties of a Latin square) and $\alpha \neq \beta$ (we do not have any repeated pairs from any two superimposed orthogonal Latin squares since the first row has pairs that agree). The same goes for all other symbols in the other cells leaving us with $s-1$ distinct choices for the cell (2, 1) that are not 1. This implies that there are $s-1$ squares in our collection of mutually orthogonal Latin squares $L_1, \dots, L_{s-1}$ □

Proposition 3.2. *Let $\mathcal{F}$ be a finite field with s elements. Then there is a collection of $s-1$ mutually orthogonal Latin squares.*

Proof. Let $\mathcal{F} = \{f_0, f_1, \dots, f_{s-1}\}$, and $f_0 = 0$, $f_1 = 1$. Then the array below is a Latin square $\forall(a \neq 0) \in \mathcal{F}$:

$$\begin{bmatrix} af_0 + f_0 & af_1 + f_0 & \dots & af_{s-1} + f_0 \\ af_0 + f_1 & af_1 + f_1 & \dots & af_{s-1} + f_1 \\ \vdots & \vdots & \ddots & \vdots \\ af_0 + f_{s-1} & af_1 + f_{s-1} & \dots & af_{s-1} + f_{s-1} \end{bmatrix},$$

where we have cell (i, j) with $af_i + f_j$. We now prove that the above array is indeed a Latin square. Suppose that along some row i, there are two cells (i, j) and (i, k)

which are the same, i.e. that

$$\begin{aligned} & af_i + f_j = af_i + f_k \\ \implies \quad & a(f_i - f_i) = (f_k + f_j) \\ \implies \quad & 0 = (f_k - f_j) \\ \implies \quad & f_j = f_k, \end{aligned}$$

and thus $j = k$ and that the two cells are not different. By similar argument, picking any column j along which are two cells (i, j) and (k, j) which are the same, we have

$$\begin{aligned} & af_i + f_j = af_k + f_j \\ \implies \quad & a(f_i - f_k) = (f_j - f_j) \\ \implies \quad & a(f_i - f_k) = 0 \\ \implies \quad & f_i = f_k, \end{aligned}$$

and thus $i = k$ and that the two cells are not different. We are thus able to generate $s - 1$ distinct Latin squares, labeled $L_a, \forall a \in \mathcal{F}$. We now prove the claim that all the Latin squares generated this way are mutually orthogonal Latin squares. Take two squares L_a, L_b and suppose that there are two cells (i, j), (k, l) which at superimposing yield the same ordered pair of symbols: i.e. that

$$af_i + f_j = af_k + f_l \text{ and } bf_i + f_j = bf_k + f_l$$

Taking the difference of the two equations

$$\begin{aligned} & (a - b)f_i = (a - b)f_k \\ \implies \quad & f_i = f_k \end{aligned}$$

and working the above result in the earlier equations, we observe that $f_j = f_l$, and therefore the two cells are not different, which proves the claim. □

We now turn our attention to the finite fields and see how they give rise to Latin squares by construction in an example.

Theorem 3.3. *There is a finite field of order s if and only if s can be expressed as a prime power.*

Definition 3.4. Galois Field *is a field containing a finite number of elements, say s, and is denoted GF(s) or $\mathcal{F}_s$.*

Definition 3.5. (Ring of Polynomials over $\mathcal{F}$) *Given a finite field $\mathcal{F}$, we can form the ring of polynomials over $\mathcal{F}$, $F[x]$, by taking all polynomials of the form*

$$a_0 + a_1x + a_2x^2 + \ldots + a_sx^s,$$

where $a_i \in \mathcal{F}$.

To extract a finite field from the ring of polynomials, find an irreducible polynomial, say $g(x)$ of degree s in $F[x]$. Multiply it with an appropriate constant to make the coefficient of x^s in $g(x)$ be 1. In $F[x]$, we now regard any two polynomials that differ by a multiple of $g(x)$ to be congruent, and we arrive at the finite field which we denote as $F[x]/\langle g(x)\rangle$, that is, the finite field has as it's elements, the residual class $(\mathrm{mod}\, g(x))$.

Suppose now, we wish to construct the set of mutually orthogonal Latin squares arising from the field $\mathcal{F}$ of order $s = 8 = 2^3$. We start by enumerating elements of $F[x]/\langle g(x)\rangle$ where $g(x)$ is $(x^3 + x^2 + 1)$, i.e.

$$ax^2 + bx + c \pmod{x^3 + x^2 + 1},\ \forall(a, b, c \in \mathcal{F}_2)$$

thus

$$x^3 = -x^2 - 1 + (2x^2 + 2) = x^2 + 1 \pmod 2$$
$$\implies \quad F[x]/\langle g(x)\rangle = \{0,\ 1,\ x,\ x^2,\ x^2 + 1,\ x^2 + x + 1,\ x + 1,\ x^2 + x\}$$

We create the addition ($+$) and multiplication ($\cdot$) tables below

$+$	0	1	x	x^2	x^2+1	x^2+x+1	$x+1$	x^2+x
0	0	1	x	x^2	x^2+1	x^2+x+1	$x+1$	x^2+x
1	1	0	$x+1$	x^2+1	x^2	x^2+x	x	x^2+x+1
x	x	$x+1$	0	x^2+x	x^2+x+1	x^2+1	1	x^2
x^2	x^2	x^2+1	x^2+x	0	1	$x+1$	x^2+x+1	x
x^2+1	x^2+1	x^2	x^2+x+1	1	0	x	x^2+x	$x+1$
x^2+x+1	x^2+x+1	x^2+x	x^2+1	$x+1$	x	0	x^2	1
$x+1$	$x+1$	x	1	x^2+x+1	x^2+x	x^2	0	x^2+1
x^2+x	x^2+x	x^2+x+1	x^2	x	$x+1$	1	x^2+1	0

,

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

and inspect them for the properties of a field - the properties of a field are satisfied by the above tables. We can form the key Latin square from the addition table and proceed thereafter to create the $s-1$ mutually orthogonal Latin squares.

It is important to note, however, that the set of $s-1$ mutually orthogonal Latin squares do not always exist for any order s, and that the maximum number of mutually orthogonal Latin squares of most non-prime-powers order are unknown.

3.2 Latin Squares and Finite Geometry

In this section, we want to prove that the existence of an affine plane is equivalent to the existence of a projective plane and that there exists an affine plane of order s iff there exists a complete set of MOLS of the same order. The existence of MOLS of the same order, s, implies the existence of a BIBD as shall be shown.

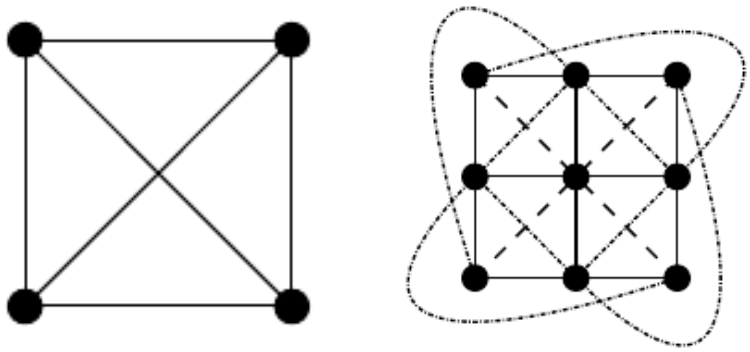
Definition 3.6. (Affine Plane) *is a collection of points and lines in space that adhere to*

(A1): There is exactly one line joining any two points.

(A2): Given a point P and a line L not containing P, there is a unique line that contains P and does not intersect L.

(A3): There exist four points such that no three of them are collinear.

The Euclidean plane is an affine plane; we restrict ourselves to finite affine planes.



(a) 4 points, 6 lines (b) 9 points, 12 lines

Figure 3-1: Affine Planes

Definition 3.7. (Projective Plane) *is a set of points and lines such that*

(P1): There is exactly one line joining any two points.

(P2): Any two lines intersect at a unique point.

(P3): There are four points such that no three of them are collinear.

Proposition 3.8. *In any affine plane, there is an integer s such that every line in the plane has exactly s points, and every point lies on precisely $s+1$ lines: s is the order of the plane.*

Proof. Suppose we can always find a third point P that does not lie on either of any two lines L_1 and L_2 of our plane. Then, given any point Q on the line L_1, we can find a line M through Q and P via property A1 of our affine plane, and this line cannot intersect any other elements on L_1. Thus, every point in L_1 is contained within one

line through P. Furthermore, by property A2, there is another line through P that does not meet L_1. Thus if $|L_1|$ denotes the total number of points contained in L_1, then we have $|L_1| + 1$ lines through P. This extends to all other lines of the plane, and since this all counts the same object: the number of lines through P, we have $|L_1| = |L_2|$. Therefore, all lines contain the same number of points, say s, and any point is contained by $s + 1$ lines. □

Proposition 3.9. *Any finite affine plane of order s contains s^2 points.*

Proof. In the affine plane, every point, say P, is on $s + 1$ lines, each of which contain $s - 1$ points different from P. By properties A1 and A2, there is exactly one line connecting any other point in the plane to P, thus there are

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

points in the plane ((s + 1) lines each contain (s - 1) points other than P in the plane). □

We see that the difference between the affine plane and the projective plane is in the prescription of their axioms, namely A2 and P2. Also, P1 and P2 together imply that the projective plane is symmetrical in that it is invariant to inverting its objects (see Tang (2009)). Tang (2009) also noted that in any projective plane of order s, every line contained $s + 1$ points and every point lay on $n + 1$ lines: each projective plane therefore contained $s^2 + s + 1$ points and $s^2 + s + 1$ lines.

Theorem 3.10. *The existence of an affine plane of order s is equivalent to the existence of a projective plane of order s.*

Proof. To transform any affine plane into a projective plane we proceed as follows: Extend the lines on each parallel class to meet at a 'point at infinity', so that $s + 1$ new points are made, then join all these 'points at infinity' with a line. The result is a plane with $s^2 + s + 1$ points and $s^2 + s + 1$ lines. Furthermore, every pair of lines now intersect at a unique point since the parallel classes now join at the 'point at infinity',

and every pair of points is still joined by a unique line since we've joined every new point that was created. Hence a projective plane. The reverse process transforms any projective plane into an affine plane. □

Definition 3.11. (Parallel Class): *is a collection of lines that are all parallel in an affine plane.*

Proposition 3.12. *In any finite affine plane of order s, there are exactly $s^2 + s$ lines that can be partitioned into $s + 1$ distinct parallel classes, each containing s lines.*

Proof. Pick any point P and any line L through P. Let M be any other line through P; then for each of the $s - 1$ non-P points in M, there is a parallel line through that point parallel to L. Taking this parallel lines along with L, constitutes a parallel class with s elements in it. Repeating this for all lines through P creates $s + 1$ different parallel classes, and every line M shows up in exactly one parallel class as (by A2) there is a unique line through P parallel to M that determines which of the $s + 1$ different parallel classes M is in. This counts each of our lines exactly once, hence $s^2 + s$ lines in total. □

We now prove that a set of $s - 1$ MOLS of order s is equivalent to a finite affine plane of order s.

Theorem 3.13. *A finite affine plane of order s exists if and only if a set of $s - 1$ MOLS of order s exist.*

Proof. We begin by describing how to turn a set of MOLS into an affine plane: we do this by the following construction; for points, take all the pairs (i, j), where $1 \leq i, j \leq s$. For lines, we list the lines of our affine plane in groups of s, corresponding to the $s + 1$ parallel classes that were shown to exist:

- Given any i, all of the cells in row i form a line. The collection of these s lines is a parallel class.

- Given any i, all of the cells in row i form a line. The collection of these s lines forms another parallel class.
- Take any Latin square L_α of our $s-1$ MOLS. Take any symbol a, and let all cells containing a in L_α be a line. The collection of all these s lines, one for each symbol constitute a parallel class. We get $s-1$ such parallel classes, one for each Latin square in our set.

The orthogonality of the Latin squares implies that none of the lines overlap. Thus, given any point (i, j), we've actually shown that it lies on $s+1$ lines, each of which contain $s-1$ other points: therefore the collection of all these lines contain

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

points, i.e., cell (i, j) is connected to every other cell in our Latin square by some line; hence A1 is satisfied.

To satisfy A2, take any line M and any other point (i, j) not on M. Suppose M is a row: the row i is a line parallel to M, and is unique in doing so since it is incident to the point (i, j). By similar argument, if M is a column, the column j is also the unique line parallel to M and incident to (i, j). Finally, if M is a set of cells with some underlying symbol a in the Latin square L_α, take the set of symbols underlying whatever symbol is in (i, j) in L_α. This is parallel to M and is unique in doing so since it is incident to (i, j): take any other line N containing (i, j), N must either be a row or a column or must come from some other symbol b and other Latin square L_β, in which case it must intersect M.

We now turn an affine plane into MOLS. Suppose we have an affine plane of order s, which can be conceived as constituting $s+1$ parallel classes $C_0, \ldots, C_s$ each with s points that we number from 1 to s. Let C_0 correspond to rows and C_s correspond to columns of our Latin square. To each of the coordinates (i, j), assign the unique point given by the intersection of the i-th line in the parallel class C_0 and the j-th line in the parallel class C_s. We have a bijection between points in our affine space and cells

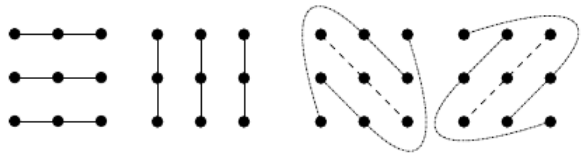
(i, j). Given any number $1 < \gamma < s - 1$, we fill the Latin square L_γ as follows: place the symbol y in the cell (i, j) if the line y of class C_γ contains the point identified with (i, j) earlier. Since every point is contained in some line of C_γ, this fills every cell, thus preserving our Latin square property, since any line from our C_γ class shows up in any row or any column exactly once by property A2. We have created $s - 1$ Latin squares by this process. Further, given any two such Latin squares, say L_α and L_β, and any two lines $a \in C_\alpha$, $b \in C_\beta$, we see that a and b intersect at exactly one point: i.e. there is exactly one cell in our square where L_α is a and L_β is b: every pair of symbols shows up exactly once through the whole series of $s - 1$ Latin squares thus proving that they are mutually orthogonal. □

Below is a pictorial representation of the above process:

1	2	3
3	1	2
2	3	1

1	2	3
2	3	1
3	1	2

(a) 3×3 MOLS



(b) Parallel classes for (a)

Figure 3-2: Affine Plane of order 3

Bringing all these results together, specifically theorems (3.13) and (3.10), we have showed that:

(a) The existence of an affine plane is equivalent to the existence of a projective plane;

(b) The existence of an affine plane is equivalent to the existence of a complete set of MOLS.

Chapter 4

Extensions

In this chapter, we shall formalise the construction of a BIBD from a set of $s-1$ MOLS where $s = 3$. It can be trivially seen that this method can be extended to $s-1$ MOLS with $s > 3$. In Chapter 3, we saw that the existence of an affine plane of order s was equivalent to the existence of a projective plane of the same order; this in turn was equivalent to the existence of a set of $s-1$ MOLS.

4.1 Constructing a BIBD from $s-1$ MOLS where $s = 3$

Supposing we had a set of 2 Latin squares of order $s = 3$ which were mutually orthogonal - the rightmost square is that of treatments. This is shown below:

A	B	C
B	C	A
C	A	B

A	B	C
C	A	B
B	C	A

0	1	2
3	4	5
6	7	8

Table 4.1: $s-1 = 2$ MOLS of order $s = 3$ and a treatment square.

We can construct a BIBD from the 2 MOLS by following the following rules:

(B1) Take the rows of the treatment square as blocks; one row per block

(B2) Take the columns of the treatment square as blocks; one column per block

(B3) Take each symbol from the $s-1$ MOLS (a Latin square at a time), and correspond it with the treatment at the same coordinate position in the treatment square. This creates additional blocks with their treatments.

The result of the above process is shown below:

Block	Treatments		
Block 1	0	1	2
Block 2	3	4	5
Block 3	6	7	8
Block 4	0	3	6
Block 5	1	4	7
Block 6	2	5	8
Block 7	0	5	7
Block 8	1	3	8
Block 9	2	4	6
Block 10	0	4	8
Block 11	2	3	7
Block 12	1	5	6

On closer inspection, the above rules correspond to the parallel classes of the affine plane that were shown in figure 3-2 in page 22. We now provide a less graphical description of the process.

4.2 A New look at the Parallel Classes of the Affine Plane of Prime Powers Order

Suppose we had a set of $s-1$ MOLS. Taking the key Latin square of this set of MOLS, we define a set of bijective maps $\mathcal{B}$ with $|\mathcal{B}| = s$ which map from the symbol set, $\mathcal{S} = \{A, B, C\}$, to the treatment space, $\mathcal{T} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, arranged to form a treatment square of the same dimensions as the Latin square. These bijective maps form a partition of the treatment space and are defined when the elements in a row or column of a key Latin square are mapped to the corresponding element in the treatment square. The bijective maps can be understood as a superimposition of the key Latin square to the treatment square. As for the remaining $s-2$ MOLS, these can be generated by definining an automorphism, Φ, on the set of bijective maps of the key Latin square.

4.2.1 Case of $s = 3$

In the case of $s = 3$, the set of bijective maps is described as follows:

$$\mathcal{B} = \{\alpha, \beta, \gamma\}$$

where

α: maps symbols of the first row/column
β: maps symbols of the second row/column
γ: maps symbols of the third row/column

We define the above bijective maps as the superimposition of the row-wise symbols of the first (key) MOL and the treatment square.

L_1		
A	B	C
C	A	B
B	C	A

$\mathcal{B}$		
α	α	α
β	β	β
γ	γ	γ

$\mathcal{T}$		
0	1	2
3	4	5
6	7	8

so that we have (row-wise):

Rows		
$\alpha(A) = 0$	$\alpha(B) = 1$	$\alpha(C) = 2$
$\beta(C) = 3$	$\beta(A) = 4$	$\beta(B) = 5$
$\gamma(B) = 6$	$\gamma(C) = 7$	$\gamma(A) = 8$

Columns		
$\alpha(A) = 0$	$\beta(C) = 3$	$\gamma(B) = 6$
$\alpha(B) = 1$	$\beta(A) = 4$	$\gamma(C) = 7$
$\alpha(C) = 2$	$\beta(B) = 5$	$\gamma(A) = 8$

To generate the remaining $s-2$ MOLS, we define a transformation, Φ, on $\mathcal{B}$, of which we compose with itself $s-2$ times. The bijection defined on the first row is invariant to the successive compositions of the transformation with itself. This transformation adds a different constant (mod s^2) to the images of the bijective maps in $\mathcal{B}$, and results in a new set of bijective maps, say $\mathcal{C}$, that are the partition of the treatment space, $\mathcal{T}$, as defined by the second Orthogonal Latin square in the set of MOLS. In the case of $s = 3$, the transformation is applied once to the set of bijective maps, $\mathcal{B}$ to define the mapping of the remaining Orthogonal Latin square.

This transformation, Φ, for the case of $s = 3$, is defined in the sequence of steps below:

(i) $\Phi(\alpha) = \alpha' = \{\alpha(b) : b \in \mathcal{S}\}$

(ii) $\Phi(\beta) = \beta' = \{(\beta(b) - 2 \times s)(mod\, s^2) : b \in \mathcal{S}\}$

(iii) $\Phi(\gamma) = \gamma' = \{(\gamma(b) - s)(mod\, s^2) : b \in \mathcal{S}\}$

Thus a first application of the transformation, Φ, on the set $\mathcal{B}$ simply generates

mappings of the second MOL to the treatment space, $\mathcal{C}$, defined as:

$$\mathcal{C} = \{\alpha, \beta', \gamma'\}$$

which are the superimposition of the symbols in the second MOL and the treatment square defined row-wise:

L_2		
A	B	C
B	C	A
C	A	B

$\mathcal{C}$		
α	α	α
β'	β'	β'
γ'	γ'	γ'

$\mathcal{T}$		
0	1	2
3	4	5
6	7	8

so that we have the new arrangement below (row-wise):

Rows		
$\alpha(A) = 0$	$\alpha(B) = 1$	$\alpha(C) = 2$
$\beta'(B) = 3$	$\beta'(C) = 4$	$\beta'(A) = 5$
$\gamma'(C) = 6$	$\gamma'(A) = 7$	$\gamma'(B) = 8$

Columns		
$\alpha(A) = 0$	$\beta'(B) = 3$	$\gamma'(C) = 6$
$\alpha(B) = 1$	$\beta'(C) = 4$	$\gamma'(A) = 7$
$\alpha(C) = 2$	$\beta'(A) = 5$	$\gamma'(B) = 8$

We have completed defining the set of bijective maps for the $s - 1 = 2$ MOLS of the Affine Plane of order $s = 3$. We now generate a BIBD from the above constructions:

Blocks	from $\mathcal{B}$ – L_1	Treatments	from $\mathcal{C}$ – L_2
Block 1	$\alpha(A), \alpha(B), \alpha(C)$	0, 1, 2	$\alpha(A), \alpha(B), \alpha(C)$
Block 2	$\beta(B), \beta(C), \beta(A)$	3, 4, 5	$\beta'(C), \beta'(A), \beta'(B)$
Block 3	$\gamma(C), \gamma(A), \gamma(B)$	6, 7, 8	$\gamma'(B), \gamma'(C), \gamma'(A)$
Block 4	$\alpha(A), \beta(C), \gamma(B)$	0, 3, 6	$\alpha(A), \beta'(B), \gamma'(C)$
Block 5	$\alpha(B), \beta(A), \gamma(C)$	1, 4, 7	$\alpha(B), \beta'(C), \gamma'(A)$
Block 6	$\alpha(C), \beta(B), \gamma(A)$	2, 5, 8	$\alpha(C), \beta'(A), \gamma'(B)$
Block 7	$\alpha(A), \beta(B), \gamma(C)$	0, 5, 7	$\alpha(A), \beta'(A), \gamma'(A)$
Block 8	$\alpha(B), \beta(C), \gamma(A)$	1, 3, 8	$\alpha(B), \beta'(B), \gamma'(B)$
Block 9	$\alpha(C), \beta(A), \gamma(B)$	2, 4, 6	$\alpha(C), \beta'(C), \gamma'(C)$
Block 10	$\alpha(A), \beta(A), \gamma(A)$	0, 4, 8	$\alpha(A), \beta'(C), \gamma'(B)$
Block 11	$\alpha(C), \beta(C), \gamma(C)$	2, 3, 7	$\alpha(C), \beta'(B), \gamma'(A)$
Block 12	$\alpha(B), \beta(B), \gamma(B)$	1, 5, 6	$\alpha(B), \beta'(A), \gamma'(C)$

From the above, we see that with a set of bijective maps, $\mathcal{B}$, that map from the symbol set, $\mathcal{S}$, of a Latin square of prime powers order $s = 3$ into a treatment set, say $\mathcal{T}$, to form a partition, we generated a BIBD by means of a transformation, Φ, defined on $\mathcal{B}$.

4.3 Further Examples

We now examine whether the method given in the above section holds for the case of $s = 8$ before we generalise it.

4.3.1 Case of $s = 8$

In the case of $s = 8$, we define the symbol set, $\mathcal{S} = \{A, B, C, D, E, F, G, H\}$, the elements are from $GF(2^3)$, and we have the irreducible polynomial $\psi(x) = x^3 + x^2 + 1$,

i.e. we have

$$ax + b \qquad (\text{mod } x^3 + x^2 + 1), \quad (a, b \in \text{GF}(2)).$$

We have

$$\begin{aligned} & \psi(x) = x^3 + x^2 + 1 = 0 \\ \Longrightarrow \qquad & x^3 = -x^2 - 1 + (2x^2 + 2) = x^2 + 1 \qquad (\text{mod } 2). \end{aligned}$$

The elements of $\mathcal{S}$ are defined as shown below:

$$\begin{aligned} & A = 0,\ B = 1,\ C = x,\ D = x^2,\ E = x^3 = x^2 + 1 \\ & F = x^4 = x(x^3) = x(x^2 + 1) = x^3 + x = x^2 + x + 1, \\ & G = x^5 = x(x^4) = x(x^2 + x + 1) = x^2 + 1 + x^2 + x = x + 1, \\ & H = x^6 = x(x + 1) = x^2 + x \end{aligned}$$

With the above symbols defined as polynomials, We now generate the key Latin square, L_1, for $s = 8$:

1. **Row 1**: Add 0 to each element of $\mathcal{S}$, to arrive at a column element in turn.

2. **Row 2**: Add 1 to each element of $\mathcal{S}$, to arrive at a column element in turn.

3. **Row 3**: Add x to each element of $\mathcal{S}$, to arrive at a column element in turn.

4. **Row 4**: Add x^2 to each element of $\mathcal{S}$, to arrive at a column element in turn.

5. **Row 5**: Add $x^2 + 1$ to each element of $\mathcal{S}$, to arrive at a column element in turn.

6. **Row 6**: Add $x^2 + x + 1$ to each element of $\mathcal{S}$, to arrive at a column element in turn.

7. **Row 7**: Add $x + 1$ to each element of $\mathcal{S}$, to arrive at a column element in turn.

8. **Row 8**: Add $x^2 + x$ to each element of $\mathcal{S}$, to arrive at a column element in turn.

which results in the key Latin square, L_1 below (the treatment square is given alongside it):

A	B	C	D	E	F	G	H
B	A	G	E	D	H	C	F
C	G	A	H	F	E	B	D
D	E	H	A	B	G	F	C
E	D	F	B	A	C	H	G
F	H	E	G	C	A	D	B
G	C	B	F	H	D	A	E
H	F	D	C	G	B	E	A

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

We now define a set of bijective maps,

$$\mathcal{B} = \{\alpha, \beta, \gamma, \epsilon, \zeta, \eta, \theta, \iota\}$$

where they are the superimposition of the symbols of L_1 in every row to the corresponding treatments in the treatment square:

α: the first row β: the second row γ: the third row ϵ: the fourth row
ζ: the fifth row η: the sixth row θ: the seventh row ι: the eighth row

We now define a transformation, Φ, on the set of bijective maps, $\mathcal{B}$:

$$\Phi(\alpha) = \alpha,\ \Phi(\beta) = \beta',\ \Phi(\gamma) = \gamma',\ \Phi(\epsilon) = \epsilon',\ \Phi(\zeta) = \zeta',\ \Phi(\eta) = \eta',\ \Phi(\theta) = \theta',\ \Phi(\iota) = \iota'$$

We define the successive compositions of the transformation with itself as successively adding the row-wise constants (mod s^2) to the images of the bijective maps in the set $\mathcal{B}$, but with α being invariant to any number of compositions of the transformation with itself, as exemplified below for the case of $s = 8 = 2^3$ (we use the super-script notation to indicate the number of compositions of the transformation):

$(\Phi \circ \Phi)(\alpha) = \alpha$ $(\Phi \circ \Phi \circ \Phi)(\alpha) = \alpha$ $(\Phi \circ \Phi \circ \Phi \circ \Phi)(\alpha) = \alpha$ $(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi)(\alpha) = \alpha$

$(\Phi \circ \Phi)(\beta) = \beta^{(2)}$ $(\Phi \circ \Phi \circ \Phi)(\beta) = \beta^{(3)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi)(\beta) = \beta^{(4)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi)(\beta) = \beta^{(5)}$

$(\Phi \circ \Phi)(\gamma) = \gamma^{(2)}$ $(\Phi \circ \Phi \circ \Phi)(\gamma) = \gamma^{(3)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi)(\gamma) = \gamma^{(4)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi)(\gamma) = \gamma^{(5)}$

$(\Phi \circ \Phi)(\epsilon) = \epsilon^{(2)}$ $(\Phi \circ \Phi \circ \Phi)(\epsilon) = \epsilon^{(3)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi)(\epsilon) = \epsilon^{(4)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi)(\epsilon) = \epsilon^{(5)}$

$(\Phi \circ \Phi)(\zeta) = \zeta^{(2)}$ $(\Phi \circ \Phi \circ \Phi)(\zeta) = \zeta^{(3)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi)(\zeta) = \zeta^{(4)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi)(\zeta) = \zeta^{(5)}$

$(\Phi \circ \Phi)(\eta) = \eta^{(2)}$ $(\Phi \circ \Phi \circ \Phi)(\eta) = \eta^{(3)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi)(\eta) = \eta^{(4)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi)(\eta) = \eta^{(5)}$

$(\Phi \circ \Phi)(\theta) = \theta^{(2)}$ $(\Phi \circ \Phi \circ \Phi)(\theta) = \theta^{(3)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi)(\theta) = \theta^{(4)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi)(\theta) = \theta^{(5)}$

$(\Phi \circ \Phi)(\iota) = \iota^{(2)}$ $(\Phi \circ \Phi \circ \Phi)(\iota) = \iota^{(3)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi)(\iota) = \iota^{(4)}$ $(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi)(\iota) = \iota^{(5)}$

$$\begin{array}{ll}
\big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\alpha) = \alpha & \big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\alpha) = \alpha \\
\big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\beta) = \beta^{(6)} & \big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\beta) = \beta^{(7)} \\
\big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\gamma) = \gamma^{(6)} & \big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\gamma) = \gamma^{(7)} \\
\big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\epsilon) = \epsilon^{(6)} & \big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\epsilon) = \epsilon^{(7)} \\
\big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\zeta) = \zeta^{(6)} & \big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\zeta) = \zeta^{(7)} \\
\big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\eta) = \eta^{(6)} & \big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\eta) = \eta^{(7)} \\
\big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\theta) = \theta^{(6)} & \big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\theta) = \theta^{(7)} \\
\big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\iota) = \iota^{(6)} & \big(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi\big)(\iota) = \iota^{(7)}
\end{array}$$

From above it is clear that

$$(\Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi \circ \Phi) = \Phi^{(0)}.$$

We now set out to create a BIBD. The process is first shown below then the blocks later. We generate the:

(i) first set of 8 (block 1 to block 8) from the row-wise parallel classes of L_1

(ii) second set of 8 blocks (block 9 to block 16) arising from the column-wise parallel classes of L_1

(iii) third set of 8 blocks (block 17 to block 24) from the parallel classes joining the symbols of L_1, the key Latin square (or $\Phi^{(0)}$):

(iv) fourth set of 8 blocks (block 25 to block 32) from the parallel classes joining the symbols of L_2 (or $\Phi^{(1)}$)

(v) fifth set of 8 blocks (block 33 to block 40) from the parallel classes joining the symbols of L_3 (or $\Phi^{(2)}$)

(vi) sixth set of 8 blocks (block 41 to block 48) from the parallel classes joining the symbols of L_4 (or $\Phi^{(3)}$)

(vii) seventh set of 8 blocks (block 49 to block 56) from the parallel classes joining the symbols of L_5 (or $\Phi^{(4)}$)

(viii) eighth set of 8 blocks (block 57 to block 64) from the parallel classes joining the symbols of L_6 (or $\Phi^{(5)}$)

(ix) ninth set of 8 blocks (block 65 to block 72) from the parallel classes joining the symbols of L_7 (or $\Phi^{(6)}$)

Blocks	Operation	Treatments
1	$(\alpha)(\mathcal{B})$	0 1 2 3 4 5 6 7
2	$(\beta)(\mathcal{B})$	8 9 10 11 12 13 14 15
3	$(\gamma)(\mathcal{B})$	16 17 18 19 20 21 22 23
4	$(\epsilon)(\mathcal{B})$	24 25 26 27 28 29 30 31
5	$(\zeta)(\mathcal{B})$	32 33 34 35 36 37 38 39
6	$(\eta)(\mathcal{B})$	40 41 42 43 44 45 46 47
7	$(\theta)(\mathcal{B})$	48 49 50 51 52 53 54 55
8	$(\iota)(\mathcal{B})$	56 57 58 59 60 61 62 63

Blocks	Operation	Treatments
9	$\alpha(A)\beta(B)\gamma(C)\epsilon(D)\zeta(E)\eta(F)\theta(G)\iota(H)$	0 8 16 24 32 40 48 56
10	$\alpha(B)\beta(A)\gamma(G)\epsilon(E)\zeta(D)\eta(H)\theta(C)\iota(F)$	1 9 17 25 33 41 49 57
11	$\alpha(C)\beta(G)\gamma(A)\epsilon(H)\zeta(F)\eta(E)\theta(B)\iota(D)$	2 10 18 26 34 42 50 58
12	$\alpha(D)\beta(E)\gamma(H)\epsilon(A)\zeta(B)\eta(G)\theta(F)\iota(C)$	3 11 19 27 35 43 51 59
13	$\alpha(E)\beta(D)\gamma(F)\epsilon(B)\zeta(A)\eta(C)\theta(H)\iota(G)$	4 12 20 28 36 44 52 60
14	$\alpha(F)\beta(H)\gamma(E)\epsilon(G)\zeta(C)\eta(D)\theta(D)\iota(B)$	5 13 21 29 37 45 53 61
15	$\alpha(G)\beta(C)\gamma(B)\epsilon(F)\zeta(H)\eta(D)\theta(A)\iota(E)$	6 14 22 30 38 46 54 55
16	$\alpha(H)\beta(F)\gamma(D)\epsilon(C)\zeta(G)\eta(B)\theta(E)\iota(A)$	7 15 23 31 39 47 55 63

Blocks	Operation	Treatments	Blocks	Operation	Treatments
17	$(\Phi^{(0)}(\mathcal{B}))(A)$	0 9 18 27 36 45 54 63	25	$(\Phi^{(1)}(\mathcal{B}))(A)$	0 10 19 28 37 46 55 57
18	$(\Phi^{(0)}(\mathcal{B}))(B)$	1 8 22 28 35 47 50 61	26	$(\Phi^{(1)}(\mathcal{B}))(B)$	1 14 20 27 39 42 53 56
19	$(\Phi^{(0)}(\mathcal{B}))(C)$	2 14 16 31 37 44 49 59	27	$(\Phi^{(1)}(\mathcal{B}))(C)$	2 8 23 29 36 41 51 62
20	$(\Phi^{(0)}(\mathcal{B}))(D)$	3 12 23 24 33 46 53 58	28	$(\Phi^{(1)}(\mathcal{B}))(D)$	3 15 16 25 38 45 50 60
21	$(\Phi^{(0)}(\mathcal{B}))(E)$	4 11 21 25 32 42 55 62	29	$(\Phi^{(1)}(\mathcal{B}))(E)$	4 13 17 24 34 47 54 59
22	$(\Phi^{(0)}(\mathcal{B}))(F)$	5 15 20 30 34 40 51 57	30	$(\Phi^{(1)}(\mathcal{B}))(F)$	5 12 22 26 32 43 49 63
23	$(\Phi^{(0)}(\mathcal{B}))(G)$	6 10 17 29 39 43 48 60	31	$(\Phi^{(1)}(\mathcal{B}))(G)$	6 9 21 31 35 40 52 58
24	$(\Phi^{(0)}(\mathcal{B}))(H)$	7 13 19 26 38 41 52 56	32	$(\Phi^{(1)}(\mathcal{B}))(H)$	7 11 18 30 33 44 48 61

Blocks	Operation	Treatments	Blocks	Operation	Treatments
33	$(\Phi^{(2)}(\mathcal{B}))(A)$	0 11 20 29 38 47 49 48	41	$(\Phi^{(3)}(\mathcal{B}))(A)$	0 12 21 30 39 41 50 59
34	$(\Phi^{(2)}(\mathcal{B}))(B)$	1 12 19 31 34 45 48 62	42	$(\Phi^{(3)}(\mathcal{B}))(B)$	1 11 23 26 37 40 54 60
35	$(\Phi^{(2)}(\mathcal{B}))(C)$	2 15 21 28 33 43 54 56	43	$(\Phi^{(3)}(\mathcal{B}))(C)$	2 13 20 25 35 46 48 63
36	$(\Phi^{(2)}(\mathcal{B}))(D)$	3 8 17 30 37 42 52 63	44	$(\Phi^{(3)}(\mathcal{B}))(D)$	3 9 22 29 34 44 55 56
37	$(\Phi^{(2)}(\mathcal{B}))(E)$	4 9 16 26 39 46 51 61	45	$(\Phi^{(3)}(\mathcal{B}))(E)$	4 8 18 31 38 43 53 57
38	$(\Phi^{(2)}(\mathcal{B}))(F)$	5 14 18 24 35 41 55 60	46	$(\Phi^{(3)}(\mathcal{B}))(F)$	5 10 16 27 33 47 52 62
39	$(\Phi^{(2)}(\mathcal{B}))(G)$	6 13 23 27 32 44 50 57	47	$(\Phi^{(3)}(\mathcal{B}))(G)$	6 15 19 24 36 42 49 61
40	$(\Phi^{(2)}(\mathcal{B}))(H)$	7 10 22 25 36 40 53 59	48	$(\Phi^{(3)}(\mathcal{B}))(H)$	7 14 17 28 32 45 51 58

Blocks	Operation	Treatments	Blocks	Operation	Treatments
49	$(\Phi^{(4)}(\mathcal{B}))(A)$	0 13 22 31 33 42 51 60	57	$(\Phi^{(5)}(\mathcal{B}))(G)$	0 14 23 25 34 43 52 61
50	$(\Phi^{(4)}(\mathcal{B}))(B)$	1 15 18 29 32 46 52 59	58	$(\Phi^{(5)}(\mathcal{B}))(B)$	1 10 21 24 38 44 51 63
51	$(\Phi^{(4)}(\mathcal{B}))(C)$	2 12 17 27 38 40 55 61	59	$(\Phi^{(5)}(\mathcal{B}))(C)$	2 9 19 30 32 47 53 60
52	$(\Phi^{(4)}(\mathcal{B}))(D)$	3 14 21 26 36 47 48 57	60	$(\Phi^{(5)}(\mathcal{B}))(D)$	3 13 18 28 39 40 49 62
53	$(\Phi^{(4)}(\mathcal{B}))(E)$	4 10 23 30 35 45 49 56	61	$(\Phi^{(5)}(\mathcal{B}))(E)$	4 15 22 27 37 41 48 58
54	$(\Phi^{(4)}(\mathcal{B}))(F)$	5 8 19 25 39 44 54 58	62	$(\Phi^{(5)}(\mathcal{B}))(F)$	5 11 17 31 36 46 50 56
55	$(\Phi^{(4)}(\mathcal{B}))(G)$	6 11 16 28 34 41 53 63	63	$(\Phi^{(5)}(\mathcal{B}))(G)$	6 8 20 26 33 45 55 59
56	$(\Phi^{(4)}(\mathcal{B}))(H)$	7 9 20 24 37 43 54 62	64	$(\Phi^{(5)}(\mathcal{B}))(H)$	7 12 16 29 35 42 54 57

Blocks	Operation	Treatments
65	$(\Phi^{(6)}(\mathcal{B}))(A)$	0 15 17 26 35 44 53 62
66	$(\Phi^{(6)}(\mathcal{B}))(B)$	1 13 16 30 36 43 55 58
67	$(\Phi^{(6)}(\mathcal{B}))(C)$	2 11 22 24 39 45 52 57
68	$(\Phi^{(6)}(\mathcal{B}))(D)$	3 10 20 31 32 41 54 61
69	$(\Phi^{(6)}(\mathcal{B}))(E)$	4 14 19 29 33 40 50 63
70	$(\Phi^{(6)}(\mathcal{B}))(F)$	5 9 23 28 38 42 48 59
71	$(\Phi^{(6)}(\mathcal{B}))(G)$	6 12 18 25 37 47 51 56
72	$(\Phi^{(6)}(\mathcal{B}))(H)$	7 8 21 27 34 46 49 60

Chapter 5

Conclusions & Recommendations

In Chapter 2, Section 2.2 Literature Review, Tang (2009) mentioned that Latin squares were a relatively unknown aspect of Mathematics. We take this to infer that there appears to be a dearth of foundational work concerning Latin squares, yet, they have so far proved quite applicable in many real-life problems.

This project has resulted in a new look at the relationships between Finite Geometries, Latin squares and Balanced Incomplete Block Designs (BIBDs). The result of Chapter 4 showed that:

> The existence of a affine plane of prime powers order, s, implies the existence of a set of mutually orthogonal Latin squares (MOLS) of the same order, a treatment square of side equal to the prime powers order, a set of bijective maps, $\mathcal{B}$, defined on the key Latin square into the treatment space, $\mathcal{T}$, and a transformation, Φ, defined on the set of bijective maps that generates $s-2$ new sets of bijective maps that relate the $s-2$ remaining MOLS to the treatment square.

We now review the work of earlier chapters:

- Chapter 1 opened with a discussion on the subject of Experimental Designs, the problem statement, objectives and significance of the study. A general outline

of this document was also presented.

- Chapter 2 was a survey of important definitions, theorems, corollaries that helped to lay a foundation for the later work. The literature review was also provided in this chapter.

- Chapter 3 was a discussion on the relationships between MOLS, Finite Fields, Latin squares and Finite Geometries. This was supposed to show the equivalence in existence of Finite Geometries of prime powers order and sets of mutually orthogonal Latin squares of the same order. The Finite (Galois) fields were a tool used to construct the Latin squares as first developed by Bose (1938).

- Chapter 4 further extended the work of constructing MOLS from a key Latin square by proposing a set of bijective maps that corresponded with the superimposition of the key Latin square to the treatment square and a transformation operation on this set of bijective maps to produce new sets bijective maps that corresponded to the superimposition of the remaining MOLS to the treatment square. This resulted in a more algorithmic comprehension of the process.

5.1 Challenges Encountered

Algebra, was my single largest challenge. There has not been sufficient coverage of this important area of Mathematics in my past training and I had to read through various texts to gain sufficient understanding that could help me relate certain important concepts from Algebra. All the same this was so rewarding and I ended up loving Algebra.

There was also not much work, in the form of research papers, accessible to me since most research papers appeared to be locked-for-sale in some important journals. My budget could not accommodate such expenditures and I had to make do with what I had.

5.2 Further Work

There's a lot that needs to be done, for instance:

- What are the classes of BIBDs that arise from Affine planes of prime powers order? (and are there classes of BIBDs that don't?)
- What other designs could arise from the Affine planes of prime powers order?
- Provide an implementation of the process of Chapter 4 in a high-level language.

5.3 Concluding Remarks

SOLI DEO GLORIA

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A

Proofs

Proof. **(Proof of Theorem** (2.3)**)** Let $(X, \mathcal{A})$ be a (ν, k, λ)-BIBD. Suppose $x \in X$, and let r_x denote the number of blocks containing x. Define a set

$$I = \{(y, A) | y \in X, y \neq x, A \in \mathcal{A}, \{x, y\} \in A\}.$$

$|I|$ can be computed in two different ways: First, there are $\nu - 1$ different ways to choose $y \in X$ such that $y \neq x$. For each such $y \in X$, there are λ blocks A such that $\{x, y\} \subset A$. Hence

$$|I| = \lambda(\nu - 1)$$

There are r_x ways to choose a block A such that $x \in A$. For each choice of A, there are $k - 1$ ways to choose $y \in A$, $y \neq x$. Hence

$$|I| = r_x(k - 1)$$

but r_x is independent of x i.e. $r_x \equiv r$, and thus bringing the two results above together we have

$$r(k - 1) = \lambda(\nu - 1)$$

□

Proof. **(Proof of Theorem** (2.4)**)** Let $(X, \mathcal{A})$ be a (ν, k, λ)-BIBD, and let $b = |\mathcal{A}|$. Define a set

$$I = \{(x, A) | x \in X, A \in \mathcal{A}, x \in A\}.$$

$|I|$ can be computed in two different ways: First, there are ν ways to choose $x \in X$. For each such x, there are r blocks A such that $x \in A$. Hence,

$$|I| = \nu r.$$

On the other hand, there are b ways to choose a block $A \in \mathcal{A}$, and for each choice of A there are k ways to choose $x \in A$. Hence,

$$|I| = bk.$$

Bringing the two results together we have

$$bk = \nu r$$

□

Proof. **(Proof of Theorem** (2.7)**)** Suppose $(X, \mathcal{A})$ is a (ν, k, λ)-BIBD, where $X = \{x_1, \ldots, x_\nu\}$ and let $\mathcal{A} = \{A_1, \ldots, A_b\}$. Let M be it's incidence matrix. The (i, j)-entry of MM^T is

$$\sum_{h=1}^{b} m_{i,h} m_{j,h} = \begin{cases} r & , i = j \\ \lambda & , i \neq j. \end{cases}$$

Thus all entries along the principle diagonal of MM^T is r and it's off-diagonal elements are λ, thus

$$MM^T = rJ_\nu + (r - \lambda)I_\nu.$$

Furthermore, the ith entry of $u_\nu M$ is the number of 1's in column i of M, which is k, hence

$$u_\nu M = ku_b.$$

Conversely, suppose that M is the incidence matrix of a design $(X, \mathcal{A})$ such that $MM^T = rJ_\nu + (r-\lambda)I_\nu$ and $u_\nu M = ku_b$. Clearly, $|X| = \nu$ and $|\mathcal{A}| = b$ and from $u_\nu M = ku_b$ we see that every block in $\mathcal{A}$ has k points, and from $MM^T = rJ_\nu + (r-\lambda)I_\nu$, every pair of points occurs in exactly λ blocks, and every point occurs in r blocks. Hence, $(X, \mathcal{A})$ is a (ν, b, r, k, λ)-BIBD. □

Proof. **(Proof of Theorem** (2.11)**)** Suppose that $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ have $M_{\nu\times b}$ and $N_{\nu\times b}$ incidence matrices respectively and that $X = \{x_1, \ldots, x_\nu\}$, $Y = \{y_1, \ldots, y_\nu\}$, $\mathcal{A} = \{A_1, \ldots, A_b\}$ and $\mathcal{B} = \{B_1, \ldots, B_b\}$. Further, suppose that $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ are isomorphic. Then there exists a bijection $\alpha : X \to Y$ such that $[\{\alpha(x) : x \in A\} : A \in \mathcal{A}] = \mathcal{B}$. We define

$$\gamma(i) = j \text{ iff } \alpha(x_i) = y_j \quad \text{for } 1 \le i \le \nu$$

Since α is a bijection of X and Y, it follows that γ is a permutation of $\{1, \ldots, \nu\}$. Next, there exists a permutation β of $\{1, \ldots, b\}$ with the property

$$\{\alpha(x) : x \in A_j\} = B_{\beta(j)} \quad \text{for } 1 \le j \le b$$

and such a permutation exists because α is an isomorphism of the two designs $(X, \mathcal{A})$ and $(Y, \mathcal{B})$. Thus

$$\begin{aligned} m_{i,j} = 1 &\iff x_i \in A_j \\ &\implies y_{\gamma(i)} \in B_{\beta(j)} \\ &\iff n_{\gamma(i),\beta(j)} = 1. \end{aligned}$$

Conversely, suppose we have permutations γ and β such that $m_{i,j} = n_{\gamma(i),\beta(j)}$ for all i, j. Define $\alpha : X \to Y$ by the rule

$$\alpha(x_i) = y_j \text{ iff } \gamma(i) = j$$

The it is easily seen that

$$\{\alpha(x) : x \in A_j\} = B_{\beta(j)} \quad \text{for } 1 \leq j \leq b.$$

Hence, α defines an isomorphism between the two designs $(X, \mathcal{A})$ and $(Y, \mathcal{B})$. $\square$

Bibliography

Arshaduzzaman, M. (2014). Connections between latin squares and geometries. *IOSR Journal of Mathematics (IOSR-JM)*, 9(5):14–19. e-ISSN: 2278-5728, p-ISSN:2319-765X.

Beachy, J. A. and Blair, W. D. (2005). *Abstract Algebra*. Waveland Press, Inc., Long Grove, IL, third edition.

Bose, R. C. (1938). On the application of the properties of galois fields to the problem of construction of hyper-graeco-latin squares. *SANKHYA, THE INDIAN JOURNAL OF STATISTICS*, 3(4):323–338. Edited by : P. C. MAHALANOBIS.

Fraleigh, J. B. (2002). *A First Course in Abstract Algebra*. Pearson, seventh edition.

Pachamuthu, M. (2011). Construction of (3^2) mutually orthogonal latin square and check parameter relationship of balanced incomplete block design. *Int. J. of Mathematical Sciences and Applications*, 1(2):911–922. Mind Reader Publications.

Stinson, R. D. (2004). *Combinatorial Designs: Constructions and Analysis*. Springer.

Tang, J. (2009). Latin squares and their applications. Technical report, University of Queensland.

Vanpoucke, J́. (2011–2012). Mutually orthogonal latin squares and their generalizations. Master's thesis, Ghent University, Faculty of Sciences, Department of Mathematics.