International Journal of Applied Science and Mathematics
Volume 1, Issue 2, ISSN (Online): 2394-2894

A Mathematical Review of Automorphisms for BIBD Designs and Applications

Teko Ganakmogo Motsumi
Department of Mathematics, University of Botswana

N. B. Okelo
School of Mathematics and Actuarial Science,
Jaramogi Oginga Odinga University of Science and Technology,
P. O. Box 210-40601, Bondo-Kenya
Email: bnyaare@yahoo.com

Abstract **– In this paper we review the mathematical concepts required for construction of t −designs via their isomorphisms and automorphisms. We give a description of Balanced Incomplete Block Designs (BIBDs), symmetric BIBDs and give an example of construction of a BIBD.**

Keywords **– BIBD, t-Designs, Review, Applications, Automorphisms.**

I. Introduction

In an experimental design, one is interested in comparing v different objects of interest (called treatments) by testing against b different subjects (called blocks). A complete design would require each block being subject to all v treatments and this, cost-wise is expensive, even for small values of v and b. To economize, a t −design in which not every k −set is a block can be designed in which each subject is tested in such a way that all t treatments are equally tested among the subjects. Therefore, the results of this study would be useful in; experimental design as a tool to control variability and minimization of cost.

II. Balanced Incomplete Designs

Definition.2.1.1. A block design is a family of b subsets of a set S of v elements such that, for some fixed k and λ, with $k < v$,$\lambda > 0$

- Each subset has k elements,
- Each pair of elements of t occurs together in exactly λ subsets.

The elements of S are called varieties, and the subsets of S are called the blocks.

Theorem 2.1.2. In a block design each element lies in exactly r blocks, where

$$r(k-1) = \lambda(v-1) \quad \text{and} \quad bk = vr \qquad (2.1.1)$$

Proof: Concentrate on any one of the elements, and suppose that it occurs in r blocks, for some r. Each of these r blocks contains $(k-1)$ other elements, so that the number of pairs including this chosen element is $r(k-1)$. But there are $(v-1)$ elements with which it can be paired with, and each pair occurs λ times. Hence

$$r(k-1) = \lambda(v-1) \qquad (2.1.2)$$

Since k, v and λ are fixed it follows that r must be the same for each element. For this fixed value of r, each element therefore has r appearances in the blocks, so that there are vr appearances of elements altogether. But there are b blocks each with k elements, so the number of appearances must also be bk. Thus $bk = rv$.▌

The five parameters b, v, r, k, λ of a block design are therefore not independent, but have two restrictions as stated in the theorem. Whatever b, v, r, k, λ are, they must satisfy (2.1), but conversely if five numbers b, v, r, k, λ satisfy (1.1), there is no guarantee that a (b, v, r, k, λ) −configuration exists.

(For example there is no BIBD with $v = 15, b = 21, k = 5, r = 7$ and $\lambda = 2$.This implies that there are still unsolved problems concerning BIBDs).

Corollary 2.1.3. If a(v, k, λ)-BIBD exists; then $\lambda(v-1) \equiv 0(mod\ k-1)$ and $\lambda v(v-1) \equiv 0(mod k(k-1))$.

For example an (8, 3, 1)-BIBD does not exist because $\lambda(v-1) = 7 \not\equiv 0(mod 2)$.

Apart from the above theorem, another important necessary condition for the existence of a(v, k, λ)-BIBD is known as "Fisher's inequality, proved in 1940.

Theorem 2.1.4. For a (b, v, r, k, λ)-configuration, $b \geq v$.

Proof: Let A be the incidence matrix, so that A has b rows and v columns. The aim is to find the matrix $C = A^{'}A$. Where $A^{'}$ is the transposed matrix of A. The element $a_{ij}^{'}$ in the i^{th} row and j^{th} column of $A^{'}$ is equal to a_{ji}, the element in the j^{th} row and the i^{th} column of A.

Then $C = (c_{ij})_{v\times v}$, where

$$c_{ij} = \sum_h a_{ih}^{'}\ a_{hj} = \sum_h a_{hi}\, a_{hj}$$

In particular,

$$c_{ii} = \sum_h a_{hi}^2 = \sum_h a_{hi}$$

Since each a_{ij} is 0 or 1 and $0^2 = 0, 1^2 = 1$. But $a_{hi} = 1$ if and only if the i^{th} element is the h^{th} set, and is 0 otherwise. Thus

$c_{ii} = \sum_h a_{hi}$

$= number\ of\ sets\ containing\ the\ i^{th}\ element = r$

Also, if $i \neq j$,

$c_{ij} = \sum_h a_{hi}a_{hj}$.

Now $a_{hi}a_{hj}$ is equal to 1 if and only if $a_{hi} = a_{hj} = 1$, that is, only if the h^{th} set contains both the i^{th} and the j^{th} elements.

There are λ such h's. Thus $c_{ij} = \lambda$, and

International Journal of Applied Science and Mathematics
Volume 1, Issue 2, ISSN (Online): 2394-2894

$$C = A^{'}A = \begin{bmatrix} r & \lambda & \lambda & & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & & \lambda \\ & \vdots & & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & r \end{bmatrix}$$

This result can also be written as
$A^{'}A = (r-\lambda)I + \lambda J$, where I denotes a unity matrix and J denotes the matrix with every entry equal to 1.

To show that $b \geq v$, let $\rho(C)$ denotes the rank of the matrix C,

$\rho(C) = \rho(A^{'}A) \leq \rho(A) \leq b.$ (2.1.3)

Since $\rho(XY) \leq \rho(Y)$ for all matrices X, Y, and the rank of a matrix is no greater than the number of its rows or columns.

However,

$$det \begin{bmatrix} r & \lambda & \lambda & & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & & \lambda \\ & \vdots & & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & r \end{bmatrix}$$

$$= det \begin{bmatrix} r & \lambda & \lambda & & \lambda \\ \lambda - r & r-\lambda & 0 & \cdots & 0 \\ \lambda - r & 0 & r-\lambda & & 0 \\ & \vdots & & \ddots & \vdots \\ \lambda - r & 0 & 0 & \cdots & r-\lambda \end{bmatrix}$$

On subtracting the first row from each of the others, and this in turn, on adding to the first column all the other columns, is equal to

$$det \begin{bmatrix} r+\lambda(v-1) & \lambda & \lambda & & \lambda \\ 0 & r-\lambda & 0 & & 0 \\ 0 & 0 & r-\lambda & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & r-\lambda \end{bmatrix}$$

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

$= rk(r-\lambda)^{v-1}$

$\neq 0$ since theorem above implies that $r > \lambda$

Thus C is a nonsingular $v \times v$ matrix, and so $\rho(C) = v$. Thus (1.3) gives $b \geq v$ as required.∎

III. Incidence Matrix

The incidence matrix A of a (v, b, r, k, λ)-BIBD satisfies the following properties:

1. every column of A contains exactly k "1"s;
2. every row of A contains exactly r "1"s;
3. two distinct rows of A contain "1" in exactly λ columns

Theorem 2.2.1. Let A be a $v \times b$ 0-1 matrix and let $2 \leq k < v$. Then A is an incidence matrix of a(v, b, r, k, λ)-BIBD if and only if $AA^{'} = \lambda J_v + (r-\lambda)I_v$ and $u_v A = ku_b$ where I_v denotes a $v \times v$ unity matrix and J_v denotes a $v \times v$ matrix with every entry equal to 1.

Proof: First, suppose (X, B) is a(v, k, λ)-BIBD, where $X = \{x_1, \ldots, x_v\}$ and $B = \{b_1, \ldots, b_b\}$. Let A be its incidence matrix. The (i, j)-entry of $AA^{'}$ is

$$\sum_{h=1}^{b} a_{i,h}\, a_{j,h} = \begin{cases} r \; if \; i = j \\ \lambda \; if \; i \neq j \end{cases}$$

Hence, from properties 2 and 3 enumerated above, every entry on the main diagonal of the matrix $AA^{'}$ is equal to r, and every off-diagonal entry is equal to λ so $AA^{'} = \lambda J_v + (r-\lambda)I_v$.

Furthermore, the i^{th} entry of $u_v A$ is equal to the number of "1"s in column i of A. By property 1, this equals k. Hence, $u_v A = ku_b$

Conversely, suppose that A is a $v \times b$ 0-1 matrix such that $AA^{'} = \lambda J_v + (r-\lambda)I_v$ and $u_v A = ku_b$. Let (X, B) be the design whose incidence matrix is A. Clearly *we* have $|X| = v$ and $|B| = b$. From the equation $u_v A = ku_b$, it follows that every block in A contains k points. From the equation $AA^{'} = \lambda J_v + (r-\lambda)I_v$, it follows that every pair of points occurs in exactly λ blocks. Hence, (X, B) is a (v, b, r, k, λ)-BIBD.∎

IV. Symmetric BIBDS

Definition.2.3.1. A BIBD in which $b = v$ (or equivalently,$r = k$ or $\lambda(v-1) = k^2 - k$) is called a Symmetric BIBD. (Note that this terminology does not mean that the incidence matrix is a symmetric matrix.)

The necessary existence conditions for symmetric BIBDs, which are known as "Bruck-Ryser-Chowla Theorem", are given by the following theorem which is stated without proof; it was published in 1950.

Theorem. 2.3.1 Suppose that a symmetric (v, k, λ)-configuration exists. Then:

a) if v is even, $k - \lambda$ must be a square;
b) if v is odd, the equation $z^2 = (k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$ has a solution in integers x, y, z not all zero.

The proof of (a) follows from the proof of Fisher's inequality that $(detA)^2 = detC = k^2(k-\lambda)^{v-1}$, that is $detA = k(k-\lambda)^{(v-1)/2}$. So $(k-\lambda)^{(v-1)/2}$ is a rational number. But if $v - 1$ is odd this requires that $k - \lambda$ is itself a square.

2.4. Example of constructing BIB designs

Now consider $v = 7, b = 7, k = 3$, the conditions are fulfilled with;

$$r = \frac{bk}{v} = \frac{7 \times 3}{7} = 3$$

$$\lambda = r\frac{(k-1)}{v-1} = \frac{3 \times 2}{6} = 1$$

Let the points be A, B, C, D, E, F, and G. Ordering the 3 blocks with A first and assume that B-C, D-E and F-G are together in these blocks. We obtain:

Step one

Table 2.4.1: Results of Step one

A	A	A				
B	D	F				
C	E	G				

Second step

Next B and C must occur twice more and not together (order of blocks not important). The result is:

Table 2.4.2. Results of Step two.

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

International Journal of Applied Science and Mathematics
Volume 1, Issue 2, ISSN (Online): 2394-2894

Third step

D and F must occur together. We can assume this happens in a B block. The E and G must be together in the other B block. Then there is only one choice for the two C blocks (because order is unimportant). We get:

Table 2.4.3: $2-$ (7,3,1)-configuration.

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

When using this design for practical experiments we must randomize. We randomize the treatments according to the labels, the order of the blocks, and the order of the three treatments within a block.

The complementary design

The complementary design is constructed by replacing each block with a block consisting of the remaining points. In our case we get:

Table 2.4.4: Complementary design.

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

We see that $v = 7, r = 4, b = 7, k = 4$ and $\lambda = 2$.

Note that we could construct the same BIB designs by use of PG (2, 2).

V. Construction and Resolvability of Designs

Our construction use the concept of: congruence modulo an integer n

2.5.1. Ordered Pairs, Relations, and Functions

Definition.2.5.1.1. An ordered pair (a, b) is a list with two elements. That is, ordered pair consists of two objects. A relation from a set A to a set B is a set of ordered pairs whose first entries are in A and whose second entries are in B. A is called the Domain of the relation and B is called the Range. A function from A to B is a relation from A to B that associates with each element a of A a unique element b of B.

Definition 2.5.1.2. One-to –one Function

A function f is called a one-to-one function or injection if it associates different values in the range with different values in the domain.

Definition 2.5.1.3. Onto functions and Bijections

A function f from A onto B is defined as a function from A to B such that each member of B is associated with atleast one member of A. A function from A onto B is also called a surjection from A to B.

A one-to-one function from a set A onto a set B is called a Bijection. A bijection from a set A onto itself is called a permutation of that set.

VI. Isomorphism and Automorphism

Definition 2.5.2.1. Suppose (X, A) and (Y, B) are two designs with $|X| = |Y|$. (X, A) and (Y, B) are isomorphic if there exists a bijection $\alpha: X \to Y$ such that:

$[\{\alpha(x): x \in A_1\}: A_1 \in A] = B$

In other words if we rename every point $x \in X$ by $\propto (x)$, then the collection of blocks of A is transformed into B. The bijection $\propto$ is called an isomorphism.

Definition 2.5.2.2. Suppose (X, A) is a design. An Automorphism of (X, A) is an isomorphism of this design with itself. In this case, the bijection $\propto$ is a permutation of X such that:

$[\{\propto (x): x \in A_1\}: A_1 \in A] = A$

Definition 2.5.2.3. Equivalence Relation

A relation R on a set S is a set of ordered pairs of elements of S. A set R of ordered pairs of elements of a set X is an equivalence relation on X if:

1) (x, x) is in R for all x in X (reflexive law)
2) If (x, y) is in R then (y, x) is in R for all x and y in X. (symmetric law)
3) If (x, y) and (y, z) are in R, the (x, z) is in R for all x, y and z in X. (transitive law)

Definition 2.5.2.4. Equivalence Classes

Let R be an equivalence relation on a set X. Then there is a collection C of nonempty subsets of X such that:

1) Each element x of X is in some set C_x of C
2) Any two different sets in C are disjoint.
3) For each set C_y in C, all elements of C_y are equivalent relative to R
4) If two elements x and y are equivalent relative to R, then they lie in the same set of C (in fact $C_y = C_x$)

The sets C_x in the collection C are called equivalence classes. A collection of C of nonempty, mutually disjoint sets whose union is X is called a Partition of X, or a set partition of X.

Definition 2.5.2.5. Congruence modulo an integer n a is congruent to b modulo n, written $a \equiv b \,(mod\, n)$, if and only if n is a factor of $a - b$. This relation is an equivalence relation. Since n is a factor of '$a - a = 0$' our relation is reflexive. Since n is a factor of $b - a = -(a - b)$ whenever it is a factor of $b - a$, our relation is symmetric. Now suppose $a \equiv b \,(mod\, n)$ and $b \equiv c \,(mod\, n)$, so $c - b = kn$, and $b - c = hn$. Then $a - c = a - b + b - c = kn + hn = (k + h)n$, so our relation is transitive. Thus, it is an equivalence relation.

2.5.3. Arithmetic of integers modulo n

Arithmetic of integers modulo n provides a powerful tool for constructing of designs.

Definition 2.5.3.1. Cyclic designs

A balanced design is said to be cyclic $mod\, n$ with base B if :

1) The element of v are equivalence classes $mod\, n$
2) B is a set of blocks of the design
3) Every block in the design may be obtained in exactly one way by adding some $m \,(mod\, n)$ to each element of a block in B.

International Journal of Applied Science and Mathematics
Volume 1, Issue 2, ISSN (Online): 2394-2894

Example 2.5.3.2. If $v = \{0,1,2,3,4\}$ is the set of equivalence classes mod 5, and $B = \{(0,1),(2,4)\}$, then B is a base for the design. When we add 1 to each element of (1, 0) we get another pair 1 unit apart. Continuing in this way, we get all pairs 1 unit apart [2]. We also get (4, 0) which is also a pair 1 unit apart, if we arrange 0, 1,2,3,4 around a circle in a natural order. It is this circular visualization of distance that underlies the use of the word cyclic. In the same way, we get every pair 2 units apart by repeatedly adding 1 to the pair (2, 4). By shifting our base blocks around the circle one place at a time, we ensure that every point appears the same number of times as every other point [4].

The fact that each difference appears once means that as we move around the circle, each pair of the numbers with difference 1 appears once, each pair with difference 2 appears once and so on.

In general, suppose we have a base of blocks for our design. We visualize them as sets on a circle labeled by the integers $modulo\ n$.

Theorem 2.5.3.3. A set B of k-elements of the integer's $mod\ n$ is a base (difference set) for a design which is a cyclic $mod\ n$ if and only if each nonzero integer $mod\ n$ occurs the same number of times as a difference $a - b$ of distinct elements chosen from the set in B.

Proof: Suppose B is a base. Then if the pair (a, b) is in λ blocks then $a - b$ is difference between λ pairs in the base blocks. Now suppose each nonzero integer $mod\ n$ appears the same number σ of times as a difference between pairs in B. Then for some list of numbers $m_1, m_2, m_3 \cdots m_\sigma$ the pairs $\{a + m_i, b + m_i\}$ must be distinct pairs in the blocks of B. Thus any pair $(a + m, b + m)$ will occur σ times in the blocks we generate from B by adding numbers. Thus we have a family of k-element sets generated from B such that each pair of elements of v, the integers $mod\ n$, occurs exactly σ times among the sets. Now, if one class x occurs r times and another class y occurs r' times, then x is in $r(k-1)$ pairs in the blocks and y is in $r'(k-1)$ pairs in the blocks. Since the number of pairs involving each element is the same $r = r'$. Thus B is a base for a design.∎

Definition 2.5.3.4. Cyclic Designs

Suppose we introduce a new element ∞ to the integers mod n and define

$\infty + m = \infty - m = \infty,$

$m - \infty = -\infty - m = -\infty$ for all m

A balanced design is said to be $\infty -$ cyclic $mod\ n$ if v consists of ∞ and the equivalence classes of integers $mod\ n$, and if it has a base B satisfying conditions (ii) and (iii) of the (definition 2.5.3.1).

Theorem 2.5.3.5. If B is a family of $k -$ element subsets of the equivalence classes of integers $mod\ n$ and ∞, the B is the a base for an $\infty -$cyclic design if and only if $\infty, -\infty$ and each residues $mod\ n$ occurs the same number of times as the difference of elements of the same set in B and if no proper subset of B has this property [1].

For example the sets $\{(0,1,3),(4,5,9),(2,6,8),(\infty,7,10)\}$ form a base for a (12, 3, 2) $\infty -$ cyclic design mod 11.

VII. Resolvable Design

A $t - (v, k, \lambda)$ design is resolvable if the blocks B may be grouped into a S sets each of which is a partition of V. (note, we partition the blocks into sets of blocks, each set of which is a partition of V into parts of size k).

Each of the partitions of V is called a parallel class of the blocks in analogy to the parallel line in a plane geometry[3]. A parallel class is a subset of disjoint blocks from B whose union is V. A partition of B into r parallel classes is called a resolution, and a (v, k, λ) is said to be a resolvable if B has atleast one resolution [2].

Theorem 2.5.4.1. If a design is resolvable, then $\frac{b}{r}$ and $\frac{v}{k}$ are the same integer.

Proof: Since V is a union of some number m of disjoint sets of size k, then $v = km$. Thus $\frac{v}{k}$ is an integer. But since $bk = vr$, we get by division $\frac{v}{k} = \frac{b}{r}$.

Therefore a $t - (v, k, \lambda)$ can have a parallel class only if $v \equiv 0\ mod\ k$.

Theorem 2.5.4.2. A cyclic or $\infty -$ cyclic design is resolvable if it has a base which is a partition of V.∎

2.5.5. Constructing new designs from old

This is the construction whose techniques are based on putting two designs together or modifying an existing design to get anew one [3]. There are quite a few elementary and straightforward ways to construct new designs from existing ones; we describe a number of these ways here.

2.5.5.1. Complementary Designs

Is a design obtained by replacing each block of B of a design D on V by its complement $V - B$. This design which is denoted by $\overline{D}$, is called complementary design or complement of D.A complement of a $t - (v, k, \lambda)$ design is a $t - \left(v, v-k, \lambda\binom{v-t}{t}/\binom{k}{t}\right)$ design or a $t - (v, k, \lambda_{max} - \lambda)$ design where $\lambda_{max} = \binom{v-t}{k-t}$

2.5.5.2. Residue Design

For a fixed element $x \in V$, we can partition B into two sets, those blocks B_d containing x and those blocks B_t not containing x. it is easily shown that:

$(v{:}\backslash \{x\}, B_t)$ is a

$(t-1) - [v-1, k, \lambda(v-k)/(k-t+1)]$

This is termed as the residual design of a $t - (v, k, \lambda)$.

2.5.5.3. Derived Design

Removing x from each block of B_d to form B_d^x yields a $(t-1) - (v,\ k-1,\ \lambda)$ design.

$(v{:}\backslash \{x\}, B_d^x)$ is called the derived design of a $t - (v, k, \lambda)$.

2.5.5.4. Dual design

The incidence matrix N of a design with B blocks and V varieties, then by transposing this matrix N to get N^t we get the incidence matrix of a design with V blocks and B varieties. The design whose incidence matrix is N^t is called the dual of the original design. By Fishers inequality, the dual design can be a design only if $b = v$.

2.5.5.5. Unions of designs

When a simple design D and its complement design $\overline{D}$ are put together we obtain the set of all subsets of size k

chosen from V. Thus, putting these two balanced designs together gives another balanced design[4].

2.5.5.6. Product of Designs

Given designs D_1 and D_2 on sets V_1 and V_2 we define the product design $D_1 \times D_2$ to be the design of the set of ordered pairs $V_1 \times V_2$ whose blocks are the sets $B_1 \times B_2$ with B_1 a block of D_1 and B_2 a block of D_2 .

2.5.5.7. Sum Construction

Given two BIBDs on the same point set, “sum construction” involves forming the collection of all the blocks in both designs[5].

Theorem 2.5.5.7.1. Suppose there exists a $(v, k, \lambda_1) -$ BIBD and a $(v, k, \lambda_2) -$ BIBD. Then there exists a $(v, k, \lambda_1 + \lambda_2) -$ BIBD.

Corollary 2.5.5.7.2. Suppose there exists a $(v, k, \lambda) -$ BIBD. Then there exists a $(v, k, s\lambda) -$ BIBD for all integers $s \geq 1$.

VIII. Conclusion

BIBDs are very important in research and properly developed designs give appropriate results when doing statistical analysis.

References

[1] B. Adhikari, On the symmetric differences of pairs of blocks of incomplete block designs, *Calcutta stat. Assoc. Bull* 16, p45, 1967.

[2] I. Anderson, *A first Course in Combinatorial Mathematics second edition*, Oxford University Press, New York, 1989.

[3] L. Blanchard, A construction for Steiner 3-designs, *Journal of combinatorial Theory A*, 71, p60,1995.

[4] D. R Stinson, *Combinatorial Designs: Construction and Analysis*, Springer_Verlag, New York, 2004.

[5] K. P. Bogart, *Introductory Combinatorics second edition*, Harcourt Brace Jovanovich, Inc. Orlando, Florida, 1990.

Authors Profiles

Dr. Teko Ganakmogo Motsumi
is a senior lecturer in the department of mathematics, University of Botswana.

Dr. Benard Okelo
is a lecturer in the department of mathematics, Jaramogi Oginga Odinga University of Science and Technology. He was the AU-TWAS Young scientist national award winner of Kenya, 2013.