Chapter 1

*BIBD*s

1.1 Definition and Fundamental Properties of *BIBD*s

Definition 1.1 *Let v, k and λ be integers such that $v \geq k \geq 2$ and $\lambda \geq 1$. Let X be a finite set of elements, called points, and let $\mathcal{B}$ be a finite collection of subsets of X, called blocks. The pair $(X, \mathcal{B})$ is called a (v, k, λ) balanced incomplete block design or, simply, a (v, k, λ)-BIBD, if the following conditions hold:*

(i) $|X| = v$.

(ii) $|B| = k$ *for all* $B \in \mathcal{B}$.

(iii) *Every pair of distinct points is contained in exactly λ blocks.*

The set $\{v, k, \lambda\}$ is called the set of parameters of the BIBD $(X, \mathcal{B})$. We also use the notation $\mathcal{D} = (X, \mathcal{B})$.

Remark 1.1 A *BIBD* may contain repeated blocks if $\lambda > 1$, which is why we refer to $\mathcal{B}$ as a collection of subsets rather than a set of subsets.

Remark 1.2 If $k = 1$, then we must have $\lambda = 0$; this case is excluded by the assumption $\lambda \geq 1$. Therefore for a (v, k, λ)-*BIBD* we always assume $k \geq 2$ in Definition 1.1. If $v = k$, then every block is equal to X and $(X, \mathcal{B})$ is called a *complete block design*; this is the trivial case. A (v, k, λ)-*BIBD* with $v > k \geq 2$ is said to be *nondegenerate*. In most cases we consider only nondegenerate *BIBD*s.

Example 1.1 *A $(7, 3, 1)$-BIBD.*

$$X = \{1, 2, 3, 4, 5, 6, 7\},$$
$$\mathcal{B} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 7\}, \{2, 5, 6\}, \{3, 4, 6\}, \{3, 5, 7\}\}.$$

In Section 2.3 we will see that $(X, \mathcal{B})$ is a projective plane of order 2.

Example 1.2 *A* $(9,3,1)$*-BIBD.*

$$X = \{1,2,3,4,5,6,7,8,9\},$$
$$\mathcal{B} = \{\{1,2,3\},\{4,5,6\},\{7,8,9\},\{1,4,7\},\{2,5,8\},\{3,6,9\},\\ \{1,5,9\},\{2,6,7\},\{3,4,8\},\{1,6,8\},\{2,4,9\},\{3,5,7\}\}.$$

In Section 3.2 we will see that this $(9,3,1)$-*BIBD* is an affine plane of order 3.

Example 1.3 *A* $(16,6,2)$*-BIBD.*

Let $X = \mathbb{Z}_{16} = \{0,1,2,\ldots,15\}$ *and arrange the 16 points in the following* 4×4 *array*

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

For each $i \in \mathbb{Z}_{16}$*, let* B_i *be the subset of* $\mathbb{Z}_{16}$ *consisting of the six elements which are situated in the same row or the same column of* i *and are distinct from* i*. For example,* $B_0 = \{1,2,3,4,8,12\}, B_5 = \{1,4,6,7,9,13\}$*, etc. Let* $\mathcal{B} = \{B_i : i \in \mathbb{Z}_{16}\}$*. Clearly* $|B_i| = 6$ *for all* $i \in \mathbb{Z}_{16}$ *and any pair of points is contained in exactly two blocks. For example,* $\{5,10\} \subset B_6, B_9$*. Hence* $(X,\mathcal{B})$ *is a* $(16,6,2)$*-BIBD.*

In Section 2.1 we will see that this $(16,6,2)$-*BIBD* is a symmetric design.

Example 1.4 *Let* X *be a set of* v *points and* $\mathcal{B}$ *consist of all subsets of* X *of size* k*. Then any two points are contained in* $\binom{v-2}{k-2}$ *blocks. Thus* $(X,\mathcal{B})$ *is a* $(v,k,\binom{v-2}{k-2})$*-BIBD.*

Definition 1.2 *Let* $(X,\mathcal{B})$ *be a* (v,k,λ)*-BIBD. Suppose that* $|\mathcal{B}| = b$*. Define a* $v \times b$ *0-1 matrix*

$$M = (m_{ij})_{1 \le i \le v, 1 \le j \le b},$$

whose rows are indexed by the points $p_1, p_2, \ldots, p_v$ *and columns are indexed by the blocks* $B_1,\ B_2,\ \ldots,\ B_b$*, by*

$$m_{ij} = \begin{cases} 1, & \text{if } p_i \in B_j, \\ 0, & \text{otherwise.} \end{cases}$$

Then M is called the incidence matrix of the BIBD $(X, \mathcal{B})$.

Clearly, the incidence matrix of a $BIBD$ depends on the ordering of the points and the ordering of the blocks. For another ordering of points $q_1, q_2, \ldots, q_v$ and another ordering of blocks $C_1, C_2, \ldots, C_b$, the incidence matrix M' of the design takes the form

$$M' = PMQ,$$

where $P = (p_{ij})_{1 \le i,j \le v}$ is a $v \times v$ permutation matrix defined by

$$p_{ij} = \begin{cases} 1, & \text{if } q_i = p_j, \\ 0, & \text{otherwise,} \end{cases}$$

and $Q = (q_{ij})_{1 \le i,j \le b}$ is a $b \times b$ permutation matrix defined by

$$q_{ij} = \begin{cases} 1, & \text{if } B_i = C_j, \\ 0, & \text{otherwise.} \end{cases}$$

Two incidence matrices of the same $BIBD$ with respect to different orderings of points and blocks are said to be *equivalent*.

Example 1.5 *In the $(7,3,1)$-BIBD of Example 1.1, let*

$$p_1 = 1,\ p_2 = 2,\ p_3 = 3,\ p_4 = 4,\ p_5 = 5,\ p_6 = 6,\ p_7 = 7$$

and

$$\begin{aligned} &B_1 = \{1,2,3\},\ B_2 = \{1,4,5\},\ B_3 = \{1,6,7\},\ B_4 = \{2,4,7\}, \\ &B_5 = \{2,5,6\},\ B_6 = \{3,4,6\},\ B_7 = \{3,5,7\}. \end{aligned}$$

Then the $(7,3,1)$-BIBD has incidence matrix

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

If we let

$$q_1 = 1,\ q_2 = 2,\ q_3 = 3,\ q_4 = 4,\ q_5 = 5,\ q_6 = 7,\ q_7 = 6,$$

then with respect to the ordering of points $q_1, q_2, q_3, q_4, q_5, q_6, q_7$ *and the ordering of blocks as before the* $(7,3,1)$*-BIBD has incidence matrix*

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}, \tag{1.1}$$

which is a symmetric matrix.

Example 1.6 *The incidence matrix of the* $(9,3,1)$*-BIBD of Example 1.2 is the* 9×12 *0-1 matrix*

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Now we give some basic properties of a (v,k,λ)-$BIBD$.

Theorem 1.1 *In a* (v,k,λ)*-BIBD, every point occurs in exactly*

$$r = \frac{\lambda(v-1)}{k-1} \tag{1.2}$$

blocks.

Proof. By rearranging the points and the blocks, we can assume any given point to be the first point which appears in the first r blocks. Then the incidence matrix takes the form

$$M = \begin{pmatrix} 1\ldots 1 & 0 \ldots 0 \\ M_1 & M_2 \end{pmatrix},$$

where M_1 is a $(v-1)\times r$ matrix and M_2 is a $(v-1)\times(b-r)$ matrix. Count the number of 1's in M_1 in two different ways. On the one hand, M_1 has r columns and each column has $k-1$ 1's. On the other hand, M_1 has $v-1$ rows and each row has λ 1's. Therefore, $r(k-1) = \lambda(v-1)$, which implies (1.2). ∎

By Theorem 1.1 the number of blocks containing any given point in a (v, k, λ)-$BIBD$ is a constant, which is denoted by r and is called the *replication number* of the $BIBD$.

Theorem 1.2 *A (v, k, λ)-$BIBD$ has exactly*

$$b = \frac{vr}{k} = \frac{\lambda(v^2 - v)}{k^2 - k} \tag{1.3}$$

blocks.

Proof. Let M be the incidence matrix of the (v, k, λ)-$BIBD$. Count the number of 1's in M in two different ways. Firstly, M has b columns and each column has k 1's. Secondly, M has v rows and by Theorem 1.1, each row has r 1's. Thus $bk = vr$, which implies $b = \frac{vr}{k}$. Substituting (1.2) into it, we obtain $b = \frac{\lambda(v^2-v)}{k^2-k}$. ∎

A (v, k, λ)-$BIBD$ is also called a (v, b, r, k, λ)-$BIBD$, where $r = \frac{\lambda(v-1)}{k-1}$ and $b = \frac{vr}{k}$, and $\{v, b, r, k, \lambda\}$ is also called the set of its parameters.

Theorem 1.3 *Let M be a $v \times b$ 0-1 matrix. Then M is the incidence matrix of a (v, k, λ)-$BIBD$ if and only if both*

$$M\,{}^tM = \lambda J_v + (r - \lambda) I_v \tag{1.4}$$

and

$$1_v M = k 1_b \tag{1.5}$$

hold, where ${}^tM$ denotes the transpose of M, $r = \lambda(v-1)/(k-1)$, J_v and I_v are the $v \times v$ all 1's matrix and the identity matrix, respectively, and 1_v and 1_b are the v-dimensional and b-dimensional all 1 row vectors, respectively.

Proof. First, let M be the incidence matrix of a (v, k, λ)-$BIBD$ $(X, \mathcal{B})$ and let $X = \{p_1, \ldots, p_v\}$ and $\mathcal{B} = \{B_1, \ldots, B_b\}$. Then the (i, j)-entry of $M\,{}^tM$ is

$$\sum_{k=1}^{b} m_{ik} m_{jk} = \begin{cases} r, & \text{if } i = j, \\ \lambda, & \text{if } i \neq j. \end{cases}$$

Hence every entry on the main diagonal of $M\,{}^tM$ is equal to r and every off-diagonal entry is equal to λ, so $M\,{}^tM = \lambda J_v + (r - \lambda) I_v$.

Moreover, the i-th entry of $1_v M$ is equal to the number of 1's in the i-th column of M, which is equal to the size of the i-th block, and hence, is equal to k. Therefore $1_v M = k 1_b$.

Conversely, suppose M is a $v \times b$ 0-1 matrix which satisfies (1.4) and (1.5). Let $X = \{p_1, \ldots, p_v\}$ and

$$M = (m_{ij})_{1 \le i \le v, 1 \le j \le b}.$$

Define

$$B_j = \{p_i \in X : m_{ij} = 1\}, \quad j = 1, 2, \ldots, b$$

and $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$. By (1.5), there are k 1's in every column of M, so $|B_i| = k$ for all $i = 1, 2, \ldots, b$. From (1.4) it follows that every pair of distinct points is contained in exactly λ blocks. Therefore $(X, \mathcal{B})$ is a (v, k, λ)-*BIBD* with M as its incidence matrix. ∎

Example 1.7 *Let A be the incidence matrix of the $(9,3,1)$-BIBD of Example 1.2, viz., A is the matrix given in Example 1.6. Let*

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

$$C = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

$$D = J - C,$$

where J is the 3×12 all 1 matrix. Then it can be verified directly that

$$M = \begin{pmatrix} {}^tA & {}^tA & {}^tC & {}^tD \\ B & J - B & 0 & 0 \end{pmatrix}$$

is the incidence matrix of a $(16, 6, 3)$-BIBD.

Theorem 1.4 (Fisher's Inequality) *In any nondegenerate (v, b, r, k, λ)-BIBD, $b \ge v$.*

Proof. Let M be the incidence matrix of the *BIBD*. By Theorem 1.3

$$M\,{}^tM = \lambda J_v + (r - \lambda) I_v.$$

Let us calculate $\det(M\,{}^tM)$.

$$
\begin{aligned}
&\det(M^{\,t}M)\\
&= \det\begin{pmatrix} r & \lambda & \lambda & \dots & \lambda \\ \lambda & r & \lambda & \dots & \lambda \\ \lambda & \lambda & r & \dots & \lambda \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda & \lambda & \lambda & \dots & r \end{pmatrix}\\
&= \det\begin{pmatrix} r+\lambda(v-1) & r+\lambda(v-1) & r+\lambda(v-1) & \dots & r+\lambda(v-1) \\ \lambda & r & \lambda & \dots & \lambda \\ \lambda & \lambda & r & \dots & \lambda \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda & \lambda & \lambda & \dots & r \end{pmatrix}\\
&= (r+\lambda(v-1))\det\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \lambda & r & \lambda & \dots & \lambda \\ \lambda & \lambda & r & \dots & \lambda \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda & \lambda & \lambda & \dots & r \end{pmatrix}\\
&= (r+\lambda(v-1))\det\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ \lambda & r-\lambda & 0 & \dots & 0 \\ \lambda & 0 & r-\lambda & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda & 0 & 0 & \dots & r-\lambda \end{pmatrix}\\
&= (r+\lambda(v-1))(r-\lambda)^{v-1}.
\end{aligned}
$$

Since $v \neq 1$, we have $r+\lambda(v-1) \neq 0$. Since the $BIBD$ is nondegenerate, we have $v > k$ and by Theorem 1.1 $r > \lambda$. Therefore $\det(M^{\,t}M) \neq 0$, which implies $b \geq v$. ∎

Theorems 1.1, 1.2 and 1.4 are necessary conditions for the existence of a (v, k, λ)-$BIBD$. We can use them to exclude some parameter sets to be the parameter sets of $BIBD$s as the following examples show.

Example 1.8 *There does not exist an* $(8, 3, 1)$-$BIBD$*, for*

$$r = \frac{\lambda(v-1)}{k-1} = \frac{7}{2} \notin \mathbb{Z}.$$

Example 1.9 *There does not exist a* $(19, 4, 1)$-$BIBD$*, for*

$$r = \frac{\lambda(v-1)}{k-1} = 6, \ \textit{but } b = \frac{vr}{k} = \frac{19 \cdot 3}{2} \notin \mathbb{Z}.$$

Example 1.10 *There does not exist a* $(16, 6, 1)$-*BIBD, for*

$$r = \frac{\lambda(v-1)}{k-1} = 3, \text{ but } b = \frac{vr}{k} = 8 < v = 16.$$

One of the main goals of combinatorial design theory is to determine necessary and sufficient conditions of the parameter set $\{v, k, \lambda\}$ for the existence of a (v, k, λ)-*BIBD*. This is a very difficult problem in general, and there are many parameter sets in which the answers are not yet known. For example, it is currently unknown if there exists a (22,8,4)-*BIBD* (such a *BIBD* would have $r = 12$ and $b = 33$). On the other hand, there are many known constructions for infinite classes of *BIBD*s, as well as some other necessary conditions, which will be discussed a bit later.

1.2 Isomorphisms and Automorphisms

Definition 1.3 *Let* $(X, \mathcal{B})$ *and* $(Y, \mathcal{C})$ *be two BIBDs. If there is a bijective map* $\alpha : X \to Y$ *and a bijective map* $\alpha : \mathcal{B} \to \mathcal{C}$ *such that for all* $x \in X$ *and* $B \in \mathcal{B}$, $x \in B$ *if and only if* $\alpha(x) \in \alpha(\mathcal{B})$, *then* $(X, \mathcal{B})$ *and* $(Y, \mathcal{C})$ *are said to be isomorphic and* α *is called an isomorphic map or an isomorphism. (Note that we use the same symbol* α *to denote both the map* $X \to Y$ *and the map* $\mathcal{B} \to \mathcal{C}$.)

If $(X, \mathcal{B})$ *and* $(Y, \mathcal{C})$ *are isomorphic BIBDs, we write* $(X, \mathcal{B}) \simeq (Y, \mathcal{C})$.

Example 1.11 *Consider the* $(4, 2, 2)$-*BIBDs* $(X, \mathcal{B})$ *and* $(Y, \mathcal{C})$.

$$X = \{1, 2, 3, 4\},$$
$$\mathcal{B} = \{B_1, B_2, B_3, B_4, B_5, B_6, B_7, B_8, B_9, B_{10}, B_{11}, B_{12}\},$$

where

$$B_1 = B_2 = \{1, 2\}, \ B_3 = B_4 = \{3, 4\}, \quad B_5 = B_6 = \{1, 3\},$$
$$B_7 = B_8 = \{2, 4\}, \ B_9 = B_{10} = \{1, 4\}, \ B_{11} = B_{12} = \{2, 3\},$$

and

$$Y = \{a, b, c, d\},$$
$$\mathcal{C} = \{C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, C_{10}, C_{11}, C_{12}\},$$

where

$$C_1 = C_2 = \{a, b\}, \ C_3 = C_4 = \{c, d\}, \quad C_5 = C_6 = \{a, c\},$$
$$C_7 = C_8 = \{b, d\}, \ C_9 = C_{10} = \{a, d\}, \ C_{11} = C_{12} = \{b, c\}.$$

Define a bijection $\alpha : X \to Y$ *by* $\alpha(1) = a$, $\alpha(2) = b$, $\alpha(3) = c$, $\alpha(4) = d$ *and a bijection* $\alpha : \mathcal{B} \to \mathcal{C}$ *by* $\alpha(B_1) = C_2$, $\alpha(B_2) = C_1$, *and* $\alpha(B_i) = C_i, 3 \leqslant i \leqslant 12$. *Then* α *is an isomorphism from* $(X, \mathcal{B})$ *to* $(Y, \mathcal{C})$.

If $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ are two $BIBD$s without repeated blocks, we also adopt the following definition of isomorphism.

Definition 1.4 *Let $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ be two $BIBD$s without repeated blocks. If there exists a bijection $\alpha : X \to Y$ such that*

$$\{\{\alpha(x) : x \in B\} : B \in \mathcal{B}\} = \mathcal{C},$$

then $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ are said to be isomorphic and α is called an isomorphic map or an isomorphism. In other words, if we rename every point $x \in X$ by $\alpha(x)$, then the collection of blocks $\mathcal{B}$ is transformed into $\mathcal{C}$.

Clearly, when $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ are two $BIBD$s without repeated blocks, Definitions 1.3 and 1.4 are equivalent.

Example 1.12 *Here are two $(7, 3, 1)$-$BIBD$s $(X, \mathcal{B})$ and $(Y, \mathcal{C})$:*

$X = \{1, 2, 3, 4, 5, 6, 7\}$,
$\mathcal{B} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 7\}, \{2, 5, 6\}, \{3, 4, 6\}, \{3, 5, 7\}\}$

and

$Y = \{a, b, c, d, e, f, g\}$,
$\mathcal{C} = \{\{a, b, d\}, \{a, c, e\}, \{a, f, g\}, \{b, c, g\}, \{b, e, f\}, \{c, d, f\}, \{d, e, g\}\}$.

Define a bijection $\alpha : X \to Y$ by $\alpha(1) = a, \alpha(2) = b, \alpha(3) = d, \alpha(4) = c, \alpha(5) = e, \alpha(6) = f, \alpha(7) = g$. Clearly, $\mathcal{B}$ is transformed to $\mathcal{C}$ by α. Hence $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ are isomorphic and α is an isomorphism.

If we define $\beta : X \to Y$ by $\beta(1) = a, \beta(2) = g, \beta(3) = f, \beta(4) = c, \beta(5) = e, \beta(6) = d, \beta(7) = b$. It can also be verified that $\mathcal{B}$ is transformed to $\mathcal{C}$ by β. Thus β is another isomorphism.

Clearly, isomorphic $BIBD$s have the same parameter set, and we usually do not distinguish isomorphic $BIBD$s. It is left as an exercise (Exercise 1.5) to show that there is only one (7,3,1)-$BIBD$ up to an isomorphism. In general, it is a difficult computation problem to determine whether two $BIBD$s with the same parameter set are isomorphic . There are $v!$ possible bijections between two sets of cardinality v. To identify that two (v, k, λ)-$BIBD$s are not isomorphic, we must show that none of the possible $v!$ bijections is an isomorphism. Since $v!$ grows exponentially quickly as a function of v, it soon becomes impractical to actually test every possible bijection. Thus we have to try to find more sophisticated algorithms rather than testing every possibility exhaustively.

Isomorphism of $BIBD$s can also be described in terms of incidence matrices.

Theorem 1.5 *Let $M = (m_{ij})_{1 \le i \le v, 1 \le j \le b}$ and $N = (n_{ij})_{1 \le i \le v, 1 \le j \le b}$ be the incidence matrices of two (v, b, r, k, λ)-BIBDs $(X, \mathcal{B})$ and $(Y, \mathcal{C})$, respectively. Then $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ are isomorphic, if and only if there is a permutation β of $\{1, 2, \ldots, v\}$ and a permutation γ of $\{1, 2, \ldots, b\}$ such that*

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

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

Proof. Let $X = \{x_1, \ldots, x_v\}, \mathcal{B} = \{B_1, \ldots, B_b\}, Y = \{y_1, \ldots, y_v\}$, and $\mathcal{C} = \{C_1, \ldots, C_b\}$.

Suppose first that $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ are isomorphic. Then there exists a bijection $\alpha : X \to Y$ and a bijection $\alpha : \mathcal{B} \to \mathcal{C}$ such that $x_i \in B_j$ if and only if $\alpha(x_i) \in \alpha(B_j)$. Define a permutation β of $\{1, 2, \ldots, v\}$ by

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

and a permutation γ of $\{1, 2, \ldots, b\}$ by

$$\gamma(j) = k \text{ if and only if } \alpha(B_j) = C_k.$$

Then

$$\begin{aligned} m_{ij} = 1 &\Leftrightarrow x_i \in B_j \\ &\Leftrightarrow \alpha(x_i) \in \alpha(B_j) \\ &\Leftrightarrow y_{\beta(i)} \in C_{\gamma(j)} \\ &\Leftrightarrow n_{\beta(i),\gamma(j)} = 1. \end{aligned}$$

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

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

$$\alpha(B_j) = C_k \text{ if and only if } \gamma(j) = k.$$

Then it is easy to verify that α is an isomorphism of $(X, \mathcal{B})$ and $(Y, \mathcal{C})$. ∎

Let $(X, \mathcal{B}), (Y, \mathcal{C})$, and $(Z, \mathcal{E})$ be *BIBD*s. Assume $(X, \mathcal{B}) \simeq (Y, \mathcal{C})$ and $(Y, \mathcal{C}) \simeq (Z, \mathcal{E})$. Then there is a bijective map $\alpha : X \to Y$ and a bijective map $\alpha : \mathcal{B} \to \mathcal{C}$ such that for all $x \in X$ and $B \in \mathcal{B}$, $x \in B$ if and only if $\alpha(x) \in \alpha(B)$, and there is a bijective map $\beta : Y \to Z$ and a bijective map $\beta : \mathcal{C} \to \mathcal{E}$ such that for all $y \in Y$ and $C \in \mathcal{C}$, $y \in C$ if and only if $\beta(y) \in \beta(C)$. Define a bijective map $\beta \circ \alpha : X \to Z$ by $(\beta \circ \alpha)(x) = \beta(\alpha(x))$ for all $x \in X$ and a bijective map $\beta \circ \alpha : \mathcal{B} \to \mathcal{E}$ by $(\beta \circ \alpha)(B) = \beta(\alpha(B))$

for all $B \in \mathcal{B}$. $\beta \circ \alpha$ is called the *composite* of β and α. Clearly, for all $x \in X$ and $B \in \mathcal{B}$,

$$\begin{aligned} x \in B &\Leftrightarrow \alpha(x) \in \alpha(B) \\ &\Leftrightarrow (\beta \circ \alpha)(x) = \beta(\alpha(x)) \in \beta(\alpha(B)) = (\beta \circ \alpha(B)). \end{aligned}$$

Therefore $\beta \circ \alpha$ is an isomorphism from $(X, \mathcal{B})$ to $(Z, \mathcal{E})$, and $(X, \mathcal{B}) \simeq (Z, \mathcal{E})$.

Definition 1.5 *Let $(X, \mathcal{B})$ be a (v, k, λ)-BIBD. An isomorphism of $(X, \mathcal{B})$ to itself is called an automorphism of $(X, \mathcal{B})$. The set of automorphisms of $(X, \mathcal{B})$ forms a group with respect to the composition of maps, which is called the automorphism group of $(X, \mathcal{B})$ and is denoted by $Aut(X, \mathcal{B})$.*

The identity map on X is always an automorphism of $(X, \mathcal{B})$ and is the identity element of the group $Aut(X, \mathcal{B})$.

Example 1.13 *Consider the $(7, 3, 1)$-BIBD $(X, \mathcal{B})$ again, where*

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

$\mathcal{B} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 7\}, \{2, 5, 6\}, \{3, 4, 6\}, \{3, 5, 7\}\}$.

Let $\alpha : X \to X$ be the bijection defined by

$\alpha(1) = 1,\ \alpha(2) = 6,\ \alpha(3) = 7,\ \alpha(4) = 4,\ \alpha(5) = 5,\ \alpha(6) = 2,\ \alpha(7) = 3.$

Then the blocks of $\mathcal{B}$ are transformed as follows

$$\begin{aligned} \{1, 2, 3\} &\to \{1, 6, 7\} \\ \{1, 4, 5\} &\to \{1, 4, 5\} \\ \{1, 6, 7\} &\to \{1, 2, 3\} \\ \{2, 4, 7\} &\to \{3, 4, 6\} \\ \{2, 5, 6\} &\to \{2, 5, 6\} \\ \{3, 4, 6\} &\to \{2, 4, 7\} \\ \{3, 5, 7\} &\to \{3, 5, 7\}. \end{aligned}$$

Thus α is an automorphism of the BIBD $(X, \mathcal{B})$; moreover, it is easy to verify $\alpha^2 = 1$, where 1 is the identity map of X.

Let $\beta : X \to X$ be defined by

$\beta(1) = 3,\ \beta(2) = 5,\ \beta(3) = 7,\ \beta(4) = 4,\ \beta(5) = 6,\ \beta(6) = 2,\ \beta(7) = 1.$

Then the blocks of $\mathcal{B}$ are transformed as follows

$$\begin{aligned} \{1, 2, 3\} &\to \{3, 5, 7\} \\ \{1, 4, 5\} &\to \{3, 4, 6\} \\ \{1, 6, 7\} &\to \{1, 2, 3\} \\ \{2, 4, 7\} &\to \{1, 4, 5\} \\ \{2, 5, 6\} &\to \{2, 5, 6\} \\ \{3, 4, 6\} &\to \{2, 4, 7\} \\ \{3, 5, 7\} &\to \{1, 6, 7\}. \end{aligned}$$

Thus β is also an automorphism of the BIBD $(X, \mathcal{B})$ and $\beta^3 = 1$.

It is left as exercise (Exercise 1.6) to show that the order of $Aut(X, \mathcal{B})$ is 168.

Theorem 1.6 *Let $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ be two isomorphic BIBDs and $\alpha : X \to Y$ and $\alpha : \mathcal{B} \to \mathcal{C}$ be the isomorphism. Then the map*

$$\begin{array}{ccc} \mathrm{Aut}(X, \mathcal{B}) & \to & \mathrm{Aut}(Y, \mathcal{C}) \\ \beta & \mapsto & \alpha \circ \beta \circ \alpha^{-1} \quad \forall \beta \in \mathrm{Aut}(X, \mathcal{B}), \end{array}$$

where $\alpha \circ \beta \circ \alpha^{-1}$ is defined by composition, is an isomorphism of groups.

The proof is immediate and is left to the reader.

Definition 1.6 *Let $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ be two BIBDs. If there is a bijection $\alpha : X \to \mathcal{C}$ and a bijection $\alpha : \mathcal{B} \to Y$ such that for any $x \in X$ and $B \in \mathcal{B}$, $x \in B$ if and only if $\alpha(B) \in \alpha(x)$, then $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ are said to be anti-isomorphic and α is called an anti-isomorphic map or an anti-isomorphism. (Note that we use the same symbol α to denote both the map $X \to \mathcal{C}$ and the map $\mathcal{B} \to Y$.) An anti-isomorphism from $(X, \mathcal{B})$ to itself is called a correlation. A correlation α of $(X, \mathcal{B})$ of order 2, i.e., $\alpha^2(x) = x$ for all $x \in X$, is called a polarity.*

Clearly, if $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ are anti-isomorphic, then $|X| = |\mathcal{C}|$ and $|\mathcal{B}| = |Y|$; moreover, if both $(X, \mathcal{B})$ and $(Y, \mathcal{C})$ are nondegenerate, by Fisher's inequality $|X| \leq |\mathcal{B}|$ and $|Y| \leq |\mathcal{C}|$, therefore $|X| = |\mathcal{B}| = |Y| = |\mathcal{C}|$.

Examples of anti-isomorphisms, correlations, and polarities will be given later.

1.3 Constructions of New *BIBD*s from Old Ones

We present two simple methods of constructing new *BIBD*s from old ones. The first method is called the *sum construction*. Given two *BIBD*s on the same point set X such that the sizes of their blocks are the same, if we put their blocks together as the collection of blocks, we obtain a new *BIBD* on X. From this construction we obtain

Theorem 1.7 *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.*

Example 1.14 *As a special case of Theorem 1.7 if we take two copies of every block in a (v, k, λ)-BIBD, we obtain a $(v, k, 2\lambda)$-BIBD.*

Example 1.15 *To illustrate the application of the sum construction we consider* $(16,6,\lambda)$*-BIBDs. From Example 1.10 we know that* $(16,6,1)$*-BIBD does not exist. However, both* $(16,6,2)$*-BIBD and* $(16,6,3)$*-BIBD are known to exist, by Examples 1.3 and 1.7, respectively. By Theorem 1.7 we know that there exists* $(16,6,\lambda)$*-BIBD for any* $\lambda \geq 2$.

The second construction is called the *complementation*. Suppose $(X, \mathcal{B})$ be a (v,k,λ)-*BIBD* with both k and $v-k \geq 2$. Define

$$\mathcal{B}' = \{X \backslash B : B \in \mathcal{B}\}, \tag{1.6}$$

then $(X, \mathcal{B}')$ is again a *BIBD* as stated in the following proposition.

Theorem 1.8 *Suppose there exists a* (v,b,r,k,λ)*-BIBD with both* k *and* $v-k \geq 2$*, and* $b-2r+\lambda \neq 0$*. Then there also exists a* $(v,b,b-r,v-k,b-2r+\lambda)$*-BIBD.*

Proof. Suppose $(X, \mathcal{B})$ is a (v,b,r,k,λ)-*BIBD* with both k and $v-k \geq 2$. Let $\mathcal{B}'$ be defined by (1.6). We will show that $(X, \mathcal{B}')$ is a $(v,b,b-r,v-k,b-2r+\lambda)$-*BIBD*. Clearly, $(X, \mathcal{B}')$ has v points and b blocks, every block of $(X, \mathcal{B}')$ has $v-k$ points, and every point is contained in $b-r$ blocks of $(X, \mathcal{B}')$. It remains to show that any pair of distinct points p_i and p_j of X is contained in $b-2r+\lambda$ blocks.

Let M be the incidence matrix of $(X, \mathcal{B})$. Replacing every 1 in M by 0 and every 0 by 1, we obtain a 0-1 matrix M'. Let m_i be the i-th row of M. Then $1_b - m_i$ is the i-th row of M'. Clearly, the j-th coordinate of m_i is equal to 1 if and only if the i-th point of X appears in the j-th block of $\mathcal{B}$. Then the j-th coordinate of $1_b - m_i$ is equal to 1 if and only if the i-th point of X appears in the j-th block of $\mathcal{B}'$. Then $1_b - m_i$ and $1_b - m_j$ is the i-th and j-th rows of M', respectively. Since $(X, \mathcal{B})$ is a (v,k,λ)-*BIBD*,

$$m_i \cdot m_j = \lambda \quad \text{for } i \neq j,$$

where $\cdot$ denotes the inner product. Then

$$\begin{aligned}(1_b - m_i)\cdot(1_b - m_j) &= 1_b \cdot 1_b - 1_b \cdot m_j - m_i \cdot 1_b + m_i \cdot m_j \\ &= b - 2r + \lambda.\end{aligned}$$

This shows that the pair of points p_i and p_j is contained exactly in $b-2r+\lambda$ blocks of $(X, \mathcal{B}')$. Therefore $(X, \mathcal{B}')$ is a $(v,b,b-r,v-k,b-2r+\lambda)$-*BIBD*. ∎

Example 1.16 *The complement of a* $(7,3,1)$*-BIBD is a* $(7,4,2)$*-BIBD.*

Example 1.17 *The complement of a* $(9,3,1)$*-BIBD is a* $(9,6,5)$*-BIBD.*

In virtue of Theorem 1.8 it is sufficient to study *BIBD* with $k \leq v/2$.

1.4 Exercises

1.1 Prove that the eigenvalues of J_v are v and $(n-1)$ zeros. Let M be the incidence matrix of a (v,b,r,k,λ)-$BIBD$, then deduce that the eigenvalues of M^tM are $\lambda v+r-\lambda$ and $r-v$ (with multiplicity $v-1$) so that $\det(M^tM)=(r+\lambda(v-1))(r-\lambda)^{v-1}$.

1.2 Let $(X,\mathcal{B})$ be a (v,b,r,k,λ)-$BIBD$ and B be any block. Show that the number of blocks that meet B is at least

$$k(r-1)^2/[(k-1)(\lambda-1)+(r-1)].$$

Then show that the equality holds if and only if any block not distinct from B meets it in a constant number of points.

1.3 Let $n=k-\lambda$. Show that the following conditions on a (v,b,r,k,λ)-$BIBD$ are all equivalent: (i) $\lambda(v-1)=k(k-1)$; (ii) $k^2-\lambda v=n$; (iii) $(v-k)\lambda=(k-1)(k-\lambda)$; (iv) $\lambda\lambda'=n(n-1)$, where $\lambda'=v-2k+\lambda$.

1.4 Construct a $(16,6,3)$-$BIBD$ with the incidence matrix M in Example 1.7.

1.5 Show that up to an isomorphism there is only one $(7,3,1)$-$BIBD$, as follows. Take the elements to be $1,2,\ldots,7$ and note that without loss of generality it can be assumed that $\{1,2,4\},\{2,3,5\},\{1,5,6\}$ are blocks; then deduce that the other blocks are uniquely determined.

1.6 Show that $|Aut(X,\mathcal{B})|$=168 in Example 1.13.

1.7 Prove Theorem 1.6.

1.8 (Another proof of Fisher's inequality.) Let $\alpha_1,\alpha_2,\ldots,\alpha_v$ be the rows of the incidence matrix of a (v,b,r,k,λ)-$BIBD$. Define

$$\beta_1=\alpha_1;$$
$$\beta_i=\alpha_i-\tfrac{\lambda}{r+(i-2)\lambda}(\alpha_1+\alpha_2+\cdots+\alpha_{i-1}),\ 2\le i\le v.$$

Prove that the vectors $\beta_1,\beta_2,\ldots,\beta_v$ are mutually orthogonal, and therefore independent, vectors of dimension b, whence $v\le b$.