1

Introduction to Balanced Incomplete Block Designs

1.1 What Is Design Theory?

Combinatorial design theory concerns questions about whether it is possible to arrange elements of a finite set into subsets so that certain "balance" properties are satisfied. Types of designs that we will discuss include balanced incomplete block designs, t-designs, pairwise balanced designs, orthogonal Latin squares, and many more. Many of the fundamental questions are existence questions: Does a design of a specified type exist? Modern design theory includes many existence results as well as nonexistence results. However, there remain many open problems concerning the existence of certain types of designs.

Design theory has its roots in recreational mathematics. Many types of designs that are studied today were first considered in the context of mathematical puzzles or brain-teasers in the eighteenth and nineteenth centuries. The study of design theory as a mathematical discipline really began in the twentieth century due to applications in the design and analysis of statistical experiments. Designs have many other applications as well, such as tournament scheduling, lotteries, mathematical biology, algorithm design and analysis, networking, group testing, and cryptography.

This work will provide a mathematical treatment of the most important "classical" results in design theory. This roughly covers the period from 1940 to 1980. In addition, we cover some selected recent topics in design theory that have applications in other areas, such as bent functions and resilient functions.

Design theory makes use of tools from linear algebra, groups, rings and fields, and number theory, as well as combinatorics. The basic concepts of design theory are quite simple, but the mathematics used to study designs is varied, rich, and ingenious.

1.2 Basic Definitions and Properties

Definition 1.1. *A* design *is a pair* $(X, \mathcal{A})$ *such that the following properties are satisfied:*

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

If two blocks in a design are identical, they are said to be *repeated blocks*. This is why we refer to $\mathcal{A}$ as a *multiset* of blocks rather than a set. A design is said to be a *simple design* if it does not contain repeated blocks.

If we want to list the elements in a multiset (with their multiplicities), we will use the notation $[\,]$. If all elements of a multiset have multiplicity one, then the multiset is a set. For example, we have that $[1,2,5] = \{1,2,5\}$, but $[1,2,5,2] \neq \{1,2,5,2\} = \{1,2,5\}$. The order of the elements in a multiset is irrelevant, as with a set.

Balanced incomplete block designs are probably the most-studied type of design. The study of balanced incomplete block designs was begun in the 1930s by Fisher and Yates. Here is a definition:

Definition 1.2. *Let $v, k,$ and λ be positive integers such that $v > k \geq 2$. A* (v,k,λ)-balanced incomplete block design *(which we abbreviate to* (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, and*
3. *every pair of distinct points is contained in exactly λ blocks.*

Property 3 in the definition above is the "balance" property. A BIBD is called an *incomplete block design* because $k < v$, and hence all its blocks are *incomplete blocks*.

A BIBD may possibly contain repeated blocks if $\lambda > 1$. The use of the letter "v" to denote the number of points is an artifact of the original motivation for studying BIBDs, namely to facilitate the design of agricultural experiments. "v" was an abbreviation for "varieties", as in "varieties of wheat".

We give a few examples of BIBDs now. To save space, we write blocks in the form abc rather than $\{a,b,c\}$.

Example 1.3. A $(7,3,1)$-BIBD.

$$X = \{1,2,3,4,5,6,7\}, \quad \text{and}$$
$$\mathcal{A} = \{123, 145, 167, 246, 257, 347, 356\}.$$

This BIBD has a nice diagrammatic representation; see Figure 1.1. The blocks of the BIBD are the six lines and the circle in this diagram. ∎

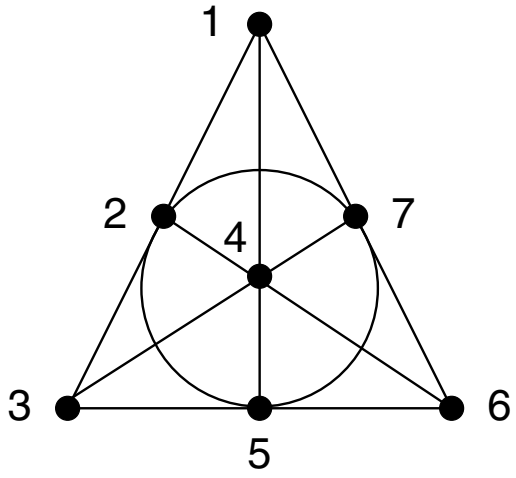

Fig. 1.1. The Fano Plane: A $(7,3,1)$-BIBD

Example 1.4. A $(9,3,1)$-BIBD.

$$X = \{1,2,3,4,5,6,7,8,9\}, \quad \text{and}$$
$$\mathcal{A} = \{123,456,789,147,258,369,159,267,348,168,249,357\}.$$

This BIBD can also be presented diagrammatically; see Figure 1.2. The 12 blocks of the BIBD are depicted as eight lines and four triangles. Observe that the blocks can be separated into four sets of three, where each of these four sets covers every point in the BIBD. ∎

Example 1.5. A $(10,4,2)$-BIBD.

$$X = \{0,1,2,3,4,5,6,7,8,9\}, \quad \text{and}$$
$$\mathcal{A} = \{0123,0145,0246,0378,0579,0689,1278,1369,1479,1568,$$
$$2359,2489,2567,3458,3467\}.$$

∎

Example 1.6. Let $\mathcal{A}$ consist of all k-subsets of X. Then $(X,\mathcal{A})$ is a $\left(v,k,\binom{v-2}{k-2}\right)$-BIBD. ∎

Example 1.7. A $(7,3,2)$-BIBD containing a repeated block.

$$X = \{0,1,2,3,4,5,6\}, \quad \text{and}$$
$$\mathcal{A} = [123,145,167,246,257,347,356,$$
$$123,147,156,245,267,346,357].$$

∎

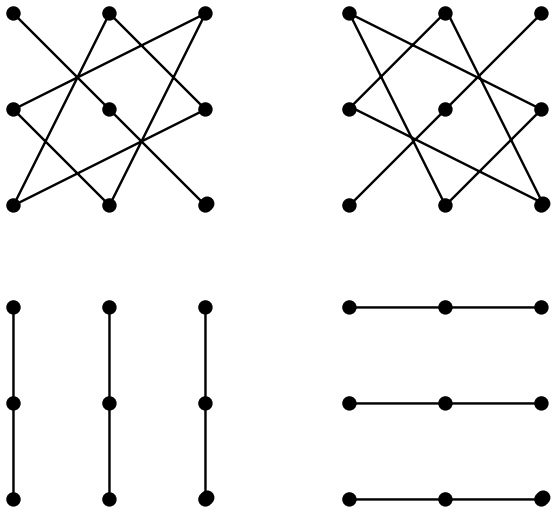

Fig. 1.2. A $(9,3,1)$-BIBD

We now state and prove two basic properties of BIBDs.

Theorem 1.8. *In a* (v,k,λ)-BIBD*, every point occurs in exactly*

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

blocks.

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

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

We will compute $|I|$ in two different ways.

First, there are $v-1$ ways to choose $y \in X$ such that $y \neq x$. For each such y, there are λ blocks A such that $\{x,y\} \subseteq A$. Hence,

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

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

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

Combining these two equations, we see that

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

Hence $r_x = \lambda(v-1)/(k-1)$ is independent of x, and the result follows. □

The value r is often called the *replication number* of the BIBD.

Theorem 1.9. *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 will compute $|I|$ in two different ways.

First, there are v ways to choose $x \in X$. For each such x, there are r blocks A such that $x \in A$. Hence,

$$|I| = vr.$$

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

$$|I| = bk.$$

Combining these two equations, we see that

$$bk = vr,$$

as desired. □

Sometimes we will use the notation (v, b, r, k, λ)-BIBD if we want to record the values of all five parameters.

Since b and r must be integers, these two theorems allow us to conclude that BIBDs with certain parameter sets do not exist. We state the following obvious corollary of Theorems 1.8 and 1.9.

Corollary 1.10. *If a* (v, k, λ)-BIBD *exists, then* $\lambda(v - 1) \equiv 0 \pmod{k - 1}$ *and* $\lambda v(v - 1) \equiv 0 \pmod{k(k - 1)}$.

For example, an $(8, 3, 1)$-BIBD does not exist because $\lambda(v - 1) = 7 \not\equiv 0 \pmod 2$. As another example, let us consider the parameter set $(19, 4, 1)$. Here, we see that $\lambda v(v - 1) = 342 \not\equiv 0 \pmod{12}$. Hence a $(19, 4, 1)$-BIBD cannot exist.

A more general use of Corollary 1.10 is to determine necessary conditions for families of BIBDs with fixed values of k and λ. For example, it is not hard to show that a $(v, 3, 1)$-BIBD exists only if $v \equiv 1, 3 \pmod 6$.

One of the main goals of combinatorial design theory is to determine necessary and sufficient conditions for the existence of a (v, k, λ)-BIBD. This is a very difficult problem in general, and there are many parameter sets where the answer is 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 BIBDs as well as some other necessary conditions that we will discuss a bit later.

1.3 Incidence Matrices

It is often convenient to represent a BIBD by means of an incidence matrix. This is especially useful for computer programs. We give the definition of an incidence matrix now.

Definition 1.11. *Let $(X, \mathcal{A})$ be a design where $X = \{x_1, \ldots, x_v\}$ and $\mathcal{A} = \{A_1, \ldots, A_b\}$. The* incidence matrix *of $(X, \mathcal{A})$ is the $v \times b$ $0-1$ matrix $M = (m_{i,j})$ defined by the rule*

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

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

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

Example 1.12. Consider the $(9, 3, 1)$-BIBD presented in Example 1.4. The incidence matrix of this design is the following 9×12 matrix:

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

∎

We need a few more definitions before stating the next theorem. Suppose I_n denotes an $n \times n$ identity matrix, J_n denotes the $n \times n$ matrix in which every entry is a "1", and $\mathbf{u}_n$ denotes the vector of length n in which every coordinate is a "1". Finally, for a matrix $M = (m_{i,j})$, define the *transpose* of M, denoted M^T, to be the matrix whose (j, i) entry is $m_{i,j}$.

Theorem 1.13. *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. First, suppose $(X, \mathcal{A})$ is a (v, k, λ)-BIBD, where $X = \{x_1, \ldots, x_v\}$ and $\mathcal{A} = \{A_1, \ldots, A_b\}$. Let M be its incidence matrix. The (i, j)-entry of MM^T is

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

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

Furthermore, the ith entry of $\mathbf{u}_v M$ is equal to the number of "1"s in column i of M. By property 1, this equals 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 the design whose incidence matrix is M. Clearly we have $|X| = v$ and $|\mathcal{A}| = b$. From the equation $\mathbf{u}_v M = k\mathbf{u}_b$, it follows that every block in $\mathcal{A}$ contains k points. From the equation $MM^T = \lambda J_v + (r - \lambda)I_v$, it follows that every pair of points occurs in exactly λ blocks, and every point occurs in r blocks. Hence, $(X, \mathcal{A})$ is a (v, b, r, k, λ)-BIBD. □

We will show that the converse part of the theorem above does not hold if the second condition is omitted. Incidence matrices satisfying the first condition are equivalent to a certain type of design, which we define now.

Definition 1.14. *A* pairwise balanced design *(or* PBD*) is a design $(X, \mathcal{A})$ such that every pair of distinct points is contained in exactly λ blocks, where λ is a positive integer. Furthermore, $(X, \mathcal{A})$ is a* regular pairwise balanced design *if every point $x \in X$ occurs in exactly r blocks $A \in \mathcal{A}$, where r is a positive integer.*

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

We state the following variation of Theorem 1.13 without proof.

Theorem 1.15. *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 $MM^T = \lambda J_v + (r - \lambda)I_v$.*

Here is an example to illustrate Theorem 1.15.

Example 1.16. Consider the following 6×11 matrix:

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

This matrix M is the incidence matrix of the following regular pairwise balanced design:

$$X = \{1,2,3,4,5,6\}, \quad \text{and}$$
$$\mathcal{A} = \{123, 456, 14, 15, 16, 24, 25, 26, 34, 35, 36\}.$$

Here $v = 6$, $b = 11$, $r = 4$, and $\lambda = 1$. The design is not a BIBD because the blocks do not all have the same size—there are two blocks of size three and nine blocks of size two.

It is easily verified that $MM^T = J_v + 3I_v = \lambda J_v + (r - \lambda)I_v$. However,

$$\mathbf{u}_6 M = (3,3,2,2,2,2,2,2,2,2,2),$$

so $\mathbf{u}_6 M \neq k\mathbf{u}_b$ for any integer k. ∎

Suppose that $(X, \mathcal{A})$ is a design with $|X| = v$ and $|\mathcal{A}| = b$. Let M be the $v \times b$ incidence matrix of $(X, \mathcal{A})$. The design having incidence matrix M^T is called the *dual design* of $(X, \mathcal{A})$. Suppose that $(Y, \mathcal{B})$ is the dual design of $(X, \mathcal{A})$; then $|Y| = |\mathcal{A}| = b$ and $|\mathcal{B}| = |X| = v$. Properties of dual designs of BIBDs are summarized in the following theorem.

Theorem 1.17. *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 in $\mathcal{B}$, and*
3. *any two distinct blocks $B_i, B_j \in \mathcal{B}$ intersect in exactly λ points.*

Example 1.18. Suppose that $(X, \mathcal{A})$ is the $(9,3,1)$-BIBD presented in Example 1.4. Then $(Y, \mathcal{B})$ is the dual design of $(X, \mathcal{A})$, where

$$Y = \{1,2,3,4,5,6,7,8,9,T,E,V\}, \quad \text{and}$$
$$\mathcal{B} = \{147T, 158E, 169V, 248E, 257V, 268T, 348V, 359T, 367E\}.$$

It is easy to verify that every block in $\mathcal{B}$ has size four, every point in Y occurs in exactly three blocks in $\mathcal{B}$, and every pair of distinct blocks in $\mathcal{B}$ intersect in exactly one point. ∎

1.4 Isomorphisms and Automorphisms

We begin with a definition.

Definition 1.19. *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 exists a bijection $\alpha : X \to Y$ such that*

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

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

Example 1.20. Here are two $(7,3,1)$-BIBDs, $(X,\mathcal{A})$ and $(Y,\mathcal{B})$:

$$X = \{1,2,3,4,5,6,7\}, \quad \text{and}$$
$$\mathcal{A} = \{123, 145, 167, 246, 257, 347, 356\};$$

$$Y = \{a,b,c,d,e,f,g\}, \quad \text{and}$$
$$\mathcal{B} = \{abd, bce, cdf, deg, aef, bfg, acg\}.$$

Suppose we define the bijection α as $\alpha(1) = a$, $\alpha(2) = b$, $\alpha(3) = d$, $\alpha(4) = c$, $\alpha(5) = g$, $\alpha(6) = e$ and $\alpha(7) = f$. Then, when we relabel the points in X using α, the blocks of $\mathcal{A}$ become the following:

$$123 \to abd$$
$$145 \to acg$$
$$167 \to aef$$
$$246 \to bce$$
$$257 \to bfg$$
$$347 \to cdf$$
$$356 \to deg.$$

Thus α is an isomorphism of the two BIBDs. ∎

We need to clarify how isomorphisms affect BIBDs having repeated blocks. Suppose that $(X,\mathcal{A})$ and $(Y,\mathcal{B})$ are two (v,k,λ)-BIBDs, and suppose that $\alpha : X \to Y$ is an isomorphism of these two designs. Suppose further that $(X,\mathcal{A})$ contains c copies of the block A. Then it must also be the case that $(Y,\mathcal{B})$ contains c copies of the block $\{\alpha(x) : x \in A\}$.

We can describe isomorphism of designs in terms of incidence matrices as follows.

Theorem 1.21. *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 exists a permutation γ of $\{1,\ldots,v\}$ and a permutation β of $\{1,\ldots,b\}$ such that*

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

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

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

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

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

Since α is a bijection of X and Y, it follows that γ is a permutation of $\{1, \ldots, v\}$.

Next, there exists a permutation β of $\{1, \ldots, b\}$ that has the property that

$$\{\alpha(x) : x \in A_j\} = B_{\beta(j)}$$

for $1 \leq j \leq b$. Such a permutation exists because α is an isomorphism of $(X, \mathcal{A})$ and $(Y, \mathcal{B})$.

Now, we have

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

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

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

Then it is easily seen that

$$\{\alpha(x) : x \in A_j\} = B_{\beta(j)}$$

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

A *permutation matrix* is a $0 - 1$ matrix in which every row and every column contain exactly one entry equal to "1". The following corollary of Theorem 1.21 provides an alternate characterization of isomorphic designs. The proof is left to the reader.

Corollary 1.22. *Suppose M and N are incidence matrices of two (v, b, r, k, λ)-*BIBD*s. 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 $M = PNQ$.*

In general, determining whether or not two designs are isomorphic is a difficult computational problem. There are $v!$ possible bijections between two sets of cardinality v. To show that two designs are not isomorphic, it must be shown that none of the $v!$ possible bijections constitutes an isomorphism. Since $v!$ grows exponentially quickly as a function of v, it soon becomes impractical to actually test every possible bijection. Fortunately, there are more sophisticated algorithms than testing every possibility exhaustively, and isomorphism testing is practical for relatively large designs.

Suppose $(X, \mathcal{A})$ is a design. An *automorphism* of $(X, \mathcal{A})$ is an isomorphism of this design with itself. In this case, the bijection α is a *permutation* of X such that

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

Of course, the identity mapping on X is always a (trivial) automorphism, but a design may have other, nontrivial automorphisms.

Example 1.23. Let $(X, \mathcal{A})$ be the following $(7, 3, 1)$-BIBD:

$$X = \{1, 2, 3, 4, 5, 6, 7\}, \quad \text{and}$$
$$\mathcal{A} = \{123, 145, 167, 246, 257, 347, 356\}.$$

Suppose we define the permutation α as follows: $\alpha(1) = 1$, $\alpha(2) = 2$, $\alpha(3) = 3$, $\alpha(4) = 5$, $\alpha(5) = 4$, $\alpha(6) = 7$, and $\alpha(7) = 6$. Then, when we relabel the points in X using α, the blocks of $\mathcal{A}$ become the following:

$$123 \to 123$$
$$145 \to 145$$
$$167 \to 167$$
$$246 \to 257$$
$$257 \to 246$$
$$347 \to 356$$
$$356 \to 347.$$

Thus α is an automorphism of the BIBD. ∎

It is often convenient to present a permutation α on a set X using the *disjoint cycle representation*. Each cycle in this representation has the form

$$(x \ \alpha(x) \ \alpha(\alpha(x)) \ \cdots)$$

for some $x \in X$. Eventually, we get back to x, creating a cycle. The cycles thus obtained are disjoint, and they have lengths that sum to $|X|$. The *order* of the permutation α is the least common multiple of the lengths of the cycles in the disjoint cycle representation. A *fixed point* of α is a point x such that $\alpha(x) = x$; note that fixed points of α correspond to cycles of length one in the disjoint cycle representation of α.

The permutation α in the example above has the disjoint cycle representation $(1)(2)(3)(4\ 5)(6\ 7)$. It is a permutation of order 2 that contains three fixed points.

It is easy to show that 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 $\mathsf{Aut}(X, \mathcal{A})$. $\mathsf{Aut}(X, \mathcal{A})$ is a subgroup of the *symmetric group* $S_{|X|}$ (where S_v is the group consisting of all $v!$ permutations on a set of v elements). Note that a subgroup of S_v is called a *permutation group*, so automorphism groups of designs are examples of permutation groups.

Example 1.24. The $(7, 3, 1)$-BIBD $(X, \mathcal{A})$ in the previous example has another automorphism, $\beta = (1\ 2\ 4\ 3\ 6\ 7\ 5)$. The composition $\gamma = \alpha \circ \beta$ is defined as $\gamma(x) = \beta(\alpha(x))$ for all $x \in X$. It can be checked that $\gamma = (1\ 2\ 4)(3\ 6\ 5)(7)$. Thus γ is an automorphism of the BIBD because it is the composition of two automorphisms.

$(X, \mathcal{A})$ has many other automorphisms. In fact, it turns out that $\mathsf{Aut}(X, \mathcal{A})$ is a group of order 168. ∎

1.4.1 Constructing BIBDs with Specified Automorphisms

In this section, we describe a method that can often be used to determine the existence or nonexistence of a (v, k, λ)-BIBD having specified automorphisms.

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

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

Suppose that G is a subgroup of S_v. Let $j \leq v$ be a positive integer, and for $A, B \in \binom{X}{j}$, define $A \sim_j B$ if $\beta(A) = B$ for some $\beta \in G$. It is not hard to prove that $\sim_j$ is an equivalence relation on $\binom{X}{j}$. The equivalence classes of this relation are called the *j-orbits* of X with respect to the group G. The j-orbits comprise a partition of the set $\binom{X}{j}$, and $\beta(A) = B$ for some $\beta \in G$ if and only if A and B are in the same *orbit* of G.

The well-known Cauchy-Frobenius-Burnside Lemma provides a method of computing the number of j-orbits of X. For each $\beta \in G$, define

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

We state the following lemma without proof.

Lemma 1.25 (Cauchy-Frobenius-Burnside Lemma). *The number of j-orbits of X with respect to the group G is exactly*

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

Suppose that $\mathcal{O}_1, \ldots, \mathcal{O}_n$ are the k-orbits, and $\mathcal{P}_1, \ldots, \mathcal{P}_m$ are the 2-orbits of X with respect to the group G. We define an $n \times m$ matrix, denoted $A_{k,2}$, as follows. For $1 \leq j \leq m$, choose any 2-subset $Y_j \in \mathcal{P}_j$. Then, for $1 \leq i \leq n$, the i, j entry of $A_{k,2}$, denoted $a_{i,j}$, is defined as follows:

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

It can be shown that the definition of $a_{i,j}$ does not depend on the particular *orbit representatives* Y_j that are chosen; this follows immediately from the next lemma.

Lemma 1.26. *Suppose that $\mathcal{O}_1, \ldots, \mathcal{O}_n$ are the k-orbits, and $\mathcal{P}_1, \ldots, \mathcal{P}_m$ are 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. There exists $\beta \in G$ such that $\beta(Y) = Y'$. For each $A \in \mathcal{O}_i$ such that $Y \subseteq A$, it holds that $Y' \subseteq \beta(A)$. β is a permutation, so $\beta(A) \neq \beta(B)$ if $A \neq B$. Therefore, for each $A \in \mathcal{O}_i$ such that $Y \subseteq A$, we obtain a block $A' = \beta(A) \in \mathcal{O}_i$ such that $Y' \subseteq A'$, and the blocks $\beta(A)$, where $A \in \mathcal{O}_i$ and $Y \subseteq A$, are all distinct. Therefore

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

The inequality in the opposite direction follows by interchanging the roles of Y and Y', and replacing β by β^{-1}. Combining the two inequalities, the desired result is proven. □

Here now is the main result of this section.

Theorem 1.27 (Kramer-Mesner Theorem). *There exists a (v, k, λ)-*BIBD *having G as a subgroup of its automorphism group if and only if there exists a solution $\mathbf{z} \in \mathbb{Z}^n$ to the matrix equation*

$$\mathbf{z}A_{k,2} = \lambda \mathbf{u}_m, \tag{1.1}$$

where $\mathbf{z}$ has nonnegative entries.

Proof. We give a sketch of the proof. First, suppose that $\mathbf{z} = (z_1, \ldots, z_n)$ is a nonnegative integral solution to equation (1.1). Define

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

The notation above is a multiset union; it means that $\mathcal{A}$ is formed by taking z_i copies of every block in $\mathcal{O}_i$ for $1 \leq i \leq n$. It is easy to see that $(X, \mathcal{A})$ 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 $\mathcal{A}$ necessarily 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 $\mathbf{z} = (z_1, \ldots, z_n)$ is a nonnegative integral solution to equation (1.1). □

As an additional remark, we observe that the BIBD in Theorem 1.27 is simple if and only if the vector $\mathbf{z} \in \{0, 1\}^n$.

Example 1.28. We use the technique described above to construct a $(6, 3, 2)$-BIBD having an automorphism of order 5. Suppose that $\alpha = (0\ 1\ 2\ 3\ 4)(5)$ and $G = \{\alpha^i : 0 \leq i \leq 4\}$. It is easy to see that there are three 2-orbits of $X = \{0, 1, 2, 3, 4, 5\}$, namely

$$\begin{aligned} \mathcal{P}_1 &= \{01, 12, 23, 34, 40\}, \\ \mathcal{P}_2 &= \{02, 13, 24, 30, 41\}, \quad \text{and} \\ \mathcal{P}_3 &= \{05, 15, 25, 35, 45\}. \end{aligned}$$

Also, there are four 3-orbits:

$$\begin{aligned}\mathcal{O}_1 &= \{012, 123, 234, 340, 401\},\\ \mathcal{O}_2 &= \{013, 124, 230, 341, 402\},\\ \mathcal{O}_3 &= \{015, 125, 235, 345, 405\}, \quad \text{and}\\ \mathcal{O}_4 &= \{025, 135, 245, 305, 415\}.\end{aligned}$$

The matrix $A_{3,2}$ is as follows:

$$A_{3,2} = \begin{pmatrix} 2\,1\,0 \\ 1\,2\,0 \\ 1\,0\,2 \\ 0\,1\,2 \end{pmatrix}.$$

The equation $\mathbf{z}A_{3,2} = 2\mathbf{u}_3$ has exactly two nonnegative integral solutions: $\mathbf{z} = (1,0,0,1)$ and $\mathbf{z} = (0,1,1,0)$. Each of these solutions yields a $(6,3,2)$-BIBD having α as an automorphism. ∎

Here is a more interesting example, in which the orbits do not all have the same size.

Example 1.29. We construct a $(9,3,1)$-BIBD having a certain automorphism of order six. Suppose that $\alpha = (0\,1\,2\,3\,4\,5)(6\,7\,8)$ and $G = \{\alpha^i : 0 \le i \le 5\}$. The permutations in G are as follows:

$$\begin{aligned}\alpha &= (0\,1\,2\,3\,4\,5)(6\,7\,8),\\ \alpha^2 &= (0\,2\,4)(1\,3\,5)(6\,8\,7),\\ \alpha^3 &= (0\,3)(1\,4)(2\,5)(6)(7)(8),\\ \alpha^4 &= (0\,4\,2)(1\,5\,3)(6\,7\,8),\\ \alpha^5 &= (0\,5\,4\,3\,2\,1)(6\,8\,7), \quad \text{and}\\ \alpha^0 &= (0)(1)(2)(3)(4)(5)(6)(7)(8).\end{aligned}$$

Lemma 1.25 can be used to compute the number of 2- and 3-orbits. First we consider 2-orbits. It is not hard to see that $\mathsf{fix}(\alpha) = \mathsf{fix}(\alpha^2) = \mathsf{fix}(\alpha^4) = \mathsf{fix}(\alpha^5) = 0$, $\mathsf{fix}(\alpha^3) = 6$, and $\mathsf{fix}(\alpha^0) = \binom{9}{2} = 36$. Therefore, the number of 2-orbits is $(36+6)/6 = 7$.

Now we turn to 3-orbits. It is not hard to check that $\mathsf{fix}(\alpha) = \mathsf{fix}(\alpha^5) = 1$, $\mathsf{fix}(\alpha^2) = \mathsf{fix}(\alpha^4) = 3$, $\mathsf{fix}(\alpha^3) = 10$, and $\mathsf{fix}(\alpha^0) = \binom{9}{3} = 84$. Therefore, the number of 3-orbits is $(84 + 10 + 2(3) + 2(1))/6 = 17$.

We leave it as an exercise for the reader to construct the $A_{3,2}$ matrix and solve the matrix equation. It turns out that there is a solution; the following $(9,3,1)$-BIBD, consisting of four of the 3-orbits, has α as an automorphism:

orbit	orbit size
018 126 237 348 456 507	6
036 147 258	3
024 135	2
678	1

The total number of blocks is 12, as it must be. ∎

It is, in general, a nontrivial task to construct an $A_{k,2}$ matrix if the set X is even of moderate size. It is a considerably more difficult problem to find the desired integral solution to the matrix equation (and of course there is no guarantee that the sought-after solution even exists). The known algorithms to find nonnegative integral solutions of matrix equations have exponential complexity and may require enormous amounts of computing time to run to completion. Nevertheless, this approach to finding designs having specified automorphisms has been very useful in practice in discovering previously unknown designs.

1.5 New BIBDs from Old

In this section, we give two simple methods of constructing new BIBDs from old. The first construction can be called the "sum construction". Given two BIBDs on the same point set, it involves forming the collection of all the blocks in both designs.

Theorem 1.30 (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 1.31. *Suppose there exists a* (v, k, λ)-BIBD. *Then there exists a* $(v, k, s\lambda)$-BIBD *for all integers* $s \geq 1$.

Note that the BIBDs produced by Corollary 1.31 with $s \geq 2$ are not simple designs, even if the initial (v, k, λ)-BIBD is simple. For $\lambda > 1$, construction of simple BIBDs is, in general, more difficult than construction of BIBDs with repeated blocks.

To illustrate an application of the sum construction, let us consider $(16, 6, \lambda)$-BIBDs. We will see in the next section that there does not exist a $(16, 6, 1)$-BIBD. However, both a $(16, 6, 2)$-BIBD and a $(16, 6, 3)$-BIBD are known to exist. By application of the sum construction, it then follows that there exists a $(16, 6, \lambda)$-BIBD if and only if $\lambda > 1$.

The second construction is called "block complementation". Suppose $(X, \mathcal{A})$ is a BIBD, and we replace every block $A \in \mathcal{A}$ by $X \backslash A$. The result is again a BIBD, as stated in the following theorem.

Theorem 1.32 (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. We will show that

$$(X, \{X \backslash A : A \in \mathcal{A}\})$$

is a BIBD. Clearly, this design has v points and b blocks, every block contains $v - k \geq 2$ points, and every point occurs in $b - r$ blocks. Hence, we just need to show that every pair of points occurs in exactly $b - 2r + \lambda$ blocks.

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

$$\begin{aligned} a_1 &= |\{A \in \mathcal{A} : x, y \in A\}|, \\ a_2 &= |\{A \in \mathcal{A} : x \in A, y \notin A\}|, \\ a_3 &= |\{A \in \mathcal{A} : x \notin A, y \in A\}|, \quad \text{and} \\ a_4 &= |\{A \in \mathcal{A} : x, y \notin A\}|. \end{aligned}$$

Then it is easy to see that

$$\begin{aligned} a_1 &= \lambda, \\ a_1 + a_2 &= r, \\ a_1 + a_3 &= r, \quad \text{and} \\ a_1 + a_2 + a_3 + a_4 &= b. \end{aligned}$$

These four equations may be solved easily to obtain

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

as desired. □

For example, the complement of a $(7, 3, 1)$-BIBD is a $(7, 4, 2)$-BIBD, and the complement of a $(9, 3, 1)$-BIBD is a $(9, 6, 5)$-BIBD. In view of Theorem 1.32, it suffices to study BIBDs with $k \leq v/2$.

1.6 Fisher's Inequality

We have already discussed two necessary conditions for the existence of a (v, k, λ)-BIBD, namely Theorems 1.8 and 1.9. Another important necessary condition is known as "Fisher's Inequality".

Theorem 1.33 (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 $X = \{x_1, \ldots, x_v\}$ and $\mathcal{A} = \{A_1, \ldots, A_b\}$. Let M be the incidence matrix of this BIBD, and define $\mathbf{s}_j$ to be the jth row of M^T (equivalently, ${\mathbf{s}_j}^T$ is the jth column of M). Note that $\mathbf{s}_1, \ldots, \mathbf{s}_b$ are all v-dimensional vectors in the real vector space $\mathbb{R}^v$.

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

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

In other words, $\mathbf{S}$ consists of all linear combinations of the vectors $\mathbf{s}_1, \ldots, \mathbf{s}_b$.

We will prove that $\mathbf{S} = \mathbb{R}^v$; i.e., the b vectors in 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 the case that $b \geq v$.

Our task is thus to show that $\mathbf{S} = \mathbb{R}^v$. For $1 \leq i \leq v$, define $\mathbf{e}_i \in \mathbb{R}^v$ to be the vector with a "1" in the ith coordinate and "0"s in all other coordinates. The vectors $\mathbf{e}_1, \ldots, \mathbf{e}_v$ form a basis for $\mathbb{R}^v$, so every vector in $\mathbb{R}^v$ can be expressed as a linear combination of these v vectors. Therefore, to show that $\mathbf{S} = \mathbb{R}^v$, it suffices to show that $\mathbf{e}_i \in \mathbf{S}$ for $1 \leq i \leq v$ (i.e., that each basis vector $\mathbf{e}_i$ can be expressed as a linear combination of vectors in S).

First, we observe that

$$\sum_{j=1}^{b} \mathbf{s}_j = (r, \ldots, r), \tag{1.2}$$

from which it follows that

$$\sum_{j=1}^{b} \frac{1}{r} \mathbf{s}_j = (1, \ldots, 1). \tag{1.3}$$

Next, fix a value i, $1 \leq i \leq v$. Then we have

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

Since $\lambda(v-1) = r(k-1)$ and $v > k$, it follows that $r > \lambda$, and hence $r - \lambda \neq 0$. Then we can combine equations (1.3) and (1.4) to obtain

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

Equation (1.5) gives a formula expressing $\mathbf{e}_i$ as a linear combination of $\mathbf{s}_1, \ldots, \mathbf{s}_b$, as desired. □

Note that the conclusion of Theorem 1.33, $b \geq v$, can be stated in other, equivalent ways, such as $r \geq k$ and $\lambda(v-1) \geq k^2 - k$.

As an example, consider the parameter set $(16, 6, 1)$. In a $(16, 6, 1)$-BIBD, we would have $r = 3$, but it would then be the case that $r < k$, which is impossible. Hence, a $(16, 6, 1)$-BIBD does not exist.

Theorem 1.33 can easily be generalized to regular pairwise balanced designs. We have the following.

Theorem 1.34. *In any nontrivial regular pairwise balanced design, $b \geq v$.*

Proof. By examining the proof of Theorem 1.33, it can be seen that the fact that all blocks have the same size is not used in the proof. Therefore, Fisher's Inequality holds for regular pairwise balanced designs in which $r > \lambda$. It

is easy to see that a regular PBD has $r > \lambda$ if and only if it is not a trivial PBD. Therefore we conclude that Fisher's Inequality is valid for all nontrivial regular PBDs. □

In fact, Fisher's Inequality holds for all nontrivial pairwise balanced designs (not just the regular ones), but a slightly different proof is required. We will return to this topic in Chapter 8.

1.7 Notes and References

Fisher's Inequality was first proven in 1940 by the famous statistician Ronald Fisher [45]. There are many proofs of this result; we have chosen to employ a linear-algebraic proof technique that will be used to prove several other results later in this book.

The Kramer-Mesner Theorem was proven in 1975 in [71]. It has since been used to find many previously unknown designs. For a nice survey of computational techniques in design theory, see Gibbons [47].

There are several reference books and textbooks on combinatorial design theory. The book "Combinatorial Designs" by Wallis [115] is a fairly easy-to-read general introduction. Two other good introductory textbooks are "Combinatorial Designs and Tournaments" by Anderson [2] and "Design Theory" by Lindner and Rodger [77]. A more advanced book that contains a great deal of useful information is the two-volume work also entitled "Design Theory" by Beth, Jungnickel, and Lenz [9, 10]. The reader can also profitably consult "Design Theory" by Hughes and Piper [61] and "Combinatorics of Experimental Design" [107] by Street and Street (however, these two books are currently out of print).

The "CRC Handbook of Combinatorial Designs", edited by Colbourn and Dinitz [27], is an enormous, encyclopedic reference work that is a valuable resource for researchers. This book also has an on-line Web page located at the following URL: `http://www.emba.uvm.edu/~dinitz/hcd.html`. "Contemporary Design Theory, A Collection of Surveys", edited by Dinitz and Stinson [41], is a collection of twelve surveys on various topics in design theory.

Two books that explore the links between combinatorial design theory and other branches of combinatorial mathematics are "Designs, Codes, Graphs and Their Links" by Cameron and van Lint [20] and "Combinatorial Configurations: Designs, Codes, Graphs" by Tonchev [110].

Several "general" combinatorics textbooks contain one or more sections on designs. Three books that are worth consulting are "Combinatorics: Topics, Techniques, Algorithms", by Cameron [19]; "Combinatorial Theory (Second Edition)", by Hall [53]; and "A Course in Combinatorics (Second Edition)", by Van Lint and Wilson [79].

Much recent research on combinatorial designs can be found in the *Journal of Combinatorial Designs*, which has been published by John Wiley & Sons since 1993.

1.8 Exercises

1.1 What is the value of b in a $(46, 6, 1)$-BIBD (if it exists)?

1.2 What is the value of r in a $(65, 5, 1)$-BIBD?

1.3 For all integers k and v such that $3 \leq k \leq v/2$ and $v \leq 10$, determine the smallest integer λ such that the parameter set (v, k, λ) satisfies the necessary conditions stated in Corollary 1.10.

1.4 For an integer $k \geq 2$, let $\lambda^*(k)$ denote the minimum integer such that the conditions stated in Corollary 1.10 are satisfied for all integers $v > k$.

(a) Compute $\lambda^*(k)$ for $k = 3, 4, 5$ and 6.

(b) Prove that

$$\lambda^*(k) = \begin{cases} \binom{k}{2} & \text{if } k \text{ is even} \\ k(k-1) & \text{if } k \text{ is odd.} \end{cases}$$

1.5 Let M be the incidence matrix of a $(v, b, r, k, 1)$-BIBD and define $N = M^T M$. Denote $N = (n_{i,j})$. Prove that

$$n_{i,j} = \begin{cases} k & \text{if } i = j \\ 0 \text{ or } 1 & \text{if } i \neq j. \end{cases}$$

1.6 Construct a regular pairwise balanced design on six points that contains exactly four blocks of size three.

1.7 Give a complete proof of Theorem 1.15.

1.8 Give a complete proof of Theorem 1.17.

1.9 (a) Prove that no $(6, 3, 2)$-BIBD can contain repeated blocks.

(b) Prove that all $(6, 3, 2)$-BIBDs are isomorphic.

1.10 Give a complete proof of Corollary 1.22.

1.11 Show that all $(7, 3, 1)$-BIBDs are isomorphic by the following method. (Fill in the details of the proof.)

(a) Without loss of generality, we can take the points to be $\{1, \ldots, 7\}$, and let the blocks containing the point 1 be $\{1, 2, 3\}$, $\{1, 4, 5\}$, and $\{1, 6, 7\}$.

(b) Find all ways to complete this structure to a $(7, 3, 1)$-BIBD.

(c) Then show that all the designs obtained are isomorphic.

1.12 Find an isomorphism π of the two $(9, 3, 1)$-BIBDs $(X, \mathcal{A})$ and $(Y, \mathcal{B})$, and give a complete verification that the two BIBDs are isomorphic.

$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$
$$\mathcal{A} = \{123, 147, 159, 168, 258, 267, 249, 369, 348, 357, 456, 789\}$$
$$Y = \{a, b, c, d, e, f, g, h, i\}$$
$$\mathcal{B} = \{abe, acd, afi, agh, bcf, bdg, bhi, ceh, cgi, dfh, dei, efg\}.$$

Hint: Observe that if $\pi(x) = \alpha$, $\pi(y) = \beta$, $\{x, y, z\} \in \mathcal{A}$, and $\{\alpha, \beta, \gamma\} \in \mathcal{B}$, then it must be the case that $\pi(z) = \gamma$.

1.13 Suppose we arrange the elements of a set $X = \{0, \ldots, 15\}$ in a 4×4 array A as follows:

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \\ 12 & 13 & 14 & 15 \end{pmatrix}.$$

For each x, $0 \leq x \leq 15$, suppose we define a block B_x consisting of the elements in the same row or column of A as x, excluding x. Then define a set of blocks $\mathcal{B} = \{B_x : 0 \leq x \leq 15\}$. We are going to study the design $(X, \mathcal{B})$.

(a) Prove that this design is a $(16, 6, 2)$-BIBD.
(b) Construct the incidence matrix of this BIBD.
(c) Prove that the mapping $\alpha(x) = (x + 4) \bmod 16$ is an automorphism of this BIBD.
(d) Prove that this BIBD has automorphisms of orders 2, 3, and 4.

1.14 Suppose that α is an automorphism of order p of a $(v, k, 1)$-BIBD, where p is prime. Let α_f denote the number of fixed points in α.

(a) Prove that $\alpha_f \equiv v \pmod{p}$.
(b) Suppose that $2 \leq \alpha_f \leq k - 1$. Prove that $k \geq p + 2$.
(c) As a corollary, prove that a $(7, 3, 1)$-BIBD cannot have an automorphism of order 5.

1.15 Let G be the permutation group of order 3 on the set $X = \{1, \ldots, 7\}$ that is generated by the permutation $\alpha = (1\ 2\ 3)(4\ 5\ 6)(7)$.

(a) Use Lemma 1.25 to compute the number of 2- and 3-orbits of X with respect to G.
(b) Use Theorem 1.27 to find all $(7, 3, 1)$-BIBDs having α as an autormorphism.

1.16 Referring to Example 1.29, carry out the following computations.

(a) Construct all the 2-orbits and 3-orbits.
(b) Construct the $A_{3,2}$ matrix.
(c) Find all solutions to the matrix equation $\mathbf{z}A_{3,2} = \mathbf{u}_7$.

1.17 Construct $(9, 3, 1)$-BIBDs having the following permutations as automorphisms.

(a) $(1)(2\ 3\ 4\ 5\ 6\ 7\ 8\ 9)$.
(b) $(1)(2)(3)(4\ 5\ 6)(7\ 8\ 9)$.
(c) $(1)(2)(3)(4\ 5)(6\ 7)(8\ 9)$.

1.18 (a) Construct a $(7, 4, 2)$-BIBD.
(b) Determine the incidence matrix of this BIBD.
(c) For the incidence matrix that you have computed, express the vector $\mathbf{e}_3$ as a linear combination of the vectors $\mathbf{s}_1, \ldots, \mathbf{s}_7$ using (1.5). Then verify that the resulting linear combination indeed yields the vector $\mathbf{e}_3$.

1.19 Let B_0 be a block in a $(v,k,1)$-BIBD, say $(X,\mathcal{B})$.
   (a) Find a formula for the number of blocks $B \in \mathcal{B}$ such that $|B \cap B_0| = 1$.
   (b) Use your formula to show that $b \geq k(r-1)+1$ if a $(v,k,1)$-BIBD exists.
   (c) Using the facts that $vr = bk$ and $v = r(k-1)+1$, deduce that $(r-k)(r-1)(k-1) \geq 1$, and hence $r \geq k$, which implies Fisher's Inequality.

1.20 Let B_0 be a block in a $(v,k,1)$-BIBD, say $(X,\mathcal{B})$. Let $x \in X \backslash B_0$, and show that there are at least k blocks that contain x and intersect B_0. From this, deduce that $r \geq k$, which implies Fisher's Inequality.

http://www.springer.com/978-0-387-95487-5

Combinatorial Designs
Constructions and Analysis
Stinson, D.
2004, XVI, 300 p., Hardcover
ISBN: 978-0-387-95487-5