



Final Report

Theory Of Block Designs

Parvathy S
MS13020

Indian Institute of Science Education and Research, Mohali



Under the supervision of
Prof. B. Sury
Theoretical Statistics And Mathematics Unit
Indian Statistical Institute, Bangalore



Acknowledgements

It is with immense gratitude that I acknowledge the support and help of my Professor B.Sury, Indian Statistical Institute(ISI), Bangalore. I express my deep sense of gratitude to him for his lectures and meetings which helped me enlighten my knowledge.

I take this opportunity to record my sincere thanks to the institution and my guide for the pleasant accommodation.

I am also thankful to my parents and friends for their help and support.

Parvathy S

Abstract

Combinatorial Design Theory is a branch of combinatorial mathematics which underlines the study of existence, construction and properties of finite sets whose arrangements satisfy some generalized concepts of balance and symmetry. We focus primarily on Balanced Incomplete Block Designs.

In this report, we deal with three chapters of which the first chapter deals with introduction to block designs and we mainly see the definition and properties of a particular kind of design, Balanced Incomplete Block Designs or BIBD's. Secondly, we shift our focus to explore a particular kind of BIBD, called symmetric BIBD's and we see the necessary and sufficient conditions for the existence of the same using the results from number theory. Finally we study the concept of difference sets and how it is related to symmetric BIBD's. We conclude the report with the proof of the multiplier theorem which uses results from algebra.

Through these three chapters we get an idea of block designs and its various properties. An interesting application of the same is construction and properties of sudoku.

Contents

Acknowledgements	ii
Abstract	iii
1 Balanced incomplete block designs	3
1.1 Design theory	3
1.2 Basic Definitions And Properties	3
1.3 Incidence Matrices	7
1.4 Isomorphisms And Automorphisms	12
1.4.1 Constructing BIBDs with specified automorphisms	14
1.5 New BIBD's from Old	16
1.6 Fisher's Inequality	17
2 Symmetric BIBD's	20
2.1 Properties of Symmetric BIBD's	20
2.2 Residual And Derived BIBD's	25
2.3 Projective Planes And Geometries	27
2.4 Bruck-Ryser-Chowla Theorem	30
2.5 Statement Of Hasse-Minkowski And Applications	37
3 Difference Sets	47
3.1 Difference Sets and Automorphisms	47
3.2 Quadratic Residue Difference Sets	53
3.3 The Multiplier Theorem	55
3.4 Multipliers of difference sets	55
3.4.1 Group Ring	57
3.5 Proof of the Multiplier Theorem	60

Chapter 1

Balanced incomplete block designs

1.1 Design theory

What is design theory and what are its applications? Combinatorial design theory deals with questions about whether it is possible to arrange elements of a finite set into subsets such that certain balance properties are satisfied. There are different types of designs like balanced incomplete block designs (BIBD), pairwise balanced designs, orthogonal Latin squares and so on. The fundamental questions in this area are those of existence and construction of certain kind of designs. Designs have many other applications in mathematical biology, scheduling lotteries, cryptography and so on.

Here we will explore a special kind of design called *balanced incomplete block design* or BIBD.

1.2 Basic Definitions And Properties

Definition 1.2.1 *Design*

A design is a pair (X, \mathcal{A}) such that the following properties are satisfied:

1. X is a set of elements called *points*.
2. \mathcal{A} is a collection(i.e a multiset) of nonempty subsets of X called *blocks*.

If two blocks in a design are identical then it is called *repeated blocks*. Hence A is a multiset of blocks rather than a set. To list the elements of a multiset, \square notation is used. If a design contains no repeated blocks, it is called a *simple design*. Here all the elements of the multiset has multiplicity one and hence is a set. For example, $[1, 2, 3, 4] = \{1, 2, 3, 4\}$ but $[1, 2, 3, 4, 3] \neq \{1, 2, 3, 4, 3\} = \{1, 2, 3, 4\}$. Order of elements is irrelevant in a multiset as with a set.

Now, we will see a particular kind of design which is called a balanced incomplete block design which we will further study.

Definition 1.2.2 *Balanced Incomplete Block Design(BIBD)*

Let v, k and λ be positive integers such that $v > k \geq 2$. A (v, k, λ) -balanced incomplete block design or (v, k, λ) -BIBD is a design (X, \mathcal{A}) such that the following properties are satisfied:

1. $|X| = v$
2. Each block contains exactly k points.
3. Every pair of distinct points is contained in exactly λ blocks.

The third property in the definition is called the "balance" property. It is called incomplete block design since $k < v$ and hence all blocks are incomplete. Thus a block design is not merely a collection of subsets of a set, but is an array of objects and blocks with a relation telling which objects belong to which blocks. A design may contain repeated blocks if $\lambda > 1$.

Example 1.2.3 $(7, 3, 1)$ -BIBD



$$X = \{1, 2, 3, 4, 5, 6, 7\}, \text{ and}$$

$$\mathcal{A} = \{123, 145, 167, 246, 257, 347, 356\}$$

The blocks can be represented as six lines and a circle.

Example 1.2.4 $(9, 3, 1)$ -BIBD



$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}, \text{ and}$$

$$\mathcal{A} = \{123, 456, 789, 147, 258, 369, 159, 267, 348, 168, 249, 357\}$$

The blocks of this BIBD can be represented as eight lines and four triangles. The blocks can also be separated as four sets of three, where each of these four sets covers all the points of BIBD.

Example 1.2.5

Let \mathcal{A} consists of all k -subsets of X . Then (X, \mathcal{A}) is a $(v, k, \binom{v-2}{k-2})$ -BIBD.



Let's now see two theorems which will give us more basic properties of BIBD.

Theorem 1.2.6 *In a (v, k, λ) -BIBD, every point occurs in exactly $r = \frac{\lambda(v-1)}{k-1}$ blocks; where r is called the replication number of BIBD.*

Proof: Let (X, \mathcal{A}) be a (v, k, λ) -BIBD. Let $x \in X$ and r_x be the number of blocks containing x . Define a set

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

We compute $|I|$ in two ways.

There are $(v-1)$ ways to choose $y \neq x \in X$, and for each y , there is exactly λ blocks such that $\{x, y\} \subseteq A$. Hence,

$$|I| = \lambda(v-1).$$

Secondly, there are r_x blocks $x \in A$. For each A , there are $k-1$ ways to choose $y \in A$ and $y \neq x$. Hence,

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

Combining these two equations of $|I|$, we get

$$\lambda(v-1) = r_x(k-1).$$

Hence, $r_x = \frac{\lambda(v-1)}{k-1}$.

We see that r_x is independent of x and any element is contained in exactly r number of blocks. \square

Theorem 1.2.7 *A (v, k, λ) -BIBD has exactly*

$$b = \frac{vr}{k} = \frac{\lambda(v^2 - v)}{k^2 - k}$$

blocks.

Proof: Let (X, \mathcal{A}) be a (v, k, λ) -BIBD and let $b = |\mathcal{A}|$. Define a set

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

We compute $|I|$ in two ways.

Firstly, there are v ways of choosing an element $x \in X$. For each x , there are exactly r blocks such that $x \in A$. Hence,

$$|I| = vr$$

Secondly, there are b blocks $A \in \mathcal{A}$. For each block A , there are k ways to choose $x \in A$. Hence,

$$|I| = bk$$

Combining the two equations we have, $bk = vr$. Hence,

$$b = \frac{vr}{k}$$

Substituting the value of r from the above theorem ,

$$b = \frac{vr}{k} = \frac{\lambda(v^2 - v)}{k^2 - k}$$

as desired. □

To record all the five parameters we use the notation (v, b, r, k, λ) . Since b and r are integers, these values will help us conclude that BIBD's with certain parameters do not exist.

Corollary 1.2.8 *If a (v, k, λ) -BIBD exists, then $\lambda(v - 1) \equiv 0 \pmod{k - 1}$ and $\lambda v(v - 1) \equiv 0 \pmod{k(k - 1)}$.*

Proof: It is clear that b and r must be integers since they indicate the number of blocks and the replication number respectively.

Since $\lambda(v - 1) = r(k - 1)$, $\lambda(v - 1) \equiv 0 \pmod{k - 1}$.

Similarly, since $b = \frac{\lambda(v^2 - v)}{k^2 - k}$, $\lambda v(v - 1) \equiv 0 \pmod{k(k - 1)}$. □

For example, a $(8, 3, 1)$ -BIBD does not exist, since $\lambda(v - 1) = 7 \not\equiv 0 \pmod{2}$. Also a $(19, 4, 1)$ -BIBD does not exist since $\lambda v(v - 1) = 342 \not\equiv 0 \pmod{12}$.

1.3 Incidence Matrices

Incidence matrices are a convenient way of expressing BIBD's in a matrix form.

Definition 1.3.1 *Incidence Matrix*

Let (X, \mathcal{A}) be a design where $X = \{x_1, \dots, x_v\}$ and $\mathcal{A} = \{A_1, \dots, A_b\}$. The incidence matrix of (X, \mathcal{A}) is the $v \times b$ 0-1 matrix $M = (m_{i,j})$ defined as

$$(m_{i,j}) = \begin{cases} 1 & \text{if } x_i \in A_j; \\ 0 & \text{if } x_i \notin A_j. \end{cases}$$

From the definition and properties of a BIBD, it is clear that the incidence matrix M of a (v, b, r, k, λ) -BIBD satisfies the following properties.

1. every column of M contain exactly k '1's.
2. every row of M contain exactly r '1's.
3. two distinct rows of M contain both '1's in exactly λ columns.

Example 1.3.2

The incidence matrix of the $(9, 3, 1)$ -BIBD is a 9×12 matrix which is represented as follows:

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Let I_n denote the $n \times n$ identity matrix, J_n denote an $n \times n$ matrix in which every entry is 1 and let \mathbf{u}_n denote a vector of length n in which every coordinate is 1. For a matrix $M = (m_{i,j})$, we define *transpose* of M , denoted by M^T , to be the matrix whose (j, i) entry is $m_{i,j}$.

Now we will see a property of incidence matrices of BIBD's.



Theorem 1.3.3 Let M be a $v \times b$ 0-1 matrix and let $2 \leq k < v$. Then M is the incidence matrix of a (v, b, r, k, λ) -BIBD if and only if

$$MM^T = \lambda J_v + (r - \lambda)I_v$$

and $\mathbf{u}_v M = k\mathbf{u}_b$.



Proof: Let (X, \mathcal{A}) be a (v, b, r, k, λ) -BIBD, where $X = x_1, \dots, x_v$ and $\mathcal{A} = A_1, \dots, A_b$. Let M be its incidence matrix. Then if $MM^T = B$, then the element b_{ij} of matrix B is the inner product of i th row of M with j th row of M . Every element on the main diagonal, b_{ii} of B counts the number of 1's in the i th row of M , which gives in how many blocks a particular element is present, which is r . But if $j \neq i$, then both the i th and j th rows have a 1 in the same column if and only if both x_i and x_j belong to the same column. And we have any pair of elements is present in exactly λ blocks, so every off diagonal entry of B is λ . Therefore,

$$MM^T = \begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \dots & r \end{pmatrix} = \lambda J_v + (r - \lambda)I_v \quad (1.1)$$

$\mathbf{u}_v M$ is a $1 \times b$ matrix whose i th entry counts the number of 1's in i th column, which is k . Hence, $\mathbf{u}_v M = k\mathbf{u}_b$.

Conversely, suppose that M is a $v \times b$ 0-1 matrix such that $MM^T = \lambda J_v + (r - \lambda)I_v$ and $\mathbf{u}_v M = k\mathbf{u}_b$. Let (X, \mathcal{A}) be a design whose incidence matrix is M . Since M is a $v \times b$ matrix, $|X| = v$ and $|\mathcal{A}| = b$. From the second condition, it follows that every block of \mathcal{A} contains k points. From the first condition, it follows that every point occurs in r blocks and every pair of points occurs in λ blocks. Hence (X, \mathcal{A}) is a (v, b, r, k, λ) -BIBD. \square

The above relation

$$MM^T = \lambda J_v + (r - \lambda)I_v \quad (1.2)$$

can also be written as a relation on quadratic forms. Let x_1, \dots, x_v be the points, and we associate the linear form L_j to the blocks A_j , and $m_{i,j}$ be the incidence numbers; where

$$L_j = \sum_{i=1}^v m_{ij}x_i, \quad 1 \leq j \leq b$$

Let us define $x = (x_1, \dots, x_v)$ and we will multiply both sides of equation (1.2) by x on the left and by x^T on the right. We can see here that x is a $1 \times v$ matrix and both sides of equation (1.2) are $v \times v$ matrix. We first see how LHS will result into after the above operation:

$$xMM^T x^T = (xM)(xM)^T$$

$xM = (x_1m_{11} + x_2m_{21} + \dots + x_vm_{v1}, \dots, x_1m_{1b} + x_2m_{2b} + \dots + x_vm_{vb}) = (L_1, \dots, L_b) = L$, say

Hence,

$$xMM^T x^T = LL^T = \sum_{j=1}^b L_j^2.$$

Now, we see how RHS would look like:

$$x(\lambda J_v + (r - \lambda)I_v)x^T = \lambda xJ_v x^T + (r - \lambda)xx^T.$$


$$xJ_v = \left(\sum_{i=1}^v x_i, \dots, \sum_{i=1}^v x_i \right) \quad v \text{ coordinates and}$$

$$\begin{aligned} \lambda xJ_v x^T &= \lambda \left(\sum_{i=1}^v x_i, \dots, \sum_{i=1}^v x_i \right) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_v \end{pmatrix} \\ &= \lambda \left(x_1 \sum_{i=1}^v x_i + \dots + x_v \sum_{i=1}^v x_i \right) \\ &= (x_1 + \dots + x_v) \sum_{i=1}^v x_i \\ &= \sum_{i=1}^v x_i \sum_{i=1}^v x_i \\ &= \lambda \left(\sum_{i=1}^v x_i \right)^2 \end{aligned}$$

$$(r - \lambda)xx^T = (r - \lambda) \sum_{i=1}^v x_i^2$$

Hence equation (1.2) now transforms into

$$\sum_{j=1}^b L_j^2 = \lambda \left(\sum_{i=1}^v x_i \right)^2 + (r - \lambda) \sum_{i=1}^v x_i^2$$


which is the relation on quadratic forms. 

We will use this relation later on in the next chapter when we prove the necessity and existence conditions.

We will now give the definition of a different kind of design known as pairwise balanced design.

Definition 1.3.4 *Pairwise Balanced Design*

A pairwise balanced design or **PBD** is a design (X, \mathcal{A}) such that every pair of distinct points occur in exactly λ blocks, where λ is a positive integer. Further, (X, \mathcal{A}) is a regular pairwise balanced design if every point in X occurs in exactly r blocks $A \in \mathcal{A}$, where r is a positive integer.

 A PBD (X, \mathcal{A}) is allowed to contains blocks of any size. If (X, \mathcal{A}) consists only of blocks of size $|X|$ (complete blocks), then it is said to be a trivial pairwise balanced design. And if it contains no complete blocks, it is a proper pairwise balanced design.

PBD's are those designs whose incidence matrices satisfy just the first condition of the above theorem , which we will restate here.

Theorem 1.3.5 *Let M be a $v \times b$ 0 – 1 matrix. Then M is the incidence matrix of a regular pairwise balanced design having v points and b blocks if and only if there exist positive integers r and λ such that $MM^T = \lambda J_v + (r - \lambda)I_v$.*

Proof: The proof follows from the proof of the above theorem, whose proof does not require the size of each block. Since size of each block is not constant, the second condition of the above theorem does not hold here. \square

Example 1.3.6

An example to illustrate the above example: Consider the 6×11 matrix:

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

This matrix M is the incident matrix of the regular pairwise balanced design

$$X = 1, 2, 3, 4, 5, 6, \text{ and}$$

$$\mathcal{A} = \{123, 456, 14, 15, 16, 24, 25, 26, 34, 35, 36\}$$

Here, $v = 6, b = 11, r = 4$ and $\lambda = 1$. The design is not a BIBD because every block does not have the same size. Also it is easily verified that $MM^T = J_v + 3I_v = \lambda J_v + (r - \lambda)I_v$ and $\mathbf{u}_6 M = (3, 3, 2, 2, 2, 2, 2, 2, 2, 2, 2)$ and $\mathbf{u}_6 M \neq k\mathbf{u}_b$ for any integer k .

Now we will see what a dual design is and give its basic property.

Definition 1.3.7 *Dual Design*

Suppose (X, \mathcal{A}) be a design with $|X| = v$ and $|\mathcal{A}| = b$ and let M be the $v \times b$ incidence matrix of (X, \mathcal{A}) . Then the design having M^T as its incidence matrix is called the dual design of (X, \mathcal{A}) .

If (Y, \mathcal{B}) is the dual design of (X, \mathcal{A}) , then $|Y| = b, |\mathcal{B}| = v$.

Theorem 1.3.8 *Suppose that (X, \mathcal{A}) is a (v, b, r, k, λ) -BIBD, and let (Y, \mathcal{B}) be the dual design of (X, \mathcal{A}) . Then the following properties hold:*

1. every block in \mathcal{B} has size r
2. every point in Y occurs in exactly k blocks, and
3. any two distinct blocks $B_i, B_j \in \mathcal{B}$ intersect in exactly λ points.

Proof: Since M^T is the incidence matrix of (Y, \mathcal{B}) , 1 holds since every column of M^T has r number of 1's. 2 holds since every row of M^T has k number of 1's and 3 holds since every distinct pair of elements is contained in λ number of blocks. \square

1.4 Isomorphisms And Automorphisms

Definition 1.4.1 *Isomorphisms of Designs*

Suppose (X, \mathcal{A}) and (Y, \mathcal{B}) are two designs with $|X| = |Y|$. (X, \mathcal{A}) and (Y, \mathcal{B}) are isomorphic if there exist a bijection $\alpha : X \rightarrow Y$ such that

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

If we rename every point x by $\alpha(x)$, then the collection of blocks \mathcal{A} is transformed into \mathcal{B} . The bijection α is called an isomorphism.

We will now see how the incidence matrices of isomorphic designs are related.

Theorem 1.4.2 *Suppose $M = (m_{i,j})$ and $N = (n_{i,j})$ are both $v \times b$ incidence matrices of designs. Then the two designs are isomorphic if and only if there exist a permutation γ of $\{1, 2, \dots, v\}$ and a permutation β of $\{1, 2, \dots, b\}$ such that*

$$m_{i,j} = n_{\gamma(i), \beta(j)}$$

for all $1 \leq i \leq v, 1 \leq j \leq b$.

Proof: Suppose that (X, \mathcal{A}) and (Y, \mathcal{B}) are designs having $v \times b$ incidences matrices M and N respectively. Suppose that $X = \{x_1, \dots, x_v\}, Y = \{y_1, \dots, y_v\}, \mathcal{A} = \{A_1, \dots, A_b\}, \mathcal{B} = \{B_1, \dots, B_b\}$.

Suppose (X, \mathcal{A}) and (Y, \mathcal{B}) are isomorphic. Then \exists a bijection $\alpha : X \rightarrow Y$ such that $[\{\alpha(x) : x \in A\} A \in \mathcal{A}] = \mathcal{B}$. For $1 \leq i \leq v$, define

$$\gamma(i) = j \text{ if and only if } \alpha(x_i) = y_j.$$

Since α is a bijection of X and Y , γ is a permutation of $\{1, \dots, v\}$.

Let $\{\alpha(x) : x \in A_j\} = B_{\beta(j)}$. $\therefore \exists$ a permutation β of $\{1, \dots, b\}$ for $1 \leq j \leq b$, since α is an isomorphism of (X, \mathcal{A}) and (Y, \mathcal{B}) .

Now,

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

Conversely, suppose we have permutations γ and β such that $m_{i,j} = n_{\gamma(i),\beta(j)} \forall i, j$. Define $\alpha : X \rightarrow Y$ such as $\alpha(x_i) = x_j$ if and only if $\gamma(i) = j$. Then,

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

for $1 \leq j \leq b$. Hence α defines an isomorphism of (X, \mathcal{A}) and (Y, \mathcal{B}) . \square

A *permutation matrix* is a 0 – 1 matrix in which every row and every column contain exactly one entry '1'.

We will use permutation matrix to give one more theorem relating incidence matrices of isomorphic designs.

Corollary 1.4.3 *Suppose M and N are incidence matrices of two (v, b, r, k, λ) -BIBDs. Then the two BIBDs are isomorphic if and only if there exists a $v \times v$ permutation matrix, say P , and a $b \times b$ permutation matrix, say Q , such that $M = PNQ$.*

Proof: Let P be the matrix whose $(i, \gamma(i))$ th entry is 1 and rest entries are all 0. And let R be the matrix whose $(j, \beta(j))$ th entry is 1 and rest entries are all 0. And let $R^T = Q$. Clearly P and Q are permutation matrices. PN is a rearrangement of rows of N which correspond to the action of the bijection on points. Post multiplying by Q gives a rearrangement of columns, but no columns are changed and the structure is preserved. \square After defining isomorphic designs we define when designs are automorphic.

Definition 1.4.4 *Automorphism Of Design*

Suppose (X, \mathcal{A}) be a design. An automorphism of (X, \mathcal{A}) is an isomorphism of this design with itself. Here α is a permutation of X such that

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

A permutation α on a set X can be represented as *disjoint cycle representation*. Each cycle has the form

$$(x, \alpha(x), \alpha(\alpha(x)), \dots)$$

for some $x \in X$. The cycles thus obtained are disjoint and they have lengths that sum upto $|X|$. Order of the permutation α is the least common multiple of the lengths of cycles in the disjoint cycle representation. A *fixed point* of α is the point x such that $\alpha(x) = x$, which will correspond to those cycles which have length 1.

The set of all automorphisms of a BIBD (X, \mathcal{A}) forms a group under the operation of composition of permutations. This group is called the *automorphism group* of the BIBD and is denoted $Aut(X, \mathcal{A})$. $Aut(X, \mathcal{A})$ is a subgroup of the symmetric group $S_{|X|}$.

1.4.1 Constructing BIBDs with specified automorphisms

Here we finally reach a theorem to show the existence or non existence of a BIBD having specified automorphisms.

Let S_v denote symmetric group on a V -set. For a positive integer $j \leq v$, let $\binom{X}{j}$ be the set of all $\binom{v}{j}$ j subsets of X . For $Y \subseteq X$ and for a permutation $\beta \in S_v$, let

$$\beta(Y) = \{\beta(x) : x \in Y\}$$

Suppose G is a subgroup of S_v . For positive integer $j \leq v$, for $A, B \in \binom{X}{j}$, define $A \sim_j B$ if $\beta(A) = B$ for some $\beta \in G$.

1. Identity permutation fixes A , hence \sim_j is reflexive.
2. Let $\beta(A) = B$ for some $\beta \in G$, then $\beta^{-1}(B) = A$, since $\beta^{-1} \in G$. Hence \sim_j is symmetric.
3. Let $\beta_1(A) = B$ and $\beta_2(B) = C$ for some $\beta_1, \beta_2 \in G$. Hence $\beta_2 \circ \beta_1(A) = \beta_2(B) = C$. Since G is a subgroup $\beta_2 \circ \beta_1 \in G$. Hence transitive.

$\therefore \sim_j$ is an equivalence relation on $\binom{X}{j}$. The equivalence classes of this relation are called *j -orbits* of X with respect to G . Hence $\beta(A) = B$ for some $\beta \in G$ if and only if A and B are in the same orbits of G and the j -orbits form a partition of the set $\binom{X}{j}$.

We state the following lemma without proof.

Lemma 1.4.5 (Cauchy-Frobenius-Burnside Lemma) *The number of j -orbits of X with respect to the group G is exactly*

$$\frac{1}{|G|} \sum_{\beta \in G} \text{fix}(\beta)$$

where for each $\beta \in G$,

$$\text{fix}(\beta) = \left| \left\{ A \in \binom{X}{j} : \beta(A) = A \right\} \right|$$

Let $\mathcal{O}_1, \dots, \mathcal{O}_n$ be the k -orbits and let $\mathcal{P}_1, \dots, \mathcal{P}_m$ be the 2-orbits of X . The $n \times m$ matrix $A_{k,2}$ is defined as :For $1 \leq j \leq m$, let Y_j be a 2-subset. Then for $1 \leq i \leq n$, (i, j) th entry of $A_{k,2}$ denoted by a_{ij} is

$$a_{ij} = |\{A \in \mathcal{O}_i : Y_j \subseteq A\}|.$$

Lemma 1.4.6 *Suppose $\mathcal{O}_1, \dots, \mathcal{O}_n$ be the k -orbits and $\mathcal{P}_1, \dots, \mathcal{P}_m$ be the 2-orbits of X with respect to the group G . Suppose that $Y, Y' \in \mathcal{P}_j$ for some j and suppose $1 \leq i \leq n$. Then*

$$|\{A \in \mathcal{O}_i : Y \subseteq A\}| = |\{A \in \mathcal{O}_i : Y' \subseteq A\}|$$

Proof: Since $Y, Y' \in \mathcal{P}_j, \exists \beta \in G$ such that $\beta(Y) = Y'$. $\forall A \in \mathcal{O}_i$ such that $Y \subseteq A, \beta(Y) \subseteq \beta(A) \implies Y' \subseteq \beta(A)$. Since β is a permutation $\beta(A) \neq \beta(B)$ if $A \neq B$.

$\therefore \forall A \in \mathcal{O}_i$ such that $Y \subseteq A$, we have $A' = \beta(A) \in \mathcal{O}_i$ such that $Y' \subseteq A'$ and the blocks $\beta(A)$ are all distinct. Hence,

$$|\{A \in \mathcal{O}_i : Y \subseteq A\}| \leq |\{A \in \mathcal{O}_i : Y' \subseteq A\}|$$


Opposite inequality is attained by interchanging Y and Y' and replacing β with β^{-1} . And the result is obtained by combining these two inequalities.

□

Through the above lemma it can be seen that a_{ij} is independent of the orbit representative Y_j chosen.

Theorem 1.4.7 (Kramer-Mesner Theorem) *There exists a (v, k, λ) -BIBD having G as the subgroup of its automorphism group if and only if there exist a solution $\mathbf{z} \in \mathbb{Z}^n$ to the matrix equation*

$$\mathbf{z}A_{k,2} = \lambda \mathbf{u}_m$$

where \mathbf{z} has  on negative entries.

Proof: We provide an outline of the proof. Suppose that $\mathbf{z} = (z_1, z_2, \dots, z_n)$ is a non negative integral solution to $\mathbf{z}A_{k,2} = \lambda \mathbf{u}_m$. Define

$$\mathcal{A} = \bigcup_{i=1}^n z_i \mathcal{O}_i.$$

i.e \mathcal{A} is formed by taking z_i copies of every block in \mathcal{O}_i for $1 \leq i \leq n$. Hence (X, \mathcal{A}) is a (v, k, λ) -BIBD having G as a subgroup of its automorphism group. Conversely, suppose that (X, \mathcal{A}) is the desired BIBD. Then \mathcal{A} must consist of a multiset union of the orbits $\mathcal{O}_i, 1 \leq i \leq n$. Let z_i denote the number of times each of the blocks of the orbit \mathcal{O}_i occurs in \mathcal{A} ; then $\mathbf{z} = (z_1, \dots, z_n)$ is a non negative integral solution to the $\mathbf{z}A_{k,2} = \lambda\mathbf{u}_m$. \square

The BIBD is simple if and only if the vector $\mathbf{z} \in \{0, 1\}^n$.

1.5 New BIBD's from Old

Here we state two methods of constructing new BIBD's from old.

Theorem 1.5.1 (Sum Construction) *Suppose there exists a (v, k, λ_1) -BIBD and a (v, k, λ_2) -BIBD. Then there exists a $(v, k, \lambda_1 + \lambda_2)$ -BIBD.*

Corollary 1.5.2 *Suppose there exists a (v, k, λ) -BIBD. Then there exists a $(v, k, s\lambda)$ -BIBD for all integers $s \geq 1$.*

Theorem 1.5.3 (Block Complementation) *Suppose there exists a (v, b, r, k, λ) -BIBD, where $k \leq v - 2$. Then there also exists a $(v, b, b - r, v - k, b - 2r + \lambda)$ -BIBD.*

Proof: Suppose (X, \mathcal{A}) is a (v, b, r, k, λ) -BIBD. Then block complementation is done by replacing every block $A \in \mathcal{A}$ by $X \setminus A$. We will show that $(X, \{X \setminus A : A \in \mathcal{A}\})$ is a BIBD. Clearly this design has v points and b blocks, and every block has $v - k \geq 2$ points and every point occurs in $b - r$ blocks. We need to show that every pair of points occurs in exactly $b - 2r + \lambda$ blocks.

Let $x, y \in X, x \neq y$. Define

$$a_1 = |\{A \in \mathcal{A} : x, y \in A\}|$$

$$a_2 = |\{A \in \mathcal{A} : x \in A, y \notin A\}|$$

$$a_3 = |\{A \in \mathcal{A} : x \notin A, y \in A\}|$$

$$a_4 = |\{A \in \mathcal{A} : x \notin A, y \notin A\}|$$

Now,

$$a_1 = \lambda, a_1 + a_2 = r = a_1 + a_3, a_1 + a_2 + a_3 + a_4 = b$$

Solving these equations gives

$$a_4 = b - 2r + \lambda$$

which is the number of blocks every pair of points occur. \square

1.6 Fisher's Inequality

Fisher's inequality is yet another important property of a BIBD, which in turn will help us to say BIBD's certain parameters do not exist.

Theorem 1.6.1 (Fisher's Inequality) *In any (v, b, r, k, λ) -BIBD, $b \geq v$.*

Proof: Let (X, \mathcal{A}) be a (v, b, r, k, λ) -BIBD, where $X = \{x_1, \dots, x_v\}$ and $\mathcal{A} = \{A_1, \dots, A_b\}$. Let M be the incidence matrix of this BIBD and \mathbf{s}_j be the j th row of M^T . It can be seen that $\mathbf{s}_1, \dots, \mathbf{s}_b$ are all v dimensional vector spaces in \mathbb{R}^v .

Define $S = \{\mathbf{s}_j : 1 \leq j \leq b\}$ and $\mathbf{S} = \text{span}(\mathbf{s}_j : 1 \leq j \leq b)$. \mathbf{S} is the subspace of \mathbb{R}^v spanned by the vectors \mathbf{s}_j 's;

$$\mathbf{S} = \left\{ \sum_{j=1}^b \alpha_j \mathbf{s}_j : \alpha_1, \dots, \alpha_b \in \mathbb{R} \right\}$$

\mathbf{S} consists of all linear combination of vectors $\mathbf{s}_1, \dots, \mathbf{s}_b$.

For $1 \leq i \leq v$, let $\mathbf{e}_i \in \mathbb{R}^v$ be the vector with 1 in the i th coordinate and 0 in all the other coordinates. The vectors $\mathbf{e}_1, \dots, \mathbf{e}_v$ form a basis of \mathbb{R}^v , so every vector in \mathbb{R}^v can be expressed as a linear combination of these v vectors. It is clear that every vector of \mathbf{S} can be expressed as a linear combination of the above v vectors. Hence $\mathbf{S} \subseteq \mathbb{R}^v$.

Now

$$\sum_{j=1}^b \mathbf{s}_j = (r, \dots, r) \implies \sum_{j=1}^b \frac{1}{r} \mathbf{s}_j = (1, \dots, 1) \quad (1.3)$$

For a particular value of $i, 1 \leq i \leq v$;

$$\sum_{\{j: x_i \in A_j\}} \mathbf{s}_j = (r - \lambda) \mathbf{e}_i + (\lambda, \dots, \lambda) \quad (1.4)$$

Since $\lambda(v-1) = r(k-1)$ and $v > k$, it follows that $r > \lambda$ and hence $r - \lambda \neq 0$. Combining equations (1.1) and (1.2), we get

$$\mathbf{e}_i = \sum_{\{j: x_i \in A_j\}} \frac{1}{r - \lambda} \mathbf{s}_j - \sum_{j=1}^b \frac{\lambda}{r(r - \lambda)} \mathbf{s}_j \quad (1.5)$$

Equation (1.3) expresses \mathbf{e}_i as a linear combination of $\mathbf{s}_1, \dots, \mathbf{s}_b$. Hence $\mathbf{e}_i \in \mathbf{S} \forall 1 \leq i \leq v. \therefore \mathbb{R}^v \subseteq \mathbf{S}$

Hence $\mathbf{S} = \mathbb{R}^v$; i.e the b vectors in \mathbf{S} span the vector space \mathbb{R}^v . Since \mathbb{R}^v has dimension v and is spanned by a set of b vectors, it must be that $b \geq v$; which is the desired result.

Fisher's inequality can also be proved in a different way by calculating determinant of the matrix in equation (1.1).

$$\det B = \det \begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \dots & r \end{pmatrix}$$

Subtracting column 1 from all the others from the above matrix, we get


$$\det B = \det \begin{pmatrix} r & \lambda - r & \dots & \lambda - r \\ \lambda & r - \lambda & \dots & 0 \\ \lambda & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & \dots & r - \lambda \end{pmatrix}$$



Now adding 2, 3, ..., v -th row to the first row we get,

$$\det B = \det \begin{pmatrix} r + \lambda(v-1) & 0 & 0 & \dots & 0 \\ \lambda & r - \lambda & 0 & \dots & 0 \\ \lambda & 0 & r - \lambda & \dots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ \lambda & 0 & \dots & & r - \lambda \end{pmatrix}$$

Now we can see that, the entries above the main diagonal are all 0. Hence determinant is product of the main diagonal elements. Hence

$$\det B = (r - \lambda)^{v-1} (r + \lambda v - \lambda)$$

If $r = \lambda$, each object occurs in r blocks, and each object paired with every other object also occurs in r blocks and hence every block contains all the v elements and the design is trivial. 

e, $r > \lambda$ and B is non singular. M is of rank at most b while B is of rank v . And rank of the product matrix cannot be more than rank of either matrix and hence $b \geq v$ and hence $r \geq k$, which is the Fisher's inequality proved using property of incidence matrices.  \square

We will now see how Fisher's inequality holds for PBD's.

Theorem 1.6.2 *In any nontrivial regular pairwise balanced design, $b \geq v$.*

Proof: From the above proof, the fact that all the blocks having the same size is not used in the proof. Hence Fisher's inequality can be applied to regular pairwise balanced design in which $r > \lambda$. And a regular PBD has $r > \lambda$ if and only if it is not a trivial PBD. Therefore Fisher's inequality is valid for all regular nontrivial PBDs. \square

In this chapter we dealt with balanced incomplete block designs, its properties and incidence matrices. Also we saw when two designs are said to be isomorphic and when BIBD with specified automorphisms exist. We will further see what symmetric BIBD's are and see some main results which deals with necessary and sufficient conditions for the existence of BIBD's.

Chapter 2

Symmetric BIBD's

In the previous chapter we saw what is a BIBD and its properties. In this chapter we specialize what a symmetric BIBD is. The main section of this chapter is the Bruck-Ryser-Chawla theorem which deals with the necessary and sufficient conditions for the existence of a symmetric BIBD. Let us first see what is a symmetric BIBD.

Definition 2.0.3 *Symmetric BIBD*

A BIBD in which $b = v$ is called a symmetric BIBD. Since $bk = vr$, and $b = v$ for a symmetric BIBD, $r = k$. Also since $\lambda(v - 1) = r(k - 1)$ and $r = k$, for a symmetric BIBD it follows that $\lambda(v - 1) = k^2 - k$.

2.1 Properties of Symmetric BIBD's

After looking the definition of symmetric BIBD , now let us see some fundamental properties of BIBD.

Theorem 2.1.1 *Suppose (X, \mathcal{A}) is a symmetric (v, k, λ) -BIBD, let $\mathcal{A} = \{A_1, \dots, A_v\}$. Then $|A_i \cap A_j| = \lambda \forall 1 \leq i, j \leq v, i \neq j$.*

Proof: For the proof of this theorem, we use the notations and equations used in the fisher's inequality. We fix a value h such that $1 \leq h \leq b = v$.

From equations (1.3) and (1.4), we calculate the sum below :

$$\begin{aligned}
 \sum_{\{i:x_i \in A_h\}} \sum_{\{j:x_i \in A_j\}} \mathbf{s}_j &= \sum_{\{i:x_i \in A_h\}} (r - \lambda)\mathbf{e}_i + (\lambda, \dots, \lambda) && \text{from (1.4)} \\
 &= (r - \lambda)\mathbf{s}_h + k(\lambda, \dots, \lambda) \\
 &= (r - \lambda)\mathbf{s}_h + \sum_{j=1}^b \frac{\lambda k}{r} \mathbf{s}_j && \text{from (1.3)}
 \end{aligned}$$

We will now compute the above sum in a different way as done below :

$$\begin{aligned}
 \sum_{\{i:x_i \in A_h\}} \sum_{\{j:x_i \in A_j\}} \mathbf{s}_j &= \sum_{j=1}^b \sum_{\{i:x_i \in A_h \cap A_j\}} \mathbf{s}_j \\
 &= \sum_{j=1}^b |A_h \cap A_j| \mathbf{s}_j
 \end{aligned}$$

Hence, we have from the above two sum calculations that

$$(r - \lambda)\mathbf{s}_h + \sum_{j=1}^b \frac{\lambda k}{r} \mathbf{s}_j = \sum_{j=1}^b |A_h \cap A_j| \mathbf{s}_j$$

Since $b = v$ and $r = k$ in a symmetric BIBD, we have

$$(r - \lambda)\mathbf{s}_h + \sum_{j=1}^v \frac{\lambda k}{r} \mathbf{s}_j = \sum_{j=1}^v |A_h \cap A_j| \mathbf{s}_j$$



In the proof of fisher's inequality we showed that $\mathbf{S} = \mathbb{R}^v$, and since $b = v$, S is a basis of \mathbb{R}^v . \therefore coefficients of any \mathbf{s}_j on the left and right must be the same. Hence, $|A_h \cap A_j| = \lambda \forall j \neq h$. Since h was chosen arbitrary, $|A \cap A'| = \lambda$ for any two different blocks. \square

So we proved above that in a symmetric BIBD any two blocks have λ objects in common. In the following theorem we see how PBD's are related to symmetric BIBD.

Theorem 2.1.2 *Let (X, \mathcal{A}) be a non trivial PBD with $b = v$. Then (X, \mathcal{A}) is a symmetric (v, k, λ) -BIBD.*

Proof: Here, we compute $\sum_{i=1}^v \sum_{\{j:x_i \in A_j\}} \mathbf{s}_j$ in two different ways. Firstly,

$$\begin{aligned} \sum_{i=1}^v \sum_{\{j:x_i \in A_j\}} \mathbf{s}_j &= \sum_{i=1}^v (r - \lambda) \mathbf{e}_i + (\lambda, \dots, \lambda) \\ &= (r - \lambda)(1, \dots, 1) + \lambda v(1, \dots, 1) \\ &= (r - \lambda + \lambda v)(1, \dots, 1) \\ &= \frac{\lambda(v - 1) + r}{r} \sum_{j=1}^b \mathbf{s}_j \quad \text{from (1.3)} \end{aligned}$$

Secondly,

$$\begin{aligned} \sum_{i=1}^v \sum_{\{j:x_i \in A_j\}} \mathbf{s}_j &= \sum_{j=1}^b \sum_{\{i:x_i \in A_j\}} \mathbf{s}_j \\ &= \sum_{j=1}^b |A_j| \mathbf{s}_j \end{aligned}$$

As similar to the above proof, using the fact that $b = v$ and that S is a basis of \mathbb{R}^v , we obtain from the above two calculations that

$$|A_j| = \frac{\lambda(v - 1) + r}{r} \quad \forall 1 \leq j \leq b = v$$

We see that number of elements in each block is the same. Hence (X, \mathcal{A}) is a symmetric (v, k, λ) -BIBD with $k = \frac{\lambda(v-1)+r}{r}$. \square

Let us now see some more properties of symmetric BIBD's along with their incidence matrices.

Corollary 2.1.3 *If M is the incidence matrix of a symmetric (v, k, λ) -BIBD, then M^T is also the incidence matrix of a symmetric (v, k, λ) - BIBD.*

Proof: From Theorem 1.3.8, which tells us the properties of dual design and using the fact that in a symmetric BIBD, $r = k$, it is clear that dual design is also a symmetric (v, k, λ) -BIBD. \square

We will now see a converse to Theorem 2.1.1.

Corollary 2.1.4 *Suppose that μ is a positive integer and (X, \mathcal{A}) is a (v, b, r, k, λ) -BIBD such that $|A \cap A'| = \mu \ \forall A, A' \in \mathcal{A}$. Then (X, \mathcal{A}) is a symmetric BIBD and $\mu = \lambda$.*

Proof: From theorem 1.3.8, dual design of (X, \mathcal{A}) has the properties that each block has r elements, each element appears in k blocks, number of blocks is v and the number of points are b and it is given that $|A \cap A'| = \mu$. Hence dual design of (X, \mathcal{A}) is (b, v, k, r, μ) -BIBD. Fisher's inequality for (X, \mathcal{A}) gives $b \geq v$ and that for the dual design, it gives $v \geq b$. Hence we have $b = v$, which makes (X, \mathcal{A}) a symmetric BIBD. And in a symmetric BIBD, we have any two blocks have λ objects in common, from which it follows that $\mu = \lambda$. \square Let us now see another fundamental property of incidence matrices of symmetric designs.

Theorem 2.1.5 *If M is incidence matrix of a symmetric block design, then M satisfies the following relations.*

$$MM^T = B = (k - \lambda)I + \lambda J \quad (2.1)$$

$$M^T M = B = (k - \lambda)I + \lambda J \quad (2.2)$$

$$MJ = kJ \quad (2.3)$$

$$JM = kJ \quad (2.4)$$

Proof: From equation (1.1) and using the fact that in a symmetric BIBD $r = k$, we get equation (2.1). (2.3) tells us that every row of M has k 1's, his number being the replication number $r = k$ and (2.4) tells us that each column of M has k 1's, which is the case since each block has k objects. Hence it remains to show (2.2), which can be shown as a consequence of the other equations. This will be proved in the following theorem.

Theorem 2.1.6 (Ryser Theorem) *Let M be a non singular $v \times v$ matrix which satisfies either (2.1) or (2.2) and also either (2.3) or (2.4). Then M satisfies all the four equations. Further $k^2 - k = \lambda(v - 1)$*

Proof: We have $\det B = (k - \lambda)^{v-1}(\lambda v - \lambda + k)$. Since M is non singular, we have $k - \lambda \neq 0$ and $(\lambda v - \lambda + k) \neq 0$. Let us first assume (2.1) and (2.3) holds.

$$\begin{aligned} MJ = kJ &\implies M^{-1}(MJ) = M^{-1}kJ \\ &\implies J = kM^{-1}J \\ &\implies k \neq 0, M^{-1}J = k^{-1}J \end{aligned}$$

$$\begin{aligned}
MJ = kJ &\implies (MJ)^T = (kJ)^T \\
&\implies J^T M^T = kJ^T \\
&\implies JM^T = kJ \quad (\because J^T = J)
\end{aligned}$$

We also observe that $J^2 = vJ$. Now we have

$$\begin{aligned}
M^T &= M^{-1}MM^T = M^{-1}(MM^T) \\
&= M^{-1}(k - \lambda)I + \lambda J \\
&= (k - \lambda)M^{-1} + \lambda M^{-1}J \\
&= (k - \lambda)M^{-1} + \lambda k^{-1}J
\end{aligned}$$

$$\begin{aligned}
kJ &= JM^T = J((k - \lambda)M^{-1}) + J(\lambda M^{-1}J) \\
&= (k - \lambda)JM^{-1} + \lambda k^{-1}vJ
\end{aligned}$$

Therefore $JM^{-1} = \frac{(k - \lambda k^{-1})J}{k - \lambda} = mJ$, where m is the constant $\frac{(k - \lambda k^{-1})}{k - \lambda}$. Hence $J = mJM$.

$$\begin{aligned}
vJ &= J^2 = (mJM)J \\
&= (mJ)(MJ) = (mJ)(kJ) \\
&= mkJ^2 = mkvJ \\
\implies v &= mkv \implies mk = 1 \implies m = k^{-1}
\end{aligned}$$

Now we have,

$$m(k - \lambda) = (k - \lambda k^{-1}v) \implies k^{-1}(k - \lambda) = (k - \lambda k^{-1}v)$$

Multiplying by k gives $k - \lambda = k^2 - \lambda v \implies k^2 - k = \lambda(v - 1)$ which is one of the results. We now see that

$$JM^{-1} = mJ = k^{-1}J \implies J = k^{-1}JM \implies kJ = JM$$

Again, we have

$$\begin{aligned}
M^T &= (k - \lambda)M^{-1} + \lambda k^{-1}J \implies M^T M = (k - \lambda)I + \lambda k^{-1}JM \\
&\implies M^T M = (k - \lambda)I + \lambda k^{-1}kJ \\
&\implies M^T M = (k - \lambda)I + \lambda J
\end{aligned}$$

Now we have proved equations (2.2) and (2.4) and the relation $k^2 - k = \lambda(v - 1)$

Now let us assume (2.1) and (2.4) holds.

$$\begin{aligned}
MM^T = (k - \lambda)I + \lambda J &\implies J(MM^T) = (k - \lambda)J + \lambda J^2 \\
&\implies (JM)M^T = (k - \lambda)J + \lambda vJ \\
&\implies kJM^T = (k - \lambda)J + \lambda vJ \\
&\implies kJM^T = (k - \lambda + \lambda v)J = mJ \\
&\implies (kJ)(M^T J) = mJ^2 \\
&\implies mJ^2 = (kJ)(JM)^T = (kJ)(kJ)^T = (kJ)^2 = k^2 J^2 \\
&\implies k^2 = m = k - \lambda + \lambda v \\
&\implies k^2 - k = \lambda(v - 1)
\end{aligned}$$

$$\begin{aligned}
kJM^T = mJ = k^2 J &\implies JM^T = kJ \\
&\implies MJ = (JM^T)^T = (kJ)^T = kJ
\end{aligned}$$

We now have $MJ = kJ = JM$. Now,

$$M^T M = M^{-1}(MM^T)M = (k - \lambda)I + \lambda M^{-1}JM \stackrel{\text{□}}{=} (k - \lambda)I + \lambda M^{-1}MJ = (k - \lambda)I + \lambda J$$

Now we have proved equations (2.2) and (2.3) and the relation. Now we need to prove the theorem by assuming (2.2) and either of (2.3) and (2.4). This can be done by replacing A^T by A . And now we have proved all the parts of the theorem. \square

There are some consequence of this theorem which we have already proved before in this section. If M is the incidence matrix of a symmetric design, (2.2) implies that any two distinct block have λ objects in common. Also it says that M^T is also incidence matrix of symmetric design, which is corollary 2.1.3.

We will now see two more different types of BIBD.

2.2 Residual And Derived BIBD's

We saw from an above theorem that any two blocks of a symmetric BIBD have λ objects in common. Using this fact we construct new BIBD's which we will look upon in this section.

Definition 2.2.1 *Residual and Derived BIBD*

Let (X, \mathcal{A}) be a symmetric (v, k, λ) -BIBD and let $A_0 \in \mathcal{A}$. Define

$$\text{Der}(X, \mathcal{A}, A_0) = (A_0, \{A \cap A_0 : A \in \mathcal{A}, A \neq A_0\})$$

and define

$$\text{Res}(X, \mathcal{A}, A_0) = (X \setminus A_0, \{A \setminus A_0 : A \in \mathcal{A}, A \neq A_0\})$$

as the derived BIBD and residual BIBD respectively.

Derived design is formed by taking a block A_0 and then forming new blocks such that they consist those points common to the old block and A_0 and then deleting A_0 , while the residual design is constructed by deleting all points in a block A_0 .

Let us now look at some of the fundamental properties of residual and derived BIBD's.

Theorem 2.2.2 *Suppose (X, \mathcal{A}) is symmetric (v, k, λ) -BIBD and let $A_0 \in \mathcal{A}$. Then $\text{Der}(X, \mathcal{A}, A_0)$ is a $(k, v - 1, k - 1, \lambda, \lambda - 1)$ -BIBD provided $\lambda \geq 2$, and $\text{Res}(X, \mathcal{A}, A_0)$ is a $(v - k, v - 1, k, k - \lambda, \lambda)$ -BIBD provided that $k \geq \lambda + 2$.*

Proof: Let us first see the case of derived BIBD. Since we choose the points from a particular block A_0 we have the number of points as k . Since we delete the block A_0 , number of blocks is one block less than the previous number $b = v$. Hence the number of blocks in a derived BIBD is $v - 1$. Each element was contained in $r = k$ number of blocks, since we delete the block A_0 , we now have replication number $k - 1$. Each new block has objects common to itself and A_0 . Hence, each block has λ points. Again since we have deleted one block, any two pair of object is contained in $\lambda - 1$ number of blocks.

We have that in a BIBD the number of points in each block is less than the the number of points. Hence in a derived BIBD with the stated parameters gives $k > \lambda \geq 2$. But we have (X, \mathcal{A}) is a symmetric BIBD, and we have $\lambda(v - 1) = k(k - 1)$ and we have $v > k$ which already gives us $k > \lambda$, hence this condition is redundant.

Now lets turn to residual BIBD. By its construction it is clear that number of points is $v - k$ since it is constructed by deleting all the points in a block A_0 and the number of blocks is $v - 1$. Each point is still present in $r =$

k blocks and every block has $k - \lambda$ points since we delete those common to A_0 . Again every pair is present in λ blocks. Hence $\text{Res}(X, \mathcal{A}, A_0)$ is a $(v - k, v - 1, k, k - \lambda, \lambda)$ -BIBD.

Again the stated parameters about the residual BIBD gives us that $v - k > k - \lambda \geq 2$ by the similar arguments from above; i.e it $v > 2k - \lambda$. Now we prove that in a symmetric BIBD this condition is already present and this condition is superfluous. Suppose $v \leq 2k - \lambda$, then

$$k(k-1) = \lambda(v-1) \leq \lambda(2k-\lambda-1) \implies k(k-1) - \lambda(2k-\lambda-1) \leq 0 \implies (k-\lambda)(k-\lambda-1) \leq 0$$

This holds if and only if $k = \lambda$ or $k = \lambda + 1$. But we have assumed that $k \geq \lambda + 2$, and we reach a contradiction. Therefore $v > 2k - \lambda$ in a symmetric BIBD and the condition is redundant. \square

Let $(v - k, v - 1, k, k - \lambda, \lambda)$ residual BIBD be $(v', b', r', k', \lambda')$ -BIBD, then it can be seen that $r' = k' + \lambda'$. A (v, b, r, k, λ) -BIBD with $r = k + \lambda$ is called a *quasiresidual* BIBD, which can be constructed as the residual design of a symmetric $(v + r, r, \lambda)$ -BIBD, provided it exists. Similarly in a derived BIBD $k' = \lambda' + 1$. A $((v, b, r, k, \lambda)$ -BIBD with $k = \lambda + 1$ is called a *quasiderived* BIBD, which can be constructed as derived design of a symmetric $(b + 1, r + 1, \lambda + 1)$ -BIBD if it exists.

2.3 Projective Planes And Geometries

In this section we see what projective planes are and then we see its relation to symmetric BIBD's. Let us start here with the definition of projective planes.

Definition 2.3.1 Projective Planes

An $(n^2 + n + 1, n + 1, 1)$ -BIBD with $n \geq 2$ is called a projective plane of order n . Here $1(n^2 + n) = (n + 1)(n)$, hence projective plane is a symmetric BIBD. We will now see through the following theorem, for what values of n the projective plane exists.

Theorem 2.3.2 For every prime power $q \geq 2$, there exists a symmetric $(q^2 + q + 1, q + 1, 1)$ -BIBD, i.e a projective plane of order q .

Proof: We prove here that a projective plane of order q exists whenever q is prime power. Suppose q is a prime power. Let \mathbb{F}_q be the finite field of order q and let \mathbf{V} be the three dimensional subspace. Let \mathcal{V}_1 consists of all the one dimensional subspace of \mathbf{V} and \mathcal{V}_2 consists of all the two dimensional subspaces of \mathbf{V} . For each $B \in \mathcal{V}_2$, define a block

$$A_B = \{C \in \mathcal{V}_1 : C \subseteq B\}$$

and define

$$\mathcal{A} = \{A_B : B \in \mathcal{V}_2\}.$$

We can see that number of elements in each one dimensional subspace is q , hence $|C| = q$. and $(0, 0, 0) \in C \forall C \in \mathcal{V}_1$. Hence the sets $C \setminus \{(0, 0, 0)\}$ form a partition of $\mathbf{V} \setminus \{(0, 0, 0)\}$ whose cardinality is $q^3 - 1$. Hence

$$|\mathcal{V}_1| = \frac{q^3 - 1}{q - 1} = q^2 + q + 1.$$

Now let $B \in \mathcal{V}_2$, we have the cardinality of each two dimensional subspace is q^2 , hence $|B| = q^2$. The sets $C \setminus \{(0, 0, 0)\}$ such that $C \in \mathcal{V}_1$ and $C \subseteq B$ from a partition of $B \setminus \{(0, 0, 0)\}$. Hence

$$|A_B| = \frac{q^2 - 1}{q - 1} = q + 1.$$

Finally there is unique two dimensional subspace B containing two distinct one dimensional subspaces. This subspace determines the block A_B containing the two distinct one dimensional subspace. Hence, there exists a projective plane $(\mathcal{V}_1, \mathcal{A})$ of order q , ie $(q^2 + q + 1, q + 1, 1)$ -BIBD. \square

We saw above that projective plane of order of a prime power q exists, but existence of projective planes of non prime power order is still an open question. But we will see later that projective planes of certain non prime power orders does not exist.

Definition 2.3.3 *Affine Plane*

Let $n \geq 2$. An $(n^2, n^2 + n, n + 1, n, 1)$ -BIBD is called an affine plane of order n .

Theorem 2.3.4 *For every prime $q \geq 2$, there exists an affine plane of order q i.e a $(q^2, q, 1)$ -BIBD.*

Proof: From theorem 2.3.2, \exists a $(q^2 + q + 1, q + 1, 1)$ -BIBD and the residual design from this is $(q^2, q^2 + q, q + 1, q, 1)$ -BIBD (from theorem 2.2.2) which is an affine plane of order q . \square

Warning: The derived design of a projective plane has block size 1 and hence is not a BIBD.

The projective planes we have constructed above are regarded as projective geometries and is denoted by $PG_2(q)$. We now generalize theorem 2.3.2 to higher dimensions and by taking $\mathbf{V} = (\mathbb{F}_q)^{d+1}$. We now state this result as a theorem (without proof).

Theorem 2.3.5 *Suppose $q \geq 2$ be a prime power and $d \geq 2$ be an integer. Then there exists a symmetric $\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right)$ -BIBD.*

The points and blocks of this BIBD would represent the points and hyperplanes of d dimensional projective geometry $PG_d(q)$. Now we will see a corollary to this theorem, which tells us the derived and residual BIBD's constructed from the above BIBD.

Corollary 2.3.6 *Suppose $q \geq 2$ be a prime power and $d \geq 2$ be an integer. Then there exists a $\left(q^d, q^{d-1}, \frac{q^{d-1}-1}{q-1}\right)$ -BIBD and a $\left(\frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}, \frac{q(q^{d-2}-1)}{q-1}\right)$ -BIBD.*

Proof: From the above theorem there exists a $\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right)$ -BIBD. Now from theorem 2.2.2 we can construct derived and residual BIBD from this. The residual BIBD will have the first parameter

$$\frac{q^{d+1} - 1 - q^d + 1}{q - 1} = \frac{q^d(q - 1)}{q - 1} = q^d$$

The second parameter is as follows:

$$\frac{q^d - 1 - q^{d-1} + 1}{q - 1} = \frac{q^d(1 - \frac{1}{q})}{q - 1} = \frac{q^d}{q} = q^{d-1}$$

And the third parameter is $\frac{q^{d-1}-1}{q-1}$. Hence there exists a $\left(q^d, q^{d-1}, \frac{q^{d-1}-1}{q-1}\right)$ -BIBD.

Now let us see how the derived BIBD would look like. It will be a

$$\left(\frac{q^d - 1}{q - 1}, \frac{q^{d-1} - 1}{q - 1}, \frac{q^{d-1} - 1}{q - 1} - 1\right) - \text{BIBD}.$$

Let us now examine the third parameter


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

which is the desired result. \square

We will now look at the most fundamental theorem on the existence of symmetric BIBD, which we will explore in the next section.


2.4 Bruck-Ryser-Chowla Theorem

Bruck-Ryser-Chowla theorem is the most fundamental theorem which talks about the conditions for the existence of symmetric designs. This theorem has two parts which will look upon one by one.

Theorem 2.4.1 (Bruck-Ryser-Chowla Theorem, v even)  Suppose there exists a symmetric (v, k, λ) -BIBD. If v is even, then $k - \lambda$ is a perfect square.

Proof: Let M be the incidence matrix of symmetric (v, k, λ) -BIBD. In a symmetric design, we have $b = v$ and $r = k$. Since M is a square matrix, $\det MM^T = \det(M)^2 = \det B = (k - \lambda)^{v-1}(v\lambda - \lambda + k)$.

Since $\lambda(v - 1) = k(k - 1)$, we have $v\lambda - \lambda + k = k(k - 1) + k = k^2$. Hence we have $\det(M)^2 = (k - \lambda)^{v-1}k^2$. This implies that $(k - \lambda)^{v-1}$ is a square, and since v is even, it must be the case that $k - \lambda$ is also a square, which is the desired result. \square

Now we will see what happens when v is odd. Before stating the theorem  we will need some results to prove it, which we will state here without the proof.

Lemma 2.4.2 (Lagrange's Theorem) Every positive integer n can be represented as the sum of squares of four integers, i.e $n = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

Lemma 2.4.3 Suppose that $C = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ -a_1 & a_0 & -a_3 & a_2 \\ -a_2 & a_3 & a_0 & -a_1 \\ -a_3 & -a_2 & a_1 & a_0 \end{pmatrix}$ and let $n = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Then $C^{-1} = \frac{1}{n}C^T$.

Now let us see the case when v is odd:



Theorem 2.4.4 (Bruck-Ryser-Chowla Theorem, v odd) Suppose there exists a symmetric (v, k, λ) -BIBD with v odd. Then there exist integers x, y , and z (not all 0) such that $x^2 = (k - \lambda)y^2 + (-1)^{\frac{v-1}{2}}\lambda z^2$.

Proof: First let us suppose $v \equiv 1 \pmod{4}$ and we denote $v = 4w + 1$. Let M be the incidence matrix of (v, k, λ) -BIBD. In the previous chapter we saw how relation (1.2) can be written as a relation on quadratic forms. Let x_1, \dots, x_v be the indeterminates, and for $1 \leq j \leq v$, let L_j be as defined before. We have the relation

$$\sum_{j=1}^v L_j^2 = \lambda \left(\sum_{i=1}^v x_i \right)^2 + (k - \lambda) \sum_{i=1}^v x_i^2. \quad (2.5)$$

We now transform variables x_1, \dots, x_v to new variables y_1, \dots, y_v such that each y_i is an integral linear combination of x_j 's. Since $k - \lambda$ is a positive integer, from Lagrange's theorem, we can express $k - \lambda = a_0^2 + a_1^2 + a_2^2 + a_3^2$, where a_0, a_1, a_2, a_3 are integers. Let C be the matrix as defined above. Then for $1 \leq h \leq w$, let

$$(y_{4h-3}, y_{4h-2}, y_{4h-1}, y_{4h}) = (x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})C$$

and let $y_v = x_v$. Finally, let $y_0 = x_1 + \dots + x_v$.

Now for $1 \leq h \leq w$, we have



$$\begin{aligned} y_{4h-3}^2 + y_{4h-2}^2 + y_{4h-1}^2 + y_{4h}^2 &= (y_{4h-3}, y_{4h-2}, y_{4h-1}, y_{4h})(y_{4h-3}, y_{4h-2}, y_{4h-1}, y_{4h})^T \\ &= ((x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})C)((x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})C)^T \\ &= (x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})CC^T(x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})^T \\ &= (x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})(k - \lambda)I_4(x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})^T \\ &= (k - \lambda)(x_{4h-3}^2 + x_{4h-2}^2 + x_{4h-1}^2 + x_{4h}^2) \end{aligned}$$

Since $v = 4w + 1$, we have

$$\sum_{i=1}^{v-1} y_i^2 = (k - \lambda) \sum_{i=1}^{v-1} x_i^2$$

Therefore we now obtain,

$$\sum_{j=1}^v L_j^2 = \lambda y_0^2 + \sum_{i=1}^{v-1} y_i^2 + (k - \lambda)y_v^2$$

We here observe that L_j 's were defined as integral linear combination of x_j 's. We can now express x_j as a rational linear combination of y_1, \dots, y_v and y_0 as a rational linear combination of y_1, \dots, y_v . So, the equation we obtained above can be seen as an identity in indeterminates y_1, \dots, y_v with rational coefficients. We can breakdown this expression further by expressing any of the indeterminate as a rational linear combination of the other indeterminates and the new expression will still be an identity in the remaining indeterminates with rational coefficients.

Let $L_1 = c_1 y_1 + \dots + c_v y_v$. If $c_1 = 1$, let $y_1 = -L_1$ and if not let $y_1 = L_1$. By this scheme we have expressed y_1 as a rational linear combination of y_2, \dots, y_v such that $L_1^2 = y_1^2$. And hence the above relation will now become,

$$\sum_{j=2}^v L_j^2 = \lambda y_0^2 + \sum_{i=2}^v -1 y_i^2 + (k - \lambda) y_v^2.$$

We proceed in this fashion eliminating the indeterminates y_2, \dots, y_v one at a time by expressing each y_i as rational linear combination of y_{i+1}, \dots, y_v such that $y_i^2 = L_i^2 \forall i$. So finally we will get

$$L_v^2 = \lambda y_0^2 + (k - \lambda) y_v^2$$

where L_v and y_0 are rational multiples of y_v . Hence let us suppose that $L_v = s y_v$ and $y_0 = t y_v$ where $s, t \in \mathbb{Q}$. Let $y_v = 1$, and then the equation becomes

$$s^2 = \lambda t^2 + (k - \lambda)$$

. Now we write $s = \frac{m}{n}$ and $t = \frac{p}{q}$ where $m, n, p, q \in \mathbb{Z}$ and $n, q \neq 0$. Now incorporating these into the equation, it now becomes,

$$(mq)^2 = \lambda(np)^2 + (k - \lambda)(nq)^2.$$

Let $x = mq, y = nq, z = np$. It is clear that $x, y, z \in \mathbb{Z}$. Hence we have an integral solution to the equation $x^2 = (k - \lambda)y^2 + (-1)^{\frac{v-1}{2}} \lambda z^2$. Note that since v is odd and $v = 4w + 1, v - 1 = 4w$ and $\frac{v-1}{2}$ is always even and $(-1)^{\frac{v-1}{2}} = 1$. Now we need to look the case when $v \equiv 3 \pmod{4}$. We denote $v = 4w - 1$. Here we introduce a new indeterminate x_{v+1} and we add $(k - \lambda)x_{v+1}^2$ to both sides of equation (2.5). We now have

$$\sum_{j=1}^v L_j^2 + (k - \lambda)x_{v+1}^2 = \lambda \left(\sum_{i=1}^v x_i \right)^2 + (k - \lambda) \sum_{i=1}^{v+1} x_i^2.$$

For $1 \leq h \leq w$, let

$$(y_{4h-3}, y_{4h-2}, y_{4h-1}, y_{4h}) = (x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})C.$$

and let $y_0 = x_1 + \dots + x_v$ and we have

$$y_{4h-3}^2 + y_{4h-2}^2 + y_{4h-1}^2 + y_{4h}^2 = (k - \lambda)(x_{4h-3}^2 + x_{4h-2}^2 + x_{4h-1}^2 + x_{4h}^2).$$

And since $v = 4w - 1$, we have

$$\sum_{i=1}^{v+1} y_i^2 = (k - \lambda) \sum_{i=1}^{v+1} x_i^2.$$

Therefore our equation now becomes

$$\sum_{j=1}^v L_j^2 + (k - \lambda)x_{v+1}^2 = \lambda y_0^2 + \sum_{i=1}^{v+1} y_i^2.$$

Now proceeding as in the above case , we obtain

$$(k - \lambda)x_{v+1}^2 = \lambda y_0^2 + y_{v+1}^2 \implies y_{v+1}^2 = (k - \lambda)x_{v+1}^2 - \lambda y_0^2$$

Hence we have obtained integral solution to the equation $x^2 = (k - \lambda)y^2 + (-1)^{\frac{v-1}{2}} \lambda z^2$. Here since $v = 4w' + 3$, $v - 1 = 4w' + 2$ and $\frac{v-1}{2} = 2w' + 1$ which is odd. Hence $(-1)^{\frac{v-1}{2}} = -1$, which is the desired result. \square



As an application of this theorem we will show that a $(43, 7, 1)$ -BIBD does not exist.



If this BIBD exist , then there must exist integer solutions to the equation $x^2 + z^2 = 6y^2$. Let $x + y + z$ be as small as possible. This equation is possible only when both x and z are both odd or both even. If both x and z are both odd, then we have $x^2 \equiv 1 \pmod{8}$ and $z^2 \equiv 1 \pmod{8}$ and hence $x^2 + z^2 \equiv 2 \pmod{8}$. But if y is odd, $6y^2 \equiv 6 \pmod{8}$ and if y is even $6y^2 \equiv 0 \pmod{8}$. Hence LHS and RHS does not satisfy each other and we discard the case. Then , x and z are both even. Since 4 divides LHS, 4 should divide RHS as well and hence y is also even. Then we can replace x, z and y by $2r, 2s$ and $2t$. Hence the equation now becomes $r^2 + s^2 = 6t^2$. Hence r, s, t satisfy the same relation which implies they integer solutions of the same equation. But $r + s + t = \frac{x+y+z}{2} < x + y + z$, which is a contradicts our choice of x, y, z . Hence the equation has no integer solutions and therefore $(43, 7, 1)$ -BIBD does not exist.



Next we analyze the conditions of the theorem in a projective plane of arbitrary order n . Firstly, let $n \equiv 0, 3 \pmod{4}$. Here $v = n^2 + n + 1$, $\lambda = 1$. When $n = 4w$, $v = n^2 + n + 1 = 16w^2 + 4w + 1$, $v - 1 = 16w^2 + 4w$, $\frac{v-1}{2}$ is even. And when $n = 4w + 3$, $v = n^2 + n + 1 = 16w^2 + 28w + 13$, $v - 1 = 16w^2 + 28w + 12$, $\frac{v-1}{2}$ is even. Hence it should satisfy the equation $x^2 = ny^2 + z^2$, which always have a non trivial solution $x = 1, y = 0, z = 1$. Hence when $n \equiv 0, 3 \pmod{4}$, the theorem does not yield any non existent results for $(n^2 + n + 1, n + 1, 1) - BIBD$.

Now let us analyse the case when $n \equiv 1, 2 \pmod{4}$. When $n = 4w + 1$, $\frac{v-1}{2} = \frac{n^2+n}{2} = \frac{16w^2+12w+2}{2}$ is odd. And when $n = 4w + 2$, $\frac{v-1}{2} = \frac{n^2+n}{2} = \frac{16w^2+20w+6}{2}$ is odd. Hence, we need to get integer solutions for the equation $x^2 + z^2 = ny^2$. We need to see the conditions when this equation have non zero integral solutions. Though we dont give a proof here, it is shown that the equation yield solutions if and only if $x^2 + z^2 = n$ has integral solution (x, z) . We use some results from number theory without proof to analyze when the above equation yields solutions of the required type.

Theorem 2.4.5 *A positive integer n can be expressed as the sum of two integral squares if and only if there does not exist a prime $p \equiv 3 \pmod{4}$ such that the largest power of p that divides n is odd.*

Using this theorem we obtain the following result.

Theorem 2.4.6 *Suppose that $n \equiv 1, 2 \pmod{4}$, and there exist a prime $p \equiv 3 \pmod{4}$ such that the largest power of p that divides n is odd, then a projective plane of order n does not exist.*



Proof: Since there exist a prime $p \equiv 3 \pmod{4}$ such that the largest power of p that divides n is odd, n cannot be expressed as the sum of two integral squares, and by the above discussion a projective plane of order n does not exist. \square

We now look at the case of arbitrary λ to see when BIBD of certain values does not exist. To analyze this we introduce the concept of quadratic residues and we also use a theorem for the same.

Definition 2.4.7 *Quadratic residue*

Suppose $m \geq 2$ is an integer and a is any integer, then a is quadratic residue modulo m , if $x^2 \equiv a \pmod{m}$ has a solution $x \in \mathbb{Z}_m \setminus \{0\}$.

Theorem 2.4.8 (Euler's criterion) *An integer a is quadratic residue modulo the odd prime p if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Definition 2.4.9 *Square-free integers*

A positive integer is called square free if it is not divisible by j^2 for any integer $j > 1$. Any positive integer n can be written uniquely as $n = A^2 n_1$, where A is a positive integer and n_1 is square free. n_1 is called the square free part of n .

We will now see the theorem which tells us the conditions when a BIBD does not exist.

Theorem 2.4.10 *Suppose that v, k, λ are positive integers such that $\lambda(v-1) = k(k-1)$ where $v > k \geq 2$. Let λ_1 be the square free part of λ and n_1 be the square free part of $k-\lambda$. Suppose that p is an odd prime such that $n_1 \equiv 0 \pmod{p}$, $\lambda_1 \not\equiv 0 \pmod{p}$ and $(-1)^{\frac{v-1}{2}} \lambda_1$ is not a quadratic residue modulo p . Then there does not exist a (v, k, λ) -BIBD.*

Proof: To prove this we will show that the equation $x^2 = (k-\lambda)y^2 + (-1)^{\frac{v-1}{2}} \lambda z^2$ does not have integral solution $(x, y, z) \neq (0, 0, 0)$. Let us assume the equation have a non zero integral solution. We can replace $k-\lambda$ by $A^2 n_1$ and λ by $B^2 \lambda_1$. Then the equation will be $x^2 = n_1 (Ay)^2 + (-1)^{\frac{v-1}{2}} \lambda_1 (Bz)^2$. Letting $y_1 = Ay, z_1 = Bz$, the equation will be

$$x^2 = n_1 y_1^2 + (-1)^{\frac{v-1}{2}} \lambda_1 z_1^2. \quad (2.6)$$

And this will have non zero integral solution (x, y_1, z_1) . We can assume without loss of generality that $\gcd(x, y_1, z_1) = 1$ (Since if $\gcd = d > 1$, then we can divide by d to get a solution whose $\gcd = 1$.)

Let $z_1 \equiv 0 \pmod{p}$. Since $n_1 \equiv 0 \pmod{p}, x \equiv 0 \pmod{p}$. But if both z_1 and x are divisible by p , then z_1^2 and x^2 are both divisible by p^2 and therefore $n_1 y_1^2$ must be divisible by p^2 . Since n_1 is square free, n_1 is not divisible by p^2 . Hence p^2 divides y_1^2 and p divides y_1 . Therefore $\gcd(x, y_1, z_1) \geq p$ which is a contradiction. Hence $z_1 \not\equiv 0 \pmod{p}$. We consider (2.5), and going modulo p , and since $n_1 \equiv 0 \pmod{p}, \lambda_1 \not\equiv 0 \pmod{p}$, we get

$$x^2 \equiv (-1)^{\frac{v-1}{2}} \lambda_1 z_1^2 \pmod{p} \implies (xz_1^{-1})^2 \equiv (-1)^{\frac{v-1}{2}} \lambda_1 \pmod{p}.$$

This gives us $(-1)^{\frac{v-1}{2}} \lambda_1$ is a quadratic residue modulo p , which is a contradiction. Hence (v, k, λ) -BIBD does not exist. \square

As an application of this theorem we derive theorem 2.4.6 as a corollary of this theorem.

Example 2.4.11

Suppose that $n \equiv 1, 2 \pmod 4$ and there exist a prime $p \equiv 3 \pmod 4$ such that the largest power of p that divides n is odd. We need to show using the above theorem that $(n^2 + n + 1, n + 1, 1)$ -BIBD does not exist. We have $\lambda_1 = \lambda = 1 \not\equiv 0 \pmod p, k - \lambda = n$. Since the largest power of p that divides n , say α is odd,

$$\frac{n}{p^\alpha} = \frac{A^2 n_1}{p^\alpha} = \left(\frac{A}{p'}\right)^2 \frac{n_1}{p} \implies n_1 \equiv 0 \pmod p.$$

Now the conditions of the theorem are satisfied. So according to the theorem we need to show that $(-1)^{\frac{v-1}{2}}$ is not a quadratic residue modulo p . $(-1)^{\frac{v-1}{2}} = (-1)^{\frac{n^2+n}{2}} = -1$ ($\because n \equiv 1, 2 \pmod 4$). If -1 is a quadratic residue modulo p , then $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$. But $(-1)^{\frac{p-1}{2}} = (-1)^{2w+1} = -1 \not\equiv 1 \pmod p$ ($\because p = 4w + 3$). Hence $(-1)^{\frac{v-1}{2}}$ is not a quadratic residue modulo p . Hence projective plane of order n does not exist in the given conditions.

We have for a symmetric BIBD, $MM^T = (k - \lambda)I + \lambda J$. And we saw that in quadratic forms it is of the form, it takes the form

$$L_1^2 + \dots + L_v^2 = (k - \lambda)(x_1^2 + \dots + x_v^2) + \lambda(x_1 + \dots + x_v)^2 \quad (2.7)$$

where $L_j = \sum_{i=1}^v a_{ij}x_i$.

We saw above that Bruck-Ryser-Chowla theorem gives necessary conditions for the existence of matrix M satisfying incidence equation, or for the existence of rational linear forms L_j satisfying equation (2.7). We will see that these conditions are infact sufficient for the rational solution of incidence equation and equation (2.7). This require Hasse-Minkowski theorem for its proof which we will see in the next section. But some cases can be proved directly which we will see here .

Firstly, if $k - \lambda$ is a square, then we need to prove that there exist a matrix M with rational entries such that $MM^T = (k - \lambda)I + \lambda J$. Let $M = pI + qJ$. If there should exist such a matrix then it should satisfy the above incidence equation. Note that $M^T = pI + qJ^T = pI + qJ = M$. Hence $MM^T = M^2 = (pI + qJ)^2 = p^2I + q^2vJ + 2pqJ = p^2I + (q^2v + 2pq)J = (k - \lambda)I + \lambda J$.

And we obtain

$$p^2 = k - \lambda \implies p = \sqrt{k - \lambda}.$$

Also,

$$q^2 v + 2pq = \lambda \implies vq^2 + 2pq - \lambda = 0 \implies q = \frac{-2p + \sqrt{4p^2 + 4v\lambda}}{2v} \implies q = \frac{-p + \sqrt{p^2 + v\lambda}}{v}.$$

$$p^2 + v\lambda = k - \lambda + v\lambda = k + \lambda(v - 1) = k + k^2 - k = k^2.$$

Hence $q = \frac{-(\sqrt{k-\lambda})+k}{v}$. Hence the matrix M takes the form

$$M = \sqrt{k - \lambda}I + \frac{-(\sqrt{k - \lambda}) + k}{v}J.$$

Also we have $L_j = a_{ij}x_i = \sqrt{k - \lambda}x_1 + \frac{-(\sqrt{k-\lambda})+k}{v}(x_1 + \dots + x_v)$.

This proves the sufficiency of first condition of Bruck Ryser-Chowla theorem, when v is even. Also it includes the cases when v is odd and $k - \lambda$ happens to be a square. To prove the sufficiency of second condition of Bruck-Ryser-Chowla theorem for rational solution of (2.7) we need Hasse-Minkowski theorem which we will look upon in the next section.



2.5 Statement Of Hasse-Minkowski And Applications

We will first see some definitions and state some theorems from number theory which we will use to state Hasse-Minkowski theorem and also to prove the rational converse.

In the previous section we saw what are quadratic residues. Let p be an odd prime. The integers $a \not\equiv 0 \pmod p$ can be divided to quadratic residues and quadratic non residues if $x^2 \equiv a \pmod p$ have or does not have a solution $x \pmod p$. This can be expressed by *Legendre Symbol* which is described below.

$$\left(\frac{a}{p}\right) = 1 \quad \text{if } a \text{ is a quadratic residue modulo } p$$

$$\left(\frac{a}{p}\right) = -1 \quad \text{if } a \text{ is not a quadratic residue modulo } p$$

We now state some theorems of quadratic residues and non residues.

Theorem 2.5.1 *If p is an odd prime, then*

$$a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \quad (2.8)$$

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p} \quad (2.9)$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \quad (2.10)$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad (2.11)$$

In the next theorem, we will see the deeper relations concerning two odd primes. This theorem along with the previous one makes the evaluation of legendre symbol easier.

Theorem 2.5.2 (Law of quadratic reciprocity) *If p and q are two odd primes, then*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad (2.12)$$

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \quad (2.13)$$

We will now look at theorem which deals with congruence modulo powers of a prime p .

Theorem 2.5.3 *Let p be a prime and let $b = p^a b_1$, where p does not divide b_1 . Then for arbitrary high powers of p , the congruence $x^2 \equiv b \pmod{p^n}$ if and only if a is even, $\left(\frac{b_1}{p}\right) = 1$, for p odd and $b_1 \equiv 1 \pmod{8}$ if $p = 2$.*

Let us now see a definition and a theorem from which we will lead to the main theorem in this section, the Hasse-Minkowski theorem.

Definition 2.5.4 *Hilbert Norm Residue symbol*

The hilbert norm residue symbol, denoted by $(b, c)_p$ takes the value $+1$ or -1 accordingly as $bx^2 + cy^2 \equiv z^2 \pmod{p^m}$ does or does not have integer solutions x, y, z , not all multiples of p for arbitrarily high powers of p . The case when $p = \infty$ is decided accordingly as $bx^2 + cy^2 = z^2$ does or does not have real solutions x, y, z not all zero. Hence $(b, c)_\infty = 1$ unless both b and c are negative.

Theorem 2.5.5 *The equation $bx^2 + cy^2 = z^2$ has solutions in integers x, y, z not all zero if and only if $(b, c)_p = 1$ for all primes p including $p = \infty$.*

Hasse-Minkowski theorem gives us the conditions for rational equivalence of any two rational quadratic forms which are expressible in terms of the hasse symbol $c_p(f)$ defined for a quadratic form

$$f = \sum_{i,j=1}^m b_{ij}x_i x_j; b_{ij} = b_{ji}$$

and primes p including $p = \infty$. We define for $r = 1, \dots, m$, the r^{th} leading principal minor of $B = (b_{ij})$, as

$$D_r = \det(b_{ij}) \quad i, j = 1, \dots, r.$$

Here, we shall suppose that b 's are all integers and D_1, \dots, D_m are all different from 0. Now we will define $c_p(f)$ for those f which takes the form above and all primes p , as

$$c_p(f) = (-1, D_m)_p \prod_{i=1}^{m-1} (D_i, -D_{i+1})_p.$$

Having stated all the requirements, we will now see the major Hasse-Minkowski theorem.

Theorem 2.5.6 (Hasse-Minkowski Theorem) *If f_1 and f_2 are integral quadratic forms in m variables, none of whose leading principal minors vanishes, then a necessary and a sufficient condition that f_1 and f_2 are rationally equivalent is that $c_p(f_1) = c_p(f_2)$ for all odd primes and $p = \infty$.*

The following theorem makes the computation of hilert norm residue symbol easier.

Theorem 2.5.7 *Hilbert norm residue symbol has the following properties:*

$$\prod_{\forall \text{primes}}^{\infty} (b, c)_p = 1 \tag{2.14}$$

$$(b, c)_p = (c, b)_p \tag{2.15}$$

$$(b_1, b_2, c)_p = (b_1, c)_p (b_2, c)_p \tag{2.16}$$

$$(bd^2, ce^2)_p = (b, c)_p \tag{2.17}$$

$$(b, -b)_p = 1 \tag{2.18}$$

$$(b^2, c)_p = 1 \tag{2.19}$$

If p is an odd prime,

$$(b, c)_p = 1, \quad \text{if } b \text{ and } c \text{ are prime to } p. \quad (2.20)$$

$$(b, b)_p = \left(\frac{b}{p}\right), \quad \text{if } b \not\equiv 0 \pmod{p}. \quad (2.21)$$

$$(p, p)_p = (-1, p)_p \quad (2.22)$$

$$(b_1, c)_p = (b_2, c)_p, \quad \text{if } b_1 = b_2 \not\equiv 0 \pmod{p}. \quad (2.23)$$

We have excluded $p = 2$ in the Hasse-Minkowski theorem whose reason we will see now. We have

$$\begin{aligned} \prod_{p=2}^{\infty} c_p(f) &= \prod_{p=2}^{\infty} (-1, D_m)_p \prod_{i=1}^{m-1} (D_i, -D_{i+1})_p \\ &= \prod_{p=2}^{\infty} (-1, D_m)_p \prod_{i=1}^{\infty} \prod_{i=1}^{m-1} (D_i, -D_{i+1})_p \\ &= \prod_{p=2}^{\infty} (-1, D_m)_p \prod_{i=1}^{m-1} \prod_{i=1}^{\infty} (D_i, -D_{i+1})_p \\ &= \prod_{p=2}^{\infty} 1 \prod_{i=1}^{m-1} \prod_{i=1}^{\infty} 1 \quad \text{from (2.14)} \\ &= 1 \end{aligned}$$

If $c_p(f_1) = c_p(f_2)$ for all primes starting from 3, then $\prod_{p \geq 3} c_p(f_1) = \prod_{p \geq 3} c_p(f_2)$.

Also we have $\prod_{p=2}^{\infty} c_p(f) = 1$. from these we get

$$\prod_{p=2}^{\infty} c_p(f_1) = \prod_{p=2}^{\infty} c_p(f_2) \implies c_2(f_1) \prod_{p \geq 3} c_p(f_1) = c_2(f_2) \prod_{p \geq 3} c_p(f_2) \implies c_2(f_1) = c_2(f_2).$$

Hence we can exclude $p = 2$ from consideration in Hasse-Minkowski theorem.

Having stated the Hasse-Minkowski theorem, we will now see the rational converse of the second condition of Bruck-Ryser-Chowla theorem. We saw above that the incidence equation (1.2) is equivalent to equation (2.5). Thus the existence of a rational matrix M satisfying (1.2) is equivalent to the existence of a rational transformation taking the form $x_1^2 + \cdots + x_v^2$ to the

form $(k - \lambda)(x_1^2 + \dots + x_v^2) + \lambda(x_1 + \dots + x_v)^2$. Now we have to show that the rational solution of (2.5), when v is odd is equivalent to the existence of integers x, y, z not all zero satisfying the equation $(k - \lambda)x^2 + (-1)^{\frac{v-1}{2}} \lambda y^2 = z^2$. Here the rational forms are

$$f_1 = (k - \lambda)(x_1^2 + \dots + x_v^2), f_2 = x_1^2 + \dots + x_v^2.$$

For f_1 , for $r = 1, \dots, v$, (let $k - \lambda = n$), we have from the definitions above,

$$\begin{aligned} D_r &= \det \begin{pmatrix} n + \lambda & \lambda & \dots & \lambda \\ \lambda & n + \lambda & & \lambda \\ \vdots & & \ddots & \vdots \\ \lambda & \lambda & \dots & n + \lambda \end{pmatrix} \\ &= (n + \lambda - \lambda)^{r-1} (r\lambda - \lambda + n + \lambda) \\ &= n^{r-1} (k + (r - 1)\lambda) \text{ from the calculation used in the previous chapter} \end{aligned}$$

Hence we have $D_i = n^{i-1} (k + (i - 1)\lambda)$. Since all the D 's are positive and since $(b, c)_\infty = 1$ unless both b and c are negative we have $c_\infty(f_1) = -1$.

For f_2 , for $r = 1, \dots, v$, $D_r = \det I_r = 1$.

$$c_\infty(f_2) = (-1, -1)_\infty \prod_{i=1}^{v-1} (1, -1)_\infty = -1 \cdot 1 = -1. \text{ Hence we have } c_\infty(f_1) =$$

$$c_\infty(f_2).$$

Now,

$$\begin{aligned} c_p(f_2) &= (-1, -1)_p \prod_{i=1}^{v-1} (1, -1)_p \\ &= (-1, -1)_p 1 \quad \text{from (2.18)} \\ &= 1 \quad \text{from (2.20)} \end{aligned}$$

So for f_1 and f_2 to be rationally equivalent we need to further show that $c_p(f_1) = 1$ for all odd primes. Let us now evaluate $c_p(f_1)$. We have $c_p(f_1) =$

$$(-1, D_v)_p \prod_{i=1}^{v-1} (D_i, -D_{i+1})_p.$$

Let $E_i = k + (i - 1)\lambda \quad \forall i = 1, \dots, v..$ We have $E_v = k + (v - 1)\lambda = k + k(k - 1) = k^2..$ And since v is odd, n^{v-1} is a square. Hence we have

$$(-1, -D_v)_p = (-1, -n^{v-1}k^2)_p = (-1, 1, -1 \cdot n^{v-1}k^2)_p = (-1, -1)_p = 1 \text{ from (2.17, 2.20).}$$

Now,

$$\begin{aligned}
c_p(f_1) &= \prod_{i=1}^{v-1} (D_i, -D_{i+1})_p \\
&= \prod_{i=1}^{v-1} (n^{i-1}E_i, -n^iE_{i+1})_p \\
&= \prod_{i=1}^{v-1} (n^{i-1}, -n^i)_p (n^{i-1}, E_{i+1})_p (E_i, n^i)_p (E_i, -E_{i+1})_p \quad \text{from (2.16)}
\end{aligned}$$

When i is even, $(n^{i-1}, -n^i)_p = (n^{i-2}n, -1.n^i)_p = (n, -1)_p$. and if i is odd ,
 $(n^{i-1}, -n^i)_p = (1, -n)_p = 1$, from (2.19). Hence $\prod_{i=1}^{v-1} (n^{i-1}, -n^i)_p = (n, -1)_p^{\frac{v-1}{2}}$.

$$\begin{aligned}
\prod_{i=1}^{v-1} (n^{i-1}, E_{i+1})_p &= \prod_{i=1}^{v-1} (n^2n^{i-1}, E_{i+1})_p \\
&= \prod_{i=1}^{v-1} (n^{i+1}, E_{i+1})_p \\
&= (n^v, E_v)_p \prod_{j=2}^v (n^j, E_j)_p \\
&= (n^{v-1}n, k^2)_p \prod_{j=2}^v (n^j, E_j)_p = (n, 1)_p \prod_{j=2}^{v-1} (n^j, E_j)_p \\
&= 1 \prod_{j=2}^{v-1} (n^j, E_j)_p = \prod_{i=2}^{v-1} (n^i, E_i)_p
\end{aligned}$$

Therefore, we now have

$$\begin{aligned}
c_p(f_1) &= (n, -1)_p^{\frac{v-1}{2}} \prod_{i=2}^{v-1} (n^i, E_i)_p (E_1, n)_p \prod_{i=2}^{v-1} (E_i, n^i)_p \prod_{i=1}^{v-1} (E_i, -E_{i+1})_p \\
&= (n, -1)_p^{\frac{v-1}{2}} (E_1, n)_p \prod_{i=2}^{v-1} (n^i, E_i)_p \prod_{i=2}^{v-1} (n^i, E_i)_p \prod_{i=1}^{v-1} (E_i, -E_{i+1})_p \\
&= (n, -1)_p^{\frac{v-1}{2}} (E_1, n)_p \prod_{i=2}^{v-1} ((n^i, E_i)_p)^2 \prod_{i=1}^{v-1} (E_i, -E_{i+1})_p \\
&= (n, -1)_p^{\frac{v-1}{2}} (k, n)_p \prod_{i=2}^{v-1} (n^2 i, E_i)_p \prod_{i=1}^{v-1} (E_i, -E_{i+1})_p \\
&= (n, -1)_p^{\frac{v-1}{2}} (k, n)_p \prod_{i=1}^{v-1} (E_i, -E_{i+1})_p \\
&= (n, -1)_p^{\frac{v-1}{2}} (k, n)_p \prod_{i=1}^{v-1} (E_i, -E_{i+1})_p
\end{aligned}$$

Now we need to evaluate $\prod_{i=1}^{v-1} (E_i, -E_{i+1})_p = P$, say.

Let p^a be the highest power of p dividing both k and λ so that $k = p^a k_1$ and $\lambda = p^a \lambda_1$ and $p \nmid (k_1, \lambda_1)$. We have $k_1 + (v-1)\lambda_1 = k_1 + (v-1)p^{-a}\lambda = k_1 + k(k-1)p^{-a} = k_1 + k_1 p^a (k_1 p^a - 1) p^{-a} = k_1 + k_1 (k_1 p^a - 1) = k_1^2 p^a$.

We also have $E_i = (k + (i-1)\lambda) = p^a (k_1 + (i-1)\lambda_1)$. Therefore we get

$$\begin{aligned}
P &= \prod_{i=1}^{v-1} (p^a (k_1 + (i-1)\lambda_1), -p^a (k_1 + i\lambda_1))_p \\
&= \prod_{i=1}^{v-1} (p^a, -p^a)_p (p^a, k_1 + i\lambda_1)_p (k_1 + (i-1)\lambda_1, p^a)_p (k_1 + (i-1)\lambda_1, -(k_1 + i\lambda_1))_p
\end{aligned}$$

We have from (2.18) that $(p^a, p^{-a})_p = 1$. Computing the second term will yield

$$\begin{aligned}
\prod_{i=1}^{v-1} (p^a, k_1 + i\lambda_1)_p &= \prod_{i=1}^{v-2} (p^a, k_1 + i\lambda_1)_p (p^a, k_1 + (v-1)\lambda_1)_p \\
&= (p^a, k_1 + (v-1)\lambda_1)_p \prod_{i=2}^{v-1} (p^a, k_1 + (i-1)\lambda_1)_p \\
&= (p^a, k_1 + (v-1)\lambda_1)_p \prod_{i=2}^{v-1} (k_1 + (i-1)\lambda_1, p^a)_p
\end{aligned}$$

Hence substituting these in the computation of P , we have

$$\begin{aligned}
P &= (p^a, k_1 + (v-1)\lambda_1)_p \prod_{i=2}^{v-1} (k_1 + (i-1)\lambda_1, p^a)_p \\
&\prod_{i=2}^{v-1} (k_1 + (i-1)\lambda_1, p^a)_p (k_1, p^a)_p \prod_{i=1}^{v-1} (k_1 + (i-1)\lambda_1, -(k_1 + i\lambda_1))_p \\
&= (k_1, p^a)_p (p^a, p^a k_1^2)_p \prod_{i=2}^{v-1} ((k_1 + (i-1)\lambda_1, p^a)_p)^2 \prod_{i=1}^{v-1} (k_1 + (i-1)\lambda_1, -(k_1 + i\lambda_1))_p \\
&= (k_1, p^a)_p (p^a, p^a)_p \prod_{i=1}^{v-1} (k_1 + (i-1)\lambda_1, -(k_1 + i\lambda_1))_p \\
&= (k_1, p^a)_p (p^a, p^a)_p \prod_{i=1}^{v-1} (k_1 + (i-1)\lambda_1, -(k_1 + i\lambda_1))_p
\end{aligned}$$

We will take two cases and show that in both the cases P has the same value.

Let us first suppose $p|\lambda_1$. Now we have $k(k-1) = \lambda(v-1) \implies k_1(k_1 p^a - 1) = \lambda_1(v-1) \implies k(k_1 p^a - 1) = \lambda(v-1) = k(k-1) \implies k_1 p^a = k \implies a = 0, k_1 = k$. Hence $p \nmid k$ and $p|\lambda$. Also we have $p \nmid k - \lambda, p \nmid k + i\lambda \forall i$. Hence we have $k_1 + (i-1)\lambda_1$ and $-(k_1 + i\lambda_1)$ are coprime to p . So we obtain

$$\prod_{i=1}^{v-1} (k_1 + (i-1)\lambda_1, -(k_1 + i\lambda_1))_p = \prod_{i=1}^{v-1} 1 = 1. \text{ Therefore in this case we have}$$

$$P = (k_1, p^a)_p (p^a, p^a)_p = (k, 1)_p (1, 1)_p = 1.$$

Also using the fact that $k^2 - k \equiv 0 \pmod{p}$, we get

$$\begin{aligned}
(k, k - \lambda)_p(\lambda, k - \lambda)_p &= 1(\lambda, k - \lambda)_p \text{ (from (2.20))} \\
&= (\lambda, k)_p \text{ (from (2.23))} \\
&= (\lambda, (k^2 - k) + k)_p \\
&= (\lambda, k^2)_p = 1
\end{aligned}$$

Hence we have $P = (k, k - \lambda)_p(\lambda, k - \lambda)_p$ in this case.

Let us take the next case when $p \nmid \lambda_1$. Then atmost one of $k_1 + (i - 1)\lambda_1$ or $k_1 + i\lambda_1$ is divisible by p . If neither is, then $(k_1 + (i - 1)\lambda_1, -(k_1 + i\lambda_1))_p = 1$. Let $0 \leq r \leq v - 1$ such that $k_1 + r\lambda_1 \equiv 0 \pmod{p}$. If $1 \leq r \leq v - 2$, then there are exactly two terms in the product P containing $k_1 + r\lambda_1$ and the product will look like ,

$$\begin{aligned}
(k_1 + (r - 1)\lambda_1, -(k_1 + r\lambda_1))_p(k_1 + r\lambda_1, -(k_1 + (r + 1)\lambda_1))_p \\
&= (-\lambda_1, -(k_1 + r\lambda_1))_p(k_1 + r\lambda_1, -\lambda_1)_p \\
&= (-\lambda_1, -(k_1 + r\lambda_1))_p(-\lambda_1, (k_1 + r\lambda_1))_p \\
&= (-\lambda_1, -(k_1 + r\lambda_1)^2)_p \\
&= (-\lambda_1, -1)_p = 1
\end{aligned}$$

Therefore we have $P = (k_1, p^a)_p(p^a, p^a)_p$ unless one or both of k_1 or $k_1 + (v - 1)\lambda_1$ is divisible by p (the cases when $r = 0$ and $r = v - 1$). When $a = 0, k_1 = k, k_1 + (v - 1)\lambda_1 = k^2$ and p divides neither of these. In this case, $P = 1$ and since $p \nmid k$ and $p \nmid \lambda$, we have $(k, k - \lambda)_p(\lambda, k - \lambda)_p = 1 \cdot 1 = 1$, if $p \nmid k - \lambda$.

If $p \mid k - \lambda$, we get $(k, k - \lambda)_p(\lambda, k - \lambda)_p = (k, k - \lambda)_p^2 = 1$, since both k and λ are coprime to p . Hence when $a = 0$, we conclude $P = (k, k - \lambda)_p(\lambda, k - \lambda)_p$.

We now need to see the case when $a > 0$, then $k_1 + (v - 1)\lambda_1 = k_1 + k_1(k_1 p^a - 1) = k_1^2 p^a$. If $p \mid (k_1 + (v - 1)\lambda_1)$, $(k_1 + (v - 2)\lambda_1, -(k_1 + (v - 1)\lambda_1))_p = (-\lambda_1, -k_1^2 p^a)_p = (-\lambda_1, p^a)_p = (-1, p^a)_p(\lambda_1, p^a)_p = (p^a, p^a)_p(\lambda_1, p^a)_p$.

If $p \nmid k_1$, we get $P = (k_1, p^a)_p(p^a, p^a)_p(p^a, p^a)_p(\lambda_1, p^a)_p = (k_1, p^a)_p(\lambda_1, p^a)_p$.

If $p \mid k_1$, we have to include the term $(k_1, -k_1 - \lambda_1)_p$ in P which will now take the form $P = (k_1, p^a)_p(\lambda_1, p^a)_p(k_1, -k_1 - \lambda_1)_p$.

Now

$$\begin{aligned}
(k, k - \lambda)_p(\lambda, k - \lambda)_p &= (p^a k_1, p^a(k_1 - \lambda_1))_p(p^a \lambda_1, p^a(k_1 - \lambda_1))_p \\
&= (p^{2a} k_1 \lambda_1, p^a(k_1 - \lambda_1))_p \\
&= (k_1 \lambda_1, p^a(k_1 - \lambda_1))_p \\
&= (k_1 \lambda_1, p^a)_p(k_1 \lambda_1, (k_1 - \lambda_1))_p \\
&= (k_1, p^a)_p(\lambda_1, p^a)_p(k_1, k_1 - \lambda_1)_p(\lambda_1, k_1 - \lambda_1)_p
\end{aligned}$$


If $p|k_1$, then $(\lambda_1, k_1 - \lambda_1)_p = 1$. Hence $P = (k_1, p^a)_p(\lambda_1, p^a)_p(k_1, k_1 - \lambda_1)_p$ which is the same as above calculation. And when $p \nmid k_1$, if $p \nmid k_1 - \lambda_1$, $(k_1, k_1 - \lambda_1)_p = (\lambda_1, k_1 - \lambda_1)_p = 1$ and hence $P = (k_1, p^a)_p(\lambda_1, p^a)_p$; else $p|k_1 - \lambda_1$, $(k_1, k_1 - \lambda_1)_p = (\lambda_1, k_1 - \lambda_1)_p$. Hence $P = (k_1, p^a)_p(\lambda_1, p^a)_p$.

Hence we have $P = (k_1, p^a)_p(\lambda_1, p^a)_p$ in every case. Substituting this in $c_p(f_1)$, we have

$$\begin{aligned}
c_p(f_1) &= (k - \lambda, -1)_{p^{\frac{v-1}{2}}} (k, k - \lambda)_p(k, k - \lambda)_p(\lambda, k - \lambda)_p \\
&= (k - \lambda, -1)_{p^{\frac{v-1}{2}}} (k, k - \lambda)_p^2(\lambda, k - \lambda)_p \\
&= (k - \lambda, -1)_{p^{\frac{v-1}{2}}} (\lambda, k - \lambda)_p \\
&= (k - \lambda, (-1)^{\frac{v-1}{2}})_p(\lambda)_p
\end{aligned}$$

Hence we proved that $c_p(f_1) = (k - \lambda, (-1)^{\frac{v-1}{2}})_p(\lambda)_p = 1$ for all finite odd primes . Since $k - \lambda$ is positive, $(k - \lambda, (-1)^{\frac{v-1}{2}})_p(\lambda)_\infty = 1$. By using (2.14), we obtain $(k - \lambda, (-1)^{\frac{v-1}{2}})_p(\lambda)_2 = 1$. Thus by theorem 2.5.5, we conclude that the rational equivalence of f_1 and f_2 is equivalent to the existence of integers x, y, z not all zero satisfying $(k - \lambda)x^2 + (-1)^{\frac{v-1}{2}} \lambda y^2 = z^2$. Therefore this becomes not only a necessary but also a sufficient condition for the rational solution of (2.7). Hence we have proved the Bruck -Ryser-Chowla theorem and its rational converse. \square



In this chapter we have dealt with symmetric BIBD's in a great detail. We saw its properties and also the necessary and sufficient conditions for the existence of symmetric  BD's, the Bruck-Ryser-Chowla theorem, one of the main results in this concept.

Chapter 3

Difference Sets

Having learnt about symmetric designs and necessary condition for the existence of symmetric designs, we will now look at an important construction method for symmetric BIBD's. 

3.1 Difference Sets and Automorphisms

Definition 3.1.1 *Difference Set*

Suppose $(G, +)$ is a finite group of order v in which identity element is denoted by 0. Let k and λ be positive integers such that $2 \leq k \leq v$. A (v, k, λ) -difference set in $(G, +)$ is a subset $D \subseteq G$ that satisfies

1. $|D| = k$
2. the multiset $[x - y : x, y \in D, x \neq y]$ contains every element in $G \setminus \{0\}$ exactly λ times.

From (ii), $\lambda(v - 1) = k(k - 1)$ if a (v, k, λ) - difference set exists.

Example 3.1.2

A $(21, 5, 1)$ -difference set in $(\mathbb{Z}_{21}, +)$ where $D = \{0, 1, 6, 8, 18\}$:
Computing differences of distinct elements modulo 21, we get from each pair of distinct elements:

0-1=20	1-0=1	6-0=6	8-1=8	18-0=18
0-6=15	1-6=16	6-1=5	8-1=7	18-1=17
0-8=13	1-8=14	6-8=19	8-6=2	18-6=12
0-18=3	1-18=4	6-18=11	8-18=11	18-8=10



So we get every element of $\mathbb{Z}_2^1 \setminus \{0\}$ exactly once as a difference of two elements in D .

Difference sets can be used to construct symmetric BIBD's. To go into this we will first see some definitions which we will require for the same.

Definition 3.1.3 *Translate of D*

Let D be a (v, k, λ) -difference set in a group $(G, +)$. For any $g \in G$, define $D + g = \{x + g | x \in D\}$. Any set $D + g$ is called translate of D .

Definition 3.1.4 *Development of D*

The collection of all v translates of D is called the development of D , denoted by $\text{Dev}(D)$.

Let us now see the relation between symmetric BIBD and difference sets.

Theorem 3.1.5 *Let D be a (v, k, λ) -difference set in an abelian group $(G, +)$. Then $(G, \text{Dev}(D))$ is a symmetric (v, k, λ) -BIBD.*

Proof: Suppose $x, y \in G, x \neq y$. Since in a symmetric BIBD every pair of points is contained in λ blocks, we first prove that there are exactly λ elements $g \in G$ such that $\{x, y\} \subseteq D + g$.

Let us first denote $x - y = d$. By the definition of difference set there are exactly λ ordered pairs (x', y') such that $x', y' \in D, x' \neq y', x' - y' = d$. We denote these ordered pairs by $(x_i, y_i), 1 \leq i \leq \lambda$. $\forall 1 \leq i \leq \lambda$, we define $g_i = -x_i + x$. Then $g_1 = -y_1 + y$ and $\{x, y\} = \{x_i + g_i, y_i + g_i\} \subseteq D + g_i$. g_i 's are distinct since x_i 's are distinct hence there are at least λ values of g such that $\{x, y\} \subseteq D + g$.

Conversely suppose that there are exactly l values of g such that $\{x, y\} \subseteq D + g$. Let us denote $g = h_1, \dots, h_l$. We have shown above that $l \geq \lambda$. Note that $(x - h_i) + (h_i - y) = (x - y) = d \forall 1 \leq i \leq l$. Therefore $\{x_i - h_i, h_i - y_i\} \subseteq D \forall 1 \leq i \leq l$. The h_i 's are distinct, so we have found l ordered pairs $(x', y') \in D$ such that $x' - y' = d$. By definition there are exactly λ such ordered pairs. Hence $l \leq \lambda$. And so we get $l = \lambda$. Hence each ordered pair is contained in λ number of $D + g$. Since $|G| = v$ we have v points. The number of blocks is $|\text{Dev}(D)| = v$. Since $|D| = k, |D + g| = k$ for all g . So the collection of v blocks $D + g, g \in G$ is a symmetric (v, k, λ) -BIBD. \square

Let us now see a corollary of this theorem.

Corollary 3.1.6 *Suppose D is a (v, k, λ) difference set in an abelian group $(G, +)$. Then $\text{Dev}(D)$ contains v distinct blocks.*

Proof: Suppose that $D + g_1 = D + g_2$ such that $g_1 \neq g_2$. Then the symmetric BIBD will contain 2 blocks that intersect in k points. But in a symmetric BIBD any two blocks intersect in λ points which is a contradiction. Hence $\text{Dev}(D)$ consists of v distinct blocks. \square

The next result establishes the existence of non trivial automorphism of symmetric BIBD's constructed from difference sets.

Theorem 3.1.7 *Suppose $(G, \text{Dev}(D))$ is the symmetric BIBD constructed from a (v, k, λ) -difference set D in a group $(G, +)$. Then $\text{Aut}(G, \text{Dev}(D))$ contains a subgroup $\hat{G} \simeq G$.*

Proof: For every $g \in G$, define $\hat{g} : G \rightarrow G$ such that $\hat{g}(x) = x + g \quad x \in G$.

$$\hat{g}(x_1) = \hat{g}(x_2) \iff x_1 + g = x_2 + g \iff x_1 = x_2.$$

Hence \hat{g} is one-one. Also for every $y \in G$, there exist an $x' \in G$ such that $\hat{g}(x') = x' + g = y \in G$. Hence \hat{g} is onto. And so \hat{g} is a permutation of G . Define $\hat{G} = \{\hat{g} | g \in G\}$. \hat{G} is a permutation group and is known as the permutation representation of G .

We will now prove that

1. $(G, +) \simeq (\hat{G}, o)$, where o represent the composition of permutations.
2. (\hat{G}, o) is a subgroup of $\text{Aut}(G, \text{Dev}(D))$.

To prove the first item, we need to exhibit an isomorphism between $(G, +)$ and (\hat{G}, o) . Define $\alpha : G \rightarrow \hat{G}$ such that $\alpha(g) = \hat{g} \quad \forall g \in G$.

$$\begin{aligned} (\alpha(g)o\alpha(h)) &= (\alpha(g)o\alpha(h))(x) \\ &= (\hat{g}o\hat{h})(x) \\ &= \hat{g}(\hat{h}(x)) \\ &= \hat{g}(h + x) \\ &= g + h + x = x + g + h \\ &= g \hat{+} h(x) \\ &= \alpha(g + h)(x) \end{aligned}$$

holds for all $g, h \in G$. Hence α is a group homomorphism. Clearly α is surjective. Also,

$$\alpha(g) = \alpha(h) \iff \hat{g} = \hat{h} \iff \hat{g}(x) = \hat{h}(x) \quad x \in G \iff g+x = h+x \forall x \in G \iff g = h.$$


hence α is injective. So we get the desired result that α is a bijection and hence there exists an isomorphism between $(G, +)$ and (\hat{G}, o) .

Now we need to prove the second assertion. We observe that ,

$$\begin{aligned} \hat{g}(D+h) &= \{\hat{g}(x) | x \in D+h\} \\ &= \{x+g | x \in D+h\} \\ &= \{x+g+h | x \in D\} \\ &D+g+h \end{aligned}$$

Hence for any permutation $\hat{g} \in \hat{G}$, and for any block $D+h \in \text{Dev}(D)$, it holds that $D+h \in \text{Dev}(D)$. That is, every $\hat{g} \in \hat{G}$ is an automorphism of $(G, \text{Dev}(D))$. Since \hat{G} is a group we get (\hat{G}, o) is a subgroup of $\text{Aut}(G, \text{Dev}(D))$ which is the desired result. \square

The converse of the above theorem holds under suitable conditions. We will prove a special case of this type for difference sets in cyclic groups. We will require some results which we will see now.

 Suppose that (X, \mathcal{A}) is a symmetric (v, k, λ) -BIBD. Let $\alpha \in \text{Aut}(X, \mathcal{A})$. α is a permutation of X and therefore it consists of a union of disjoint cycles whose lengths sum to v . *Cycle type* of α is the collection of sizes of cycles in the disjoint cycle representation of α . Fixed point of α is a point α is a point x such that $\alpha(x) = x$.

For example, consider permutation α of $\{0, \dots, 8\}$ defined as $\alpha = (0, 3)(4, 5)(2)(6, 8)(7)$.

Then the cycle type of α is $[1, 1, 2, 2, 3]$ and the fixed points are 2 and 7.

An automorphism α of (X, \mathcal{A}) will permute the blocks in set \mathcal{A} . We can also write the cycle type of this permutation of \mathcal{A} induced by α . Fixed point of this permutation is a block $A \in \mathcal{A}$ that is fixed setwise by α , i.e $\{\alpha(x) | x \in A\} = A$, which we call as fixed blocks.

We will now prove a useful result which we will require later.

Lemma 3.1.8 *Suppose (X, \mathcal{A}) be a symmetric (v, k, λ) -BIBD and suppose that $\alpha \in \text{Aut}(X, \mathcal{A})$ has exactly f points. Then α fixes exactly f blocks in \mathcal{A} .*

Proof: Suppose that α fixes exactly F blocks. Define

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

We compute $|I|$ in two ways. Firstly,

$$\begin{aligned} |I| &= \sum_{x \in X} |\{A \in \mathcal{A} | \{x, \alpha(x)\} \subseteq A\}| \\ &= \sum_{\{x \in X | \alpha(x) = x\}} |\{A \in \mathcal{A} | \{x, \alpha(x)\} \subseteq A\}| + \sum_{\{x \in X | \alpha(x) \neq x\}} |\{A \in \mathcal{A} | \{x, \alpha(x)\} \subseteq A\}| \\ &= fk + (v - f)\lambda \end{aligned}$$

Secondly we compute $|I|$ as follows.

$$\begin{aligned} |I| &= \sum_{A \in \mathcal{A}} |\{x \in X | \{x, \alpha(x)\} \subseteq A\}| \\ &= \sum_{\{A \in \mathcal{A} | \alpha(A) = A\}} |\{x \in X | \{x, \alpha(x)\} \subseteq A\}| + \sum_{\{A \in \mathcal{A} | \alpha(A) \neq A\}} |\{x \in X | \{x, \alpha(x)\} \subseteq A\}| \end{aligned}$$

If $\alpha(A) = A, \alpha(x) \in A \forall x \in X \implies \{x \in X | \{x, \alpha(x)\} \subseteq A\} = A$.
 If $\alpha(A) \neq A, \{x, \alpha(x)\} \subseteq A \iff x \in A \cap \alpha^{-1}(A)$. Since $\alpha^{-1}(A) \neq A, |A \cap \alpha^{-1}(A)| = \lambda$.

Hence, $|I| = Fk + (v - F)\lambda$.

Therefore we get,

$$\begin{aligned} fk + (v - f)\lambda &= Fk + (v - F)\lambda \implies (f - F)k + \lambda(v - f - v + F) = 0 \\ &= (f - F)k - \lambda(f - F) = 0 \implies (f - F)(k - \lambda) = 0 \end{aligned}$$

We have $k \neq \lambda$, hence $f = F$, which is the desired result. \square

We will define one more tool required later.

Definition 3.1.9 Mobius Function

Mobius function, denoted as μ , for positive integers is defined as

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \times \dots \times p_k \text{ where } P_i \text{'s are distinct primes} \\ 0 & \text{if } n \text{ is divisible by } p^2 \text{ for some prime } p \end{cases}$$

Now we will state an important theorem of mobius function (without proof).

Theorem 3.1.10 (Möbius Inversion Formula) Suppose that $f, g : \mathbb{Z}^+ \rightarrow \mathbb{R}$ are functions and suppose that $f(j) = \sum_{i|j} g(i)$ holds for every positive integer j , then for every positive integer i ,

$$g(i) = \sum_{j|i} \mu\left(\frac{i}{j}\right) f(j).$$

Having stated the result we will see a theorem which uses the above facts.

Theorem 3.1.11 Suppose that (X, \mathcal{A}) is a symmetric (v, k, λ) -BIBD and $\alpha \in \text{Aut}(X, \mathcal{A})$. Then the cycle type of permutation of X induced by α is the same as cycle type of permutation of \mathcal{A} induced by α .

Proof: Suppose a permutation α of a finite set S has exactly c_i cycles of length i , $1 \leq i \leq |S|$. Let f_j denote the number of fixed points of the permutation α^j . A point $x \in S$ is fixed by permutation α^j if and only if x lies in a cycle whose length divides j ($i|j$) in α . This gives us that $f_j = \sum_{i|j} ic_i$.

Set $g(i) = ic_i$. Applying Möbius inversion formula we get

$$ic_i = \sum_{j|i} \mu\left(\frac{i}{j}\right) f_j \implies c_i = \frac{1}{i} \sum_{j|i} \mu\left(\frac{i}{j}\right) f_j.$$

Let us now suppose that α is a permutation of symmetric (v, k, λ) -BIBD (X, \mathcal{A}) . For every j greater than or equal to 1, α^j is an automorphism of (X, \mathcal{A}) . Hence by the above lemma, the permutation of X and \mathcal{A} induced by α^j have the same number of fixed points. Hence from the formula of c_i , both permutations induced by α have the same cycle type. \square

We will now prove a converse to theorem 3.1.5 where the symmetric BIBD has an automorphism which is a single cycle of length v .

Theorem 3.1.12 Suppose that (X, \mathcal{A}) is asymmetric (v, k, λ) -BIBD having an automorphism α that permutes the points in X in a single cycle of length v . Then there is a (v, k, λ) -difference set in $(\mathbb{Z}_v, +)$.

Proof: By relabelling the points if necessary, we can assume, without loss of generality, $X = \{x_0, \dots, x_{v-1}\}$ and $\alpha(x_i) = x_{i+1} \pmod v$ for $0 \leq i \leq v-1$. We get $\alpha = (x_0, \dots, x_{v-1})$. We choose any block $A \in \mathcal{A}$. We define $A_0 = A$ and

for each integer $j \geq 0$, define $A_j = \{\alpha^j(x) | x \in A_0\} = \{x_{j+1} \bmod v | x_i \in A_0\}$. Every block $A_j \in \mathcal{A} \cdot: \alpha^j \in \text{Aut}(X, \mathcal{A})$. From the above theorem, α permutes the block in \mathcal{A} in a single cycle of length v . Hence A_0, \dots, A_{v-1} are all distinct and $\mathcal{A} = \{A_j | 0 \leq j \leq v-1\}$ and α permutes the blocks in \mathcal{A} as $\alpha = (A_0, \dots, A_{v-1})$.

Now, we define $D = \{i | x_I \in A_0\}$ and we move on to show that D is the desired difference set. Let $g \in \mathbb{Z}_v, g \neq 0$. The pair $\{x_0, x_g\}$ occurs in exactly λ blocks in \mathcal{A} , say $A_{i_1}, \dots, A_{i_\lambda}$. For each occurrence of this pair in A_{i_j} , we have a pair in difference set $D, (g - i_j) - (-i_j) \equiv g \pmod v$, and $\{-i_j \bmod v, g - i_j \bmod v\} \subseteq D$. These λ pairs in D are distinct. Thus the difference g occurs λ times in the set D for all nonzero $g \in \mathbb{Z}_v$. All occurrences of g are included by this method. Hence D is the desired difference set. \square

We will see a generalisation to the above theorem in the case for arbitrary finite groups for which we will first see a definition.

Definition 3.1.13 *Sharply transitive*

Let $G \subseteq S_V$, is a permutation group acting on a set v -set X . G is sharply transitive if for all $x, x' \in X$, there exists a unique permutation $g \in G$ such that $g(x) = x'$. Also $|G| = v$ if G is sharply transitive.

Now we state the theorem which can be proved in a similar procedure of previous theorem.

Theorem 3.1.14 *Suppose (X, \mathcal{A}) is a symmetric (v, k, λ) -BIBD such that G is a sharply transitive subgroup of $\text{Aut}(X, \mathcal{A})$. Then there exists a (v, k, λ) -difference set in the group (G, o) .*

3.2 Quadratic Residue Difference Sets

We will now see the concept of quadratic residues in a finite field \mathbb{F}_q , where q is an odd prime power. The quadratic residues of \mathbb{F}_q are the elements in the set $QR(q) = \{z^2 | z \in \mathbb{F}_q, z \neq 0\}$. The quadratic non residues of \mathbb{F}_q are $QNR(q) = \mathbb{F}_q \setminus (QR(q) \cup \{0\})$.

We now characterize the quadratic residues and non residues. We use the fact that the multiplicative group $(\mathbb{F}_q \setminus \{0\}, \cdot)$ is a cyclic group. A generator of this group, say w , is called the primitive element of the field \mathbb{F}_q . And therefore w is a primitive element if and only if $\{w^i | 0 \leq i \leq q-2\} = \mathbb{F}_q \setminus \{0\}$. It is clear that the set $\{w^{2i} | 0 \leq i \leq \frac{q-3}{2}\}$ is a subset of $QR(q)$. We can see that

the cardinality of the above set is $\frac{q-3}{2} + 1 = \frac{q-1}{2} = |QR(q)|$. Hence we have proven the following result that

Lemma 3.2.1 *Suppose q is an odd prime power and w is a primitive element in \mathbb{F}_q . Then $QR(q) = \{w^{2i} | 0 \leq i \leq \frac{q-3}{2}\}$.*

Now we will see a corollary of this lemma.

Corollary 3.2.2 *Suppose q is an odd prime power. Then $-1 \in QR(q) \iff q \equiv 1 \pmod{4}$.*

Proof: Let $w \in \mathbb{F}_q$ be primitive element and let $\gamma = w^{\frac{q-1}{2}} \neq 1$. Hence $\gamma^2 = w^{q-1} = 1$. So $\gamma \neq 1, \gamma^2 = 1$. Hence we get $\gamma = w^{\frac{q-1}{2}} = -1$. Now $-1 \in QR(q) \iff w^{\frac{q-1}{2}} = z^2 \iff \frac{q-1}{2} = 2k \iff q-1 = 4k \iff q \equiv 1 \pmod{4}$. \square

Now we will see a result which provides an infinite class of difference sets.

Theorem 3.2.3 (Quadratic Residue Difference Sets) *Suppose $q \equiv 3 \pmod{4}$ is a prime power. Then $QR(q)$ is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$ -difference set in $(\mathbb{F}_q, +)$.*

Proof: Let $QR(q) = D$. We have $|D| = \frac{q-1}{2}$. Hence, we only need to show that every non zero element of \mathbb{F}_q occurs $\frac{q-3}{4}$ times as a difference of 2 elements in D .

For any $d \in \mathbb{F}_q \setminus \{0\}$, define $a_d = |\{(x, y) | x, y \in D, x - y = d\}|$.

Now, $gx - gy = g(x - y) \forall g, x, y$. So the number of times any difference d occurs in D is same as the number of times difference gd occurs in $gD = \{gx | x \in D\}$. Suppose $g \in QR(q)$. Since product of two quadratic residues is also a quadratic residue, we have $gD = D$. And we get $a_d = a_{gd} \forall g \in QR(q)$. Hence there exists a constant λ such that $a_d = \lambda \forall d \in QR(q)$.

Let $d \in QNR(q), e = -d$. WE have $-1 \in QNR(q)$. And $-1 \times d = e \in QR(q)$. $a_d = a_e$ since $x - y = d \iff y - x = e$. Hence it follows that $a_d = \lambda \forall d \in \mathbb{F}_q \setminus \{0\}$. Hence D is a $(q, \frac{q-1}{2}, \lambda)$ difference set. We have $\lambda(v-1) = k(k-1)$, which gives $\lambda = \frac{\frac{q-1}{2} \frac{q-3}{2}}{q-1} = \frac{q-3}{4}$. Hence we get $QR(q)$ is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$ -difference set in $(\mathbb{F}_q, +)$. \square

Now we will see construction of difference sets in a different class of elements.

Definition 3.2.4 *Quartic residues*

For prime power $q \equiv 1 \pmod{4}$, quartic residue in \mathbb{F}_q are the elements of the set $\{z^4 | z \in \mathbb{F}_q, z \neq 0\}$. Equivalently, we can also say that quartic residue is the set $\{w^{4i} | 0 \leq i \leq \frac{q-5}{4}\}$; where w is the primitive element.

Now we will state a theorem without proof which involves quartic residues.

Theorem 3.2.5 *Suppose that $p = 4t^2 + 1$ is prime and t is an odd integer. Then quartic residues in \mathbb{Z}_p form a $(4t^2 + 1, t^2, \frac{t^2-1}{4})$ -difference set in $(\mathbb{Z}_p, +)$, and the quartic residues in $\mathbb{Z}_p \cup \{0\}$ form $(4t^2 + 9, t^2 + 4, \frac{t^2+3}{4})$ -difference set in $(\mathbb{Z}_p, +)$.*

Let us now explore some more properties related to difference sets.

3.3 The Multiplier Theorem

3.4 Multipliers of difference sets

We focus on abelian groups in this section and now we define a concept from which we further move on.

Definition 3.4.1 *Multiplier*

Let D be a (v, k, λ) -difference set in an abelian group $(G, +)$ of order v . For an integer m , define $mD = \{mx | x \in D\}$, where mx is the sum of m copies of x . Then m is called the multiplier of D if $mD = D + g$ for some $g \in G$. D is fixed by the multiplier m if $mD = D$.

We will now see some basic results regarding multipliers.

Lemma 3.4.2 *Suppose that m is a multiplier of a (v, k, λ) -difference set in D in an abelian group $(G, +)$ of order v . Then $\gcd(m, v) = 1$.*

Proof: Suppose that $\gcd(m, v) > 1$. Let p be a prime divisor of m and v . Let $d \in G$ have order p . There exists $x, y \in D$ such that $x - y = d$. Then $mx - my = m(x - y) = md = kpd = k(pd) = 0$. So mD contains repeated elements. Hence we get that $mD \neq D + g$ for any g and m is not a multiplier of D . Hence it must be the case that $\gcd(m, v) = 1$. \square

Lemma 3.4.3 *Suppose that m is a multiplier of a (v, k, λ) -difference set in D in an abelian group $(G, +)$ of order v . Define $\alpha : G \rightarrow G$ by $\alpha(x) = mx$. Then $\alpha \in \text{Aut}(G, \text{Dev}(D))$.*

Proof: We have $mD = D + g$ for some $g \in G$. We apply α to arbitrary block of $(G, \text{Dev}(D))$. We have $\alpha(D + h) = m(D + h) = mD + mh = D + g + mh \in \text{Dev}(D)$. Hence α maps any arbitrary block to another block. And we get the desired result. \square

Now we will see an important result known as the multiplier theorem which establishes the existence of multipliers in difference sets, whose parameters satisfy certain conditions.

Theorem 3.4.4 (Multiplier Theorem) *Suppose there exists a (v, k, λ) -difference set in an abelian group $(G, +)$ of order v . Suppose that the conditions given are satisfied :*

1. p is prime
2. $\gcd(p, v) = 1$
3. $k - \lambda \equiv 0 \pmod{p}$
4. $p > \lambda$

Then p is a multiplier of D .

Applying the multiplier theorem is made easier by the result we will see now.

Theorem 3.4.5 *Suppose that m is a multiplier of a (v, k, λ) -difference set in D in an abelian group $(G, +)$ of order v . Then there exist a translate of D that is fixed by m .*

Proof: Define $\alpha(x) = mx$ for every $x \in G$. Then we have $\alpha \in \text{Aut}(G, \text{Dev}(D))$. We can easily see that $\alpha(0) = m0 = 0$ and therefore α fixes atleast one point. Then by lemma 3.1.8 α fixes atleast one block of $\text{Dev}(D)$. This means that α fixes atleast one translate of D . $\alpha(D + h) = m(D + h) = d + h$. Hence there exists a translate of D that is fixed by m . \square

Let us now see a more general result in the case when $\gcd(v, k) = 1$.

Theorem 3.4.6 *Suppose there exists a (v, k, λ) -difference set in an abelian group $(G, +)$ of order v . Then there exists a translate of D that is fixed by every multiplier m .*

Proof: Let us denote $s = \sum_{x \in D} x$. Then we get $\sum_{x \in D+g} = \sum_{x \in D} x + |D|g = s + kg$.

If $s + kg = s + kh; g, h \in G, g \neq h$. Then $k(g - h) = 0$. And we get order of $g - h$ divides k . However in a finite group, order of any element divides the order of group. Hence order of $g - h$ divides v . Since $\gcd(v, k) = 1$, order of $g - h = 1 \implies g - h = 0 \implies g = h$ which is a contradiction.

Hence we have now shown that the map $g \mapsto s + kg$ is one-one. Since this



map is from G into G and G is finite, G is surjective. Hence there exists a unique $g \in G$ such that $s + kg = 0 \implies \sum_{x \in D+g} x = 0$.

Let m be any multiplier of D . Then m is also multiplier of the translate $D + g$ and we have

$$\sum_{x \in m(D+g)} x = m \sum_{x \in D+g} x = 0.$$

Since it is for a unique g , $D + g$ is the unique translate of D whose elements sum to 0. Hence $m(D + g) = D + g$ and the translate $D + g$ is fixed by any multiplier m . \square

A difference set or a translate of a difference set is said to be *normalized* if its elements sum to 0. Hence we showed above that for any (v, k, λ) -difference set D in an abelian group $(G, +)$ of order v where $\gcd(v, k) = 1$, there is a unique normalized translate and this translate is fixed by every multiplier of D .

Before proceeding to the proof of the multiplier theorem,  need to see some requirements which we need for the proof. Let us take a look at these now. 

3.4.1 Group Ring

The proof of the multiplier theorem uses an algebraic structure called the group ring. We will see the definition and some properties of the same.

Definition 3.4.7 Group Ring

Let $(G, +)$ be an abelian group. The group ring, $\mathbb{Z}[G]$, consists of all formal sums of the form $\sum_{g \in G} a_g x^g$; $a_g \in \mathbb{Z}$, where x is the indeterminate. It is easy to see that an element of $\mathbb{Z}[G]$ is a polynomial in the indeterminate x having integer coefficients and the exponents are the elements of the group G .

Let us see some of its properties. Let $a(x) = \sum_{g \in G} a_g x^g, b(x) = \sum_{g \in G} b_g x^g$, then

$$(a + b)(x) = \sum_{g \in G} (a_g + b_g) x^g$$

$$(a \cdot b)(x) = \sum_{g \in G} \sum_{h \in G} (a_g b_h) x^{g+h}$$

$$a(x) \equiv b(x) \pmod{p} \text{ if } a_g \equiv b_g \pmod{p}$$

These are the operations carried out. We may also make use of the group ring $\mathbb{Z}_p[G]$ which is defined in the same way as above, except that here the coefficients are in \mathbb{Z}_p . We will now define some more notations.

For any $a(x) = \sum_{g \in G} a_g x^g$, define

$$a(x^m) = \sum_{g \in G} a_g x^{mg}$$

$$a(x^{-1}) = \sum_{g \in G} a_g x^{-g}$$

$$a(1) = \sum_{g \in G} a_g 1 = \sum_{g \in G} a_g$$

Finally, let $G(x) = \sum_{g \in G} x^g$ and for a difference set D in G , define $D(x) = \sum_{g \in D} x^g$.

Now let us see some results regarding difference sets and group ring.


Lemma 3.4.8 *Suppose D is a (v, k, λ) -difference set in an abelian group G . Then $D(x)D(x^{-1}) = \lambda G(x) + (k - \lambda)x^0$.*

Proof: We have $D(x) = \sum_{g \in D} x^g$ and $D(x^{-1}) = \sum_{h \in D} x^{-h}$. So we get, $D(x)D(x^{-1}) =$

$\sum_{g, h \in D} x^{g-h}$. Let $g - h = d$ and define $\alpha_d = |\{(g, h) | g, h \in D, g - h = d\}|$. So

we get $D(x)D(x^{-1}) = \sum_{d \in G} \alpha_d x^d$. Clearly, we have

$$\alpha_d = \begin{cases} \lambda & \text{if } d \neq 0 \\ k & \text{if } d = 0 \end{cases}$$

Therefore we get, $D(x)D(x^{-1}) = \lambda G(x) + (k - \lambda)x^0$.  \square

Now if $\gcd(m, v) = 1$, where m is a positive integer, then we state the result similar to above in this case.

Lemma 3.4.9 *If D is a (v, k, λ) difference set in an abelian group G . Suppose m is a positive integer such that $\gcd(m, v) = 1$, then*

$$D(x^m)D(x^{-m}) = \lambda G(x) + (k - \lambda)x^0.$$

Lemma 3.4.10 *Suppose $a(x) \in \mathbb{Z}[G]$. Then $a(x)G(x) = a(1)G(x)$.*

Proof: We have

$$\begin{aligned} a(x)G(x) &= \sum_{g, h \in G} a_g x^{g+h} \\ &= \sum_{i \in G} \left(\sum_{g \in G} a_g \right) x^i; g + h = 1 \\ &= \sum_{i \in G} a(1)x^i \\ &= a(1)G(x) \end{aligned}$$

as required. \square

Lemma 3.4.11 *Suppose p is a prime and $a(x) \in \mathbb{Z}[G]$. Then $a(x)^p \equiv a(x^p) \pmod{p}$.*

Proof: We prove this result by induction on the number of non zero coefficients in $a(x)$. Suppose that $a(x)$ has no nonzero coefficients, then $a(x) = 0$ and the result holds trivially. If $a(x)$ has one non zero coefficient, then $a(x) = a_g x^g$ for some $a_g \neq 0$. Then computing in $\mathbb{Z}_p[x]$, we have

$$\begin{aligned} a(x)^p &= (a_g x^g)^p \\ &= a_g^p x^{gp} \\ &= a_g x^{pg} \\ &= a(x^p) \end{aligned}$$

Now let us assume the result holds when $a(x)$ has at most i nonzero coefficients for some $i \geq 1$. Let $a(x)$ have $i + 1$ nonzero coefficients. Then $a(x) =$


$a_i(x) + a_g x^g$; where $a_i(x)$ has i nonzero coefficients and $a_g \neq 0$. Then we get,

$$\begin{aligned}
a(x)^p &= ((a_i(x) + a_g(x)))^2 \\
&= a_i(x)^p + \sum_{j=1}^{p-1} \binom{p}{j} a_i(x)^j (a_g x^g)^{p-j} + (a_g x^g)^p \\
&= a_i(x)^p + (a_g x^g)^p \quad \because \binom{p}{j} \equiv 0 \pmod{p} \quad \forall 1 \leq j \leq p-1 \\
&= a_i(x)^p + a_g x^{pg} \\
&= a(x^p)
\end{aligned}$$

by induction. Hence the result holds for all $a(x) \in \mathbb{Z}[G]$. □

Now using all these results let us see the proof of the multiplier theorem.

3.5 Proof of the Multiplier Theorem

In this section we see the result of theorem 3.4.4.  *Proof:* We begin the proof by computing the product $D(x^p)D(x^{-1})$.

$$\begin{aligned}
D(x^p)D(x^{-1}) &= D(x)^p D(x^{-1}) \quad \text{by lemma 3.4.11} \\
&= D(x)^{p-1} D(x) D(x^{-1}) \\
&= D(x)^{p-1} (\lambda G(x) + (k - \lambda)x^0) \quad \text{by lemma 3.4.8} \\
&= \lambda D(x)^{p-1} G(x) + (k - \lambda) D(x)^{p-1} \\
&= \lambda D(1)^{p-1} G(x) + (k - \lambda) D(x)^{p-1} \quad \text{by lemma 3.4.10} \\
&= \lambda k^{p-1} G(x) + (k - \lambda) D(x)^{p-1} \quad \because D(1) = k \\
&= \lambda k^{p-1} G(x) \quad \because k - \lambda \equiv 0 \pmod{p} \\
&= \lambda^p G(x) \quad \because k \equiv \lambda \pmod{p} \\
&= \lambda G(x) \quad \because \lambda^p \equiv \lambda \pmod{p}
\end{aligned}$$

Now we define $S(x) = D(x^p)D(x^{-1}) - \lambda G(x)$. Hence we have $S(x) \equiv 0 \pmod{p}$. So all coefficients of S are divisible by p . Since all coefficients of $D(x^p)D(x^{-1})$ are non negative it follows that all coefficients of $S(x)$ are greater than or equal to $-\lambda$. Since we have $p > \lambda$, all coefficients of $S(x)$ are also non negative.

Note that $G(x^{-1}) = \sum_{g \in G} x^{-g}$. Since every element has a unique inverse, pair

them up and we get $G(x^{-1}) = G(x)$.

Now we compute $S(x)S(x^{-1})$.

$$\begin{aligned}
S(x)S(x^{-1}) &= (D(x^p)D(x^{-1}) - \lambda G(x))(D(x^{-p})D(x) - \lambda G(x^{-1})) \\
&= (D(x^p)D(x^{-1}) - \lambda G(x))(D(x^{-p})D(x) - \lambda G(x)) \\
&= D(x^p)D(x^{-p})D(x^{-1})D(x) + \lambda^2 G(x)^2 - \lambda D(x^p)D(x^{-1})G(x) - \lambda G(x)D(x^{-p})D(x) \\
&= D(x^p)D(x^{-p})D(x^{-1})D(x) + \lambda^2 G(x)^2 - \lambda G(x)(D(x^p)D(x^{-1}) + D(x^{-p})D(x))
\end{aligned}$$

Now

$$\begin{aligned}
D(x^p)D(x^{-p})D(x^{-1})D(x) &= (\lambda G(x) + (k - \lambda)x^0)(\lambda G(x) + (k - \lambda)x^0) \\
&= (\lambda G(x) + (k - \lambda)x^0)^2 \\
&= \lambda^2 G(x)^2 + (k - \lambda)^2 + 2\lambda(k - \lambda)G(x)
\end{aligned}$$

Now $G(x)^2 = G(x)G(x) = G(1)G(x) = vG(x)$. Hence we get $D(x^p)D(x^{-p})D(x^{-1})D(x) = \lambda^2 vG(x) + (k - \lambda)^2 + 2\lambda(k - \lambda)G(x)$.

We also have that

$$\begin{aligned}
-\lambda G(x)(D(x^p)D(x^{-1}) + D(x^{-p})D(x)) + \lambda^2 G(x)^2 &= \lambda G(x)D(x^p)D(x^{-1}) - \lambda G(x)D(x^{-p})D(x) + \lambda^2 vG(x) \\
&= -\lambda D(1)G(x)D(x^{-1}) - \lambda D(1)G(x)D(x) + \lambda^2 vG(x) \\
&= -\lambda D(1)^2 G(x) - \lambda D(1)^2 G(x) + \lambda^2 vG(x) \\
&= -2\lambda k^2 G(x) + \lambda^2 vG(x)
\end{aligned}$$

Therefore, we get

$$\begin{aligned}
S(x)S(x^{-1}) &= \lambda^2 G(x)^2 + (k - \lambda)^2 + 2\lambda(k - \lambda)G(x) - 2\lambda k^2 G(x) + \lambda^2 vG(x) \\
&= (\lambda^2 v + 2\lambda(k - \lambda) - 2\lambda k^2 + \lambda^2 v)G(x) + (k - \lambda)^2 \\
&= 2\lambda(\lambda v + k - \lambda - k^2)G(x) + (k - \lambda)^2 \\
&= 2\lambda(\lambda(v - 1) + k - k^2)G(x) + (k - \lambda)^2 \\
&= 2\lambda(k(k - 1) - k(k - 1))G(x) + (k - \lambda)^2 \\
&= (k - \lambda)^2 \\
&= (k - \lambda)^2 x^0
\end{aligned}$$

Now let $S(x) = \sum_{g \in G} s_g x^g$. We have shown above that $s_g \geq 0 \forall g \in G$.

Suppose that there exists $g, h \in G, g \neq h$ such that $s_g > 0, s_h > 0$. Then

the coefficient of x^{g-h} in $S(x)S(x^{-1})$ is atleast $s_g s_h > 0$, which is a contradiction. Hence $S(x) = s_g x^g$ for some $g \in G$. Then we get $S(x)S(x^{-1}) = (s_g x^g)(s_g x^{-g}) = (s_g)^2 x^0$. And we get $s_g^2 = (k - \lambda)^2$. Since $s_g \geq 0$, we get $s_g = k - \lambda$ and $S(x) = (k - \lambda)x^g$ for some $g \in G$.

Substituting this in the equation $S(x) = D(x^p)D(x^{-1}) - \lambda G(x)$, we see that $D(x^p)D(x^{-1}) = (k - \lambda)x^g + \lambda G(x)$. Multiplying both sides by $D(x)$, we get

$$\begin{aligned}
 D(x^p)D(x)D(x^{-1}) &= D(x)((k - \lambda)x^g + \lambda G(x)) \\
 &\implies D(x^p)(\lambda G(x) + (k - \lambda)x^0) = D(x)(k - \lambda)x^g + \lambda G(x) \\
 &\implies D(x^p)\lambda G(x) + D(x^p)(k - \lambda)x^0 = D(x)(k - \lambda)x^g + \lambda D(x)G(x) \\
 &\implies \lambda D(1)G(x) + D(x^p)(k - \lambda)x^0 = D(x)(k - \lambda)x^g + \lambda D(1)G(x) \\
 &\implies D(x^p)(k - \lambda)x^0 = D(x)(k - \lambda)x^g \\
 &\implies D(x^p) = D(x)x^g
 \end{aligned}$$

Therefore we proved that $pD = D + g$ for some $g \in G$. Hence we proved that p is a multiplier of D . \square

In this chapter we explored difference sets and how symmetric BIBD's can be constructed from difference sets. An important theorem in this chapter was the multiplier theorem, which establishes the existence of multipliers in difference sets, which we dealt with a great detail.

Bibliography



- [1] .Combinatorial Designs:Constructions and Analysis by Douglas R.Stinson
- [2] .Combinatorial Theory by Marshall Hall,Jr.
- [3] .file:///E:/proj/block 20design/Combinatorial-20design