INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Mathematics using the construction of designs

S. Kolanchinathan
sknathan100@gmail.com
PRIST Deemed University, Thanjavur, Tamil Nadu

Dr. R.Balakumar
balaphdmaths@gmail.com
PRIST Deemed University, Thanjavur, Tamil Nadu

ABSTRACT

Statistics is defined as the science of collection, presentation analysis and interpretation of numerical data. The field is divided into small plots of the same size and the same treatments are applied to all the plots and the yield in each plot is noted. This enables one to divide the field into relatively homogeneous subgroups is called block of equal fertility to control the experimental error. Additional points (or) lines to supplement geometrical figures so as to prove some property of the figure are called constructions.

Keywords: *Galois field, Finite projective, Euclidean geometry, Black designs*

1. INTRODUCTION

Statistics is concerned with scientific methods for collecting, organizing, summarizing presenting and analyzing data as well as the basis of such analysis.

Mathematical statistics covers some of the topics of applied statistics. Analysis of variance and design of Experiments, Economic statistics and time series industrial statistics, vital statistics and Demography, a statistical method in psychometry and Educational statistics.

Construction is geometric with a clear link to mathematics. Buildings, bridges, furniture, vehicles they all have a unique shape. In controlled experiments, we have a limited number of experimental units which respond to a certain kind of treatments and on the basis experiments, we are to compare the response produced by different treatments. The allocation of treatments to units depends on the choice of the experiments.

GALOIS FIELD

A field F is a set of more than one element for which there are defined operations of additions and multiplications which satisfy the following laws:

i. Commutative Law:

$$a + b = b + a$$
$$a.b = b.a$$

ii. Associative Law:

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

iii. Distributive Law:

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

iv. Every pair (a,b) there exists an y such that y + a = b,

v. Every pair (a,b) for which a $\neq$ o, there exists an z such that

$$za = b.$$

DEFINITION: 1

A commutative skew field is called a **field**. In other words, a field is a system (F, +, .) satisfying the following conditions,

(i) (F, +) is an abelian group.

(ii) $\left(F-\{0\},.\right)$ is an abelian group.

(iii) $a. \quad (b+c)=a\ .\ b+a\ .\ c$ For all a, b, c $\in$ F.

DEFINITION: 2

A collection of well-defined objects is called **set**.

DEFINITION: 3

A ring R is said to be **commutative** if a.b = b.a for all a, b $\in$ R.

DEFINITION: 4

A positive integer p > 1 is called **prime**. If and only if positive factors of p and p is a positive integer >1 and is not prime is called **composite**.

DEFINITION: 5

Let p be a prime and let g.c.d (a, p) = 1 is $x^2 \equiv a(\text{mod } p)$ has a solution. If 'a' is a quadratic residue **modulo p**.

DEFINITION: 6

Let R be a ring. A polynomial $f(x)$ with coefficients in R is defined to be an expression of the form $a_0+a_1x+\cdots+a_nx^n$.

Where n is a positive integer and $a_0, a_1 \cdots a_n \in R$, a_n is called the co-efficient of x^n and $a_n\ x^n$ is called the term of the **polynomial**.

DEFINITION: 7

The polynomial $f(x)$ = $a_0+a_1x+\cdots+a_nx^n$ where the coefficients a_i are the integers said to be **primitive** if the g.c.d of the coefficients $a_0, a_1 \cdots a_n$ is 1.

DEFINITION: 8

A polynomial $P(x)$ in $F[x]$ is said to be **irreducible** over F.

Whenever $P(x)=a(x).b(x)$ with $a(x)$, $b(x)\in F[x]$. Then one of $a(x)$ (or) $b(x)$ has degree 0.

DEFINITION: 9

If g is an integer belonging to the exponent $\phi(m)$ modulo m, then g is called a **primitive root** modulo m.

DEFINITION: 10

A population may be finite (or) infinite according to as the number of observations (or) items in it is **Finite (or) infinite.**

DEFINITION: 11

If V is a vector space and if $v_1, v_2, \cdots, v_n$ are in V, they are **linearly dependent** over F. if there exist elements $\lambda_1, \lambda_2, \cdots, \lambda_n$ in F, not all of them 0, such that,

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$$

If the vectors $v_1, v_2, \cdots, v_n$ are not linearly dependent over F, they are said to be **linearly independent** over F.

DEFINITION: 12

Let v be a vector space over a field F. A no-empty subset W of v is called a **subspace** of v if W itself is a vector space over F under the operations of v.

DEFINITION: 13

A square matrix A is said to be **singular** if $|A| = 0$.

DEFINITION: 14

A square matrix A is called a **non – singular** if $|A| \neq 0$.

DEFINITION: 15

A square matrix $A = (a_{ij})$ is said to be **symmetric** if $a_{ij} = a_{ji}$ for all i, j.

DEFINITION: 16

Let v be an inner product space and let $x, y \in V,$ x is said to be **orthogonal** to y. if (x , y) = 0.

DEFINITION: 17

Let v be an inner product space. A set S of vectors in v is said to be an **orthogonal set** if any two distinct vectors is s are orthogonal.

DEFINITION: 18

Let A and B are non - empty sets. A function or a **mapping** f from A into B written an f: A $\rightarrow$ B is a rule which assigns to each element $a \in A$ a unique element $b \in B$.

DEFINITION: 19

Let a and b are two integers with $a \neq 0$. If a divides b then a is called a **divisor** of a factor of b.

DEFINITION: 20

The **intersection** of two sets A and B denoted by $A \cap B$ is the set of elements that belong to both A and B.

$$A \cap B = \{x / x \in A \text{ and } x \in B\}.$$

A field containing a finite number of elements is called a **Galois Field** and is denoted by GF(s). A Galois Field can always be constructed when $s = p^n,$ where p is a prime and n is a positive integer. When n=1, the residue classes modulo p constitute GF (p). In general, the elements of GF$\left(p^n\right)$ can be constructed.

We can divide $x^{p^n-1} - 1$ by the least common multiple of all the factors $x^t - 1$ in which t is a divisor of $p^n - 1$ $(t \neq p^n - 1)$ and represent all the coefficients of the resultant polynomial by their smallest positive residues (mod p) the cyclotomic polynomial corresponding to GF (p^n).

An irreducible factor of this cyclotomic polynomial is called a **minimum function** $P(x)$. A minimum function is not necessarily unique. A minimum function can be used to generate the elements of GF (p^n). Let F (x) be any polynomial in x with integer coefficients.

$$\text{Let, f}(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \longrightarrow \quad \textbf{(1)}$$

with integer coefficients $a_i (i = 0, 1, \ldots, n-1)$ that are elements of GF(p). The function F (x) can be written in the form

$$\text{F}(x) = \text{f}(x) + \text{p.q}(x) + \text{p}(x).\ \text{Q}(x) \longrightarrow \quad \textbf{(2)}$$

Where, q (x) and Q (x) are any functions of x. We write

$$\text{F}(x) = \text{f}(x)\ (\text{mod p, P}(x)) \longrightarrow \quad \textbf{(3)}$$

If f (x) is the residue of F (x) modulus p and P (x). If f (x), p and P (x) are fixed function F (x) that satisfy equation (3) form a class. If p and P (x) are fixed and f (x) is allowed to take all possible values we get p^n classes. Since each coefficient, $a_{n\,i}$ in f (x) can take p values of GF (p). It can be seen that these p^n classes form a Galois Field if and only if P (x) is a minimum function of GF (p^n) and p is prime.

$F(x)$ = 0, $x^0, x^1 .... x^{p^n-2}$, and find corresponding polynomials $f(x)$ in equation (3). These polynomials form elements of $GF(p^n)$.

The elements of $GF(p^n)$ can also be written as $0, x^0, x, x^2, \ldots, x^{p^n-2}$, where x is a primitive root of the equation.

$$x^{p^n-1} - 1 \;= 0 \qquad \longrightarrow \qquad \textbf{(4)}$$

The quantity x is a primitive root of equation (4) if x is a root of (4) but $x^t \neq 1$ (always) for all divisors t of $p^n - 1$. GF (3). We divide $x^2 - 1$ by x – 1 (because the only divisor of 2 is 1) to get the cyclotomic polynomial

$$x^2 - 1 = (x + 1)\,(x - 1)$$

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

This is also the minimum function P (x). The 3 elements of GF (3) are.

$$\alpha = 0$$
$$\alpha_1 = x^0 = 1$$
$$\alpha_2 = x = (x+1) - 1 = 2$$

Hence the elements are 0,1,2. GF (2^2). We divide $x^3 - 1$ by $x - 1$ (because the only divisor of 3 is 1) to get the cyclotomic polynomial

$$x^3 - 1 = (x^2 + x + 1)(x - 1)$$
$$\frac{x^3-1}{x-1} = x^2 + x + 1$$

Which is also the minimum function.

The elements of GF (2^2) are 0,1, x, x^2 = – (x +1) =(x +1).

FINITE PROJECTIVE

Let s = p^h where p is a prime and h an integer. Every order set $x = (x_0, x_1, ..., x_n)$ of (n+1) elements from the GF(s), where at least one of x_i (i=0,1,2,…,n) ≠ 0 is called a **point in finite projective geometry PG(n,s),** (n+1) ≤ s.

The two points x and y = $(y_0, y_1, ..., y_n)$ in PG (n, s) are identical if and only if $y_i = qx_i$ (i = 0,1,…,n) for any q (≠ 0) ∈ GF(s) . The elements x_i (i=0,1,2,…n) of x are called the **co-ordinates of x .**

All points x of a PG (n,s) which satisfy (n – m) linearly independent homogeneous equations.

$$\sum_{i=0}^{n} a_{ji} x_i = 0, \quad j = 1, \cdots, n-m, \quad a_{ji} \in GF(s) \qquad \longrightarrow \qquad \textbf{(5)}$$

Form an **m - dimensional subspace** or a **m - flat in PG (n, s).**

Subspaces of PG (n, s) in which $x_0 = 0$ are called subspaces at **infinity.** Points of P (n, s) for which $x_0 = 0$ are called points at infinity. All other points of PG (n, s) are called **finite points**.

Then there exists a finite projective geometry PG (n, s). The number of different points in PG (n, s) is

$$P_n = \frac{s^{n+1}-1}{s-1} \longrightarrow \quad \textbf{(6)}$$

The number of points in an m- dimensional subspace of PG (n, s) is

$$P_m = \frac{s^{m+1}-1}{s-1} \longrightarrow \quad \textbf{(7)}$$

The number of m- dimensional subspaces of a PG (n, s) is

$$\phi(n,m,s) = \frac{(s^{n+1}-1)(s^{n+2}-1)...(s^{n-m+1}-1)}{(s^{m+1}-1)(s^{m}-1)...(s-1)} \quad (m \geq 0, n \geq m) \longrightarrow \quad \textbf{(8)}$$

If q ($\neq$ 0) be an element of GF(s), then ($x_0, x_1, ...x_n$) and ($qx_0, qx_1...qx_n$). Thus there are $\frac{s^{n+1}-1}{(s-1)}$ different points in PG (n, s). Again a m-flat is generated by the points x which satisfy equations

$$\mathbf{A}\, x\ \mathbf{= 0} \longrightarrow \quad \textbf{(9)}$$

Where A = (a_{ji}). A particular solution of the equation (9) is obtained by assigning a set of arbitrary values to $(x_{n-m},...,x_n)$ when the matrix of the coefficients of the remaining co-ordinates $(x_0, x_1,..., x_{n-m-1})$ is non-singular and then solving the resulting equations for $(x_0, x_1,..., x_{n-m-1})$.

The number of different possible values of $(x_{n-m},...,x_n)$ is $\frac{s^{m+1}-1}{(s-1)}$ values subject to the restriction that, $x^0 = (x_{n-m},...,x_n) \neq$ (0,…,0).In fact if we allot values (1,0,…0) (0,1,…0) …(0,0,…1) to $(x_{n-m}, x_{n-m+1},..., x_n)$ then solution:

$$x = \eta_0,...,\eta_m \longrightarrow \quad \textbf{(10)}$$

Linearly independent and a general solution of equation (9) for a particular choice of co-ordinate set $(a_0,...,a_n)$ of $(x_{n-m},...,x_n)$ is:

$$x = a_0\eta_0 + ... + a_m\eta_m \longrightarrow \quad \textbf{(11)}$$

Where, a_j can take values in GF(s) subject to restrictions mentioned above.

The total number of m-flats in PG(n, s) from equation (11) it is clear that each m-flat is determined by any set of (m+1) linearly independent points $\xi_0, \xi_1,..., \xi_m$ of PG(n, s).

Hence, the total number of m-flats denoted by ϕ (n, m, s) is equal to the number of ways of selecting (m+1) independent points from the total number P_n of points of the geometry PG (n, s), divided by the number of ways of selecting (m+1) independent points on an m-flat. The second point in (P_n – 1) = $P_n - P_0$ ways.

The third point must be chosen in such a way that it is linearly independent of the first and second point. That is it is not a point on the 1-flat formed by the first two points. Now there are P_1 points in a 1-flat.

Similarly, it does not lie on the (k–1) flat formed by them. Now there are P_{k-1} points in a (k–1) flat. Hence the $(k+1)^{th}$ point can be chosen in $(P_n - P_{k-1})$ ways (k = 1,…, m). Hence the total number of ways of selecting (m+1) linearly independent points from P_n is,

$$P_n(P_n - P_o)(P_n - P_1)....(P_n - P_{m-1})$$

Similarly, P_m is $P_m(P_m - P_o)(P_m - P_1)(P_m - P_2)...(P_m - P_{m-1})$

Hence the total number of m- flats in PG (n, s) is,

$$\phi(n,m,s)=\frac{P_n\left(P_n-P_0\right)\left(P_n-P_1\right)\cdots\left(P_n-P_{m-1}\right)}{P_m\left(P_m-P_0\right)\left(P_m-P_1\right)\cdots\left(P_m-P_{m-1}\right)}$$

$$=\frac{(s^{n+1}-1)(s^n-1)...(s^{n-m+1}-1)}{(s^{m+1}-1)(s^m-1)...(s-1)}$$

It can be easily verified that,

$$\phi\text{ (n, m, s)} = \phi\text{ (n, n – m – 1, s)} \qquad \longrightarrow \qquad \textbf{(12)}$$

It can be shown that the total number of distinct m-flats of PG (n, s) passing through a fixed point is ϕ (n–1, m–1, s), (m $\geq$ 1) and the number of distinct m-flats of PG (n, s) passing through two fixed points is ϕ (n – 2, m –2,s) (m $\geq$ 2).

Consider PG (2, s) the number of different points:

$$P_2=\frac{s^3-1}{s-1}$$

$$= s^2+s+1$$

The number of points in a 1-flat (straight line) is:

$$p_1=\frac{s^2-1}{s-1}$$

$$= s + 1$$

The number of straight lines is:

$$\phi(2,1,s)=\frac{(s^3-1)(s^2-1)}{(s^2-1)(s-1)}$$

$$= s^2+ s + 1$$

The number of distinct straight lines passing through a fixed point is.

$$\phi(1,0,s)=\frac{s^2-1}{s-1}$$

$$= s + 1$$

The number of points (0, x_2, x_3) at infinity is

$$\frac{s^2-1}{s-1}=s+1$$

The number of straight lines (by + cz = 0) at infinity is s + 1

Construct finite projective plane PG (2, 3).

Points in this geometry are:

$$x=(x_0,x_1,x_2) \quad (\neq (0,0,0))$$

$$x_i \in \text{GF (3)} \qquad \text{(i = 0, 1, 2)}$$

Also $x = y$ = (y_0, y_1, y_2) if and only if $y_i = ax_i$ (0, 1, 2) for any $\alpha(\neq 0)$ $\in$ GF (3).

The lines (1- dimensional flat) in this plan are,

$$a_0x_0 + a_1x_1 + a_2x_2 = 0 \longrightarrow \quad \textbf{(13)}$$

Where, (a_0 , a_1 , a_2) $\neq$ (0, 0, 0) and a_i $\in$ GF (3) (i = 0, 1,2)

Table 1: The points of PG (2, 3)

Sl. No.	(x_0, x_1, x_2)
1	(1, 0, 0)
2	(0,1, 0)
3	(0, 0, 1)
4	(1, 1, 0)
5	(1, 0, 1)
6	(0, 1, 1)
7	(1, 2, 0)
8	(1, 0, 2)
9	(0, 1, 2)
10	(1, 1, 1)
11	(1, 1, 2)
12	(1, 2, 1)
13	(1, 2, 2)

Points with serial numbers 2, 3, 6 and 9 are the points at infinity.

Table 2: Lines of PG (2, 3)

Sl. No.	**Equation of the line**	**Sl. No. of the points in the line**
I	$x_0 = 0$	2, 3, 6, 9
II	$x_1 = 0$	1, 3, 5, 8
III	$x_2 = 0$	1, 2, 4, 7
IV	$x_0 + x_1 = 0$	3, 7, 12, 13
V	$x_0 + x_2 = 0$	2, 8, 11, 13
VI	$x_1 + x_2 = 0$	1, 9, 11, 12
VII	$x_0 + 2x_1 = 0$	4, 8, 10, 11
VIII	$x_0 + 2x_2 = 0$	2, 5, 10, 12

IX	$x_1+2x_2=0$	1, 6, 10, 13
X	$x_0+x_1+x_2=0$	7, 8, 9, 10
XI	$x_0+x_1+2x_2=0$	6, 5, 7, 11
XII	$x_0+2x_1+x_2=0$	4, 6, 8, 12
XIII	$x_0+2x_1+2x_2=0$	4, 5, 9, 13

There are 4 points on each of the 13 lines in the plane. A number of distinct straight lines passing through a fixed point is 4.

FINITE EUCLIDEAN GEOMETRY

An ordered set $x=\left(x_1,\cdots,x_n\right)$ of n elements from a GF$\left(s\right)$ is called a **Finite Euclidean Geometry** EG (n, s).

Two points x and $y=\left(y_1,\cdots,y_n\right)$ of EG (n, s) are identical if and only if $x_i=y_i\left(i=1,\cdots,n\right)$. All points satisfying (n–m) linearly independent homogeneous equations

$$\sum_{i=0}^{n}a_{ji}x_i=0\ \ \left(j=1,\cdots,n-m;x_0=1\right)\qquad\longrightarrow\qquad\textbf{(14)}$$

$$a_{ji}\in GF\left(s\right)$$

Form on **m - dimensional subspace** or **m - flat** of EG (n, s).

An EG (n, s) contains exactly s^n points and m – dimensional subspace of EG (n, s) contains exactly s^m points.

The number of m-dimensional subspaces of EG (n, s) is,

$$\phi\left(n,m,s\right)-\phi\left(n-1,m,s\right)\qquad\longrightarrow\qquad\textbf{(15)}$$

Where, $\phi\left(n,m,s\right)$ is defined in equation (8)

$$\phi\left(n,m,s\right)=\frac{(s^{n+1}-1)(s^n-1)...(s^{n-m+1}-1)}{(s^{m+1}-1)(s^m-1)...(s-1)}\quad\left(m\geq 0,n\geq m\right)$$

The number of m-dimensional subspaces of EG (n, s) passing through one fixed point is $\phi\left(n-1,m-1,s\right)$ and the number passing through two fixed points is $\phi\left(n-2,m-2,s\right)$.

By known equation,

$$\sum_{i=0}^{n}\ a_{ji}x_i=0\ \ \left(j=1,\cdots,n-m;x_0=1\right)$$

$$a_{ji}\in GF\left(s\right)$$

If we exclude from PG (n, s) the points satisfying $x_0=0$, which constitute a (n – 1) dimensional. Flat in PG (n, s). The number of m - flats in EG (n, s), where m < n, is thus:

$$\phi\left(n,m,s\right)-\phi\left(n-1,m,s\right).$$

Consider EG (2, s). A total number of points (x, y) is s^2. Every straight line $ax+by+c=0$. Contains exactly s points. The number of straight lines is $\phi(2,1,s)-\phi(1,1,s)=s^2+s$. The number of straight lines passing through a fixed point is $\phi(1,0,s)=s+1$.

If we consider the first principle, in EG (2, s), lines are given by the linear equation.

$$ax+by+c=0, \qquad (a,b)\neq(0,0) \longrightarrow \quad \textbf{(16)}$$

The line (16) is same as line:

$$a^1x+b^1y+c^1=0 \longrightarrow \quad \textbf{(17)}$$

If, $a/a^1=b/b^1=c/c^1$. Thus there are $(s^2-s)/s-1=s(s+1)$ lines.

Let us find the point of two lines,

$$a_1x+b_1y+c_1=0$$
$$a_2x+b_2y+c_2=0$$

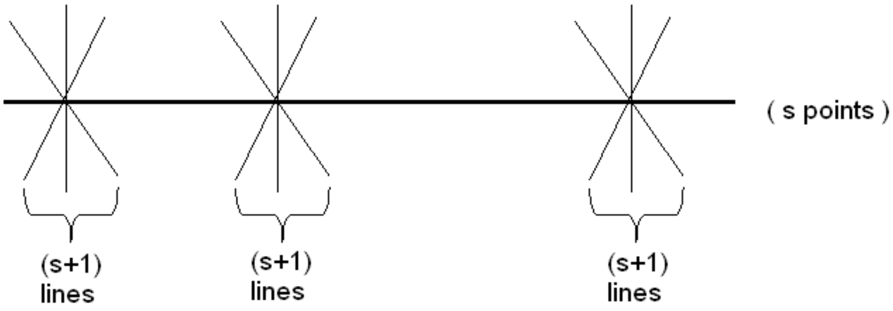
This is given by,

$$\frac{x}{b_1c_2-b_2c_1}=\frac{y}{a_2c_1-a_1c_2}=\frac{1}{a_1b_2-a_2b_1}$$

If $a_1b_2\neq a_2b_1$, then we get a unique point of intersection. If $a_1b_2=a_2b_1$, then we do not get any point of intersection at all and say that the lines are parallel.

Hence, if we start with a line $ax+by+c=0$ and give to c all possible values keeping a, b fixed we get a set of s mutually parallel lines which may be said to form a pencil of parallel lines.

Now there are s points on a line. Also through any point passes (s + 1) lines. Hence the totality of s^2+s lines in EG$(s,2^n)$ can be grouped into s +1 pencils of parallel lines, each pencil consisting of s lines:



Let us consider the s lines of a parallel pencil

$$X_i\left[ax+by+c=0; x=x_i\right]$$

These s lines may be assumed to pass through a common point at infinity. Hence for $(s+1)$ pencils of parallel lines we get $(s+1)$ points at infinity. Again these $(s+1)$ points at infinity may be considered to lie on a line at infinity.

Thus we have the s^2+s+1 points and s^2+s line of PG$(2,s)$. The original s^2 points and s^2+s may be called finite points finite lines of PG$(2,s)$ respectively.

The points of a PG (n, s) for which $x_0\neq 0$ and the points of a

EG (n, s) can be mapped one - to - one onto each other.

If the first co-ordinate of a point in PG (n, s) is not zero, it can be regarded as $\left(1, x_1 / x_0 = x_1^{'}, \cdots, x_n / x_0 = x_n^{'}\right)$

Hence, there is a one-to-one correspondence between the finite points $\left(1, x_1{}', \cdots, x_n{}'\right)$ of PG (n, s) and the points $\left(x_1{}', \cdots, x_n{}'\right)$ of EG (n, s).

Consider a finite m-flat of PG (n, s) given by the equation:

$$a_{i0}x_0 + a_{i1}x_1 + \cdots + a_{in}x_n = 0 \qquad \left(i = 1, \cdots n - m; x_0 \neq 0\right) \longrightarrow \qquad \textbf{(18)}$$

A corresponding m-flat of EG(n, s) given by the equation:

$$a_{i0}x_0 + a_{i1}x_1 + \cdots + a_{in}x_n = 0 \qquad \left(i = 1, \cdots, n - m\right) \longrightarrow \qquad \textbf{(19)}$$

Thus there exists a one-to-one correspondence between the finite m - flats of PG (n, s) and the finite m - flats of EG (n, s). The finite points of the m - flats of PG (n, s) correspond to the points of m - flats of EG (n, s). Thus the geometry of EG (n, s) can be derived from PG(n, s) by removing from it all points at infinity and the m - flats wholly lying at infinity.

Conversely, one can construct PG(n, s) from EG(n, s)by treating the points in EG (n, s) as finite points of PG (n, s) and adding to it the (n – 1) - flat lying at infinity. $x_0 = 0$ As well as the distinct points lying on the flat.

LATIN SQUARES

Two Latin square is said to be orthogonal if on super imposition any letter of the first square comes together just once with each letter of the second square. The following are two orthogonal 4 x 4 Latin squares.

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

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

If we can find another Latin square which is orthogonal to each of the above two, we have a system of 3 mutually orthogonal Latin squares. The third square may be written as.

BLOCK DESIGN'S

Consider EG (2, p^n), where p is a prime and n any integer, p^n = s. let the parallel pencil { $x = \alpha_j$, j = 0, 1,..., s – 1 }

Where, α_j is an element of GF (p^n) be denoted as (X). Similarly the parallel pencil { $y = \alpha_j$, j = 0, 1, …, s – 1}is denoted as (Y). Again let the parallel pencil

$$\{ \ x + \alpha_j \ \ y = \alpha_j \}$$

Where, α_i is fixed but α_j takes all possible values be denoted as (W_i). Thus we have the (s + 1) pencils (X), (Y), (W_1), (W_2)… (W_{s-1})

The point at infinity on (X), (Y), (W_1), (W_2)… (W_{s-1}) are denoted by, X , Y , W_1 , …, W_{s-1} respectively.

The lines of these pencil can be numbered. Thus the j^{th} line of the pencil (X) whose equation is $x = \alpha_j$ will be denoted as line numbered j of (X). Similarly, for other pencils.

Consider now an s$\times$s Latin square. The rows (columns) may be numbered 0, 1, …, s – 1. To the cell (c, d) of the Latin square, we may correspond the point (α_e, α_d) of EG (2, s). That is the point given by the intersection of c^{th} the row of (X) and d^{th} column of (Y).

Now consider the pencil (W_i). Through the point (α_c, α_d) only one member of this pencil can pass. If this is the j^{th} line of this pencil we put the number j in the $(c, d)^{th}$ cell of an s x s square.

The arrangement we thus get is Latin square, because to any row of our square there corresponds a line of the pencil (X) and through each of s points of this line passes one line of the pencil (Y) and through each of the finite points (α_c, α_d) of this square there passes one line of the pencil (W_i). It is readily found that if,

$$\alpha_c + \alpha_i \alpha_d = \alpha_j$$

Then,

$$\alpha_c + \alpha_i \alpha_{d'} \neq \alpha_j \qquad \text{For } d \neq d^1$$

$$\text{and} \quad \alpha_{c'} + \alpha_i \alpha_d \neq \alpha_j \qquad \text{For } c \neq c^1$$

Hence the arrangement we have got a Latin square. This Latin square derived from the pencil (W_i) will be denoted as [L_i]. Corresponding to (s – 1) pencils $W_i, \ldots, W_{s-1}$ we thus get (s – 1) Latin squares. It is required to prove that [L_i] is orthogonal to [L_j] (i $\neq$ j).

If the square [L_i] is superimposed on [L_j] then the number c of the first square will occur with the number d in the second square if and only if the c^{th} line of W_i intersects the d^{th} line of W_j at the point corresponding to the cell in which c and d occur together. These two lines, however, intersect at one and only one point. This shows that [L_i] and [L_j] are orthogonal.

2. CONCLUSIONS

The three chapters, which I have presented in this dissertation, give a study of the topic

“A CONSTRUCTION OF DESIGNS”

Here, **“statistics”** could not be discussed in detail due to the precise nature of the project. Yet I have tried my level best to put all the details in a nutshell.

REFERENCES

1.	**PARIMAL MUKHOPADHYAY**	Applied Statistics, Books & Allied (p) Ltd, Kolkata
2.	**GUPTA. S. C and Kapoor**	Fundamentals of Mathematical Statistics, Sultan Chand & sons, New Delhi.
3.	**SINGARAVELU. A**	Probability and statistics, A. R. Publications, Tamil Nadu.