Balanced Incomplete Block Designs and Other Combinatorial Objects

Ian T.W. Neill

1 Introduction to Balanced Incomplete Block Designs

Suppose we have a committee composed of a large number of members, and from this committee we wish to create a number of smaller subcommittees, each containing exactly the same number of members. Furthermore, in order to preserve equality and keep all committee members happy, each member must sit on exactly the same number of subcommittees and each pair of members must also sit on the same number of subcommittees. Is it possible to create such a family of subcommittees?

The structure of such a system of subcommittees can be described mathematically by a *balanced block design*, and the existence of a suitable design depends on the desired value of each of the parameters.

Definition A Balanced Incomplete Block Design (BIBD) may be defined as a pair $(V, \mathcal{B})$ where V is a $v \geq 2$ element set and $\mathcal{B}$ is a family of $b > 0$ subsets of V, called *blocks*, such that each block is of order $k < v$, each element of V is contained in exactly $r > 0$ blocks, and each *pair* of elements in V is contained in exactly $\lambda > 0$ blocks. The values $\{v, b, k, r, \lambda\}$ are called the parameters of the design.

In the case that $k = v$, the design is referred to as the *complete* block design and the parameters will have values $v = k, b = r = \lambda = 1$. This particular design is of no interest in the study of block designs and will be hereafter omitted from consideration. For any design over v elements where $k = 2$ there is only one possible BIBD. The blocks of this design are all the possible combinations of the v elements in pairs and $b = \binom{v}{2}$, $r = v - 1$, and $\lambda = 1$.

Definition A BIBD $(X, \mathcal{D})$ is a *subdesign* of the BIBD $(V, \mathcal{B})$ if $X \subseteq V$ and $\mathcal{D} \subseteq \mathcal{B}$. The BIBD is a *proper subdesign* if $X \subset V$ and $\mathcal{D} \subset \mathcal{B}$.

In order to determine whether or not a design exists, there are a number of necessary relationships we may rely on.

Theorem 1.1 For a $\{v, b, k, r, \lambda\}$ design we have the two following necessary relationships:

$$bk = vr, \tag{1}$$

$$\lambda(v - 1) = r(k - 1) \tag{2}$$

A parameter set which satisfies these equations is *admissable*.

Proof [**?**] To prove equation (1), we simply perform a count of the number of positions available over the total number of blocks. This number is easily attained by multiplying the total number of blocks, b, by the number of positions available in each block, k. However, we may perform this same count using another method. If we multiply the total number of elements, v, by the number of blocks each element is contained within, r, we will also count the number of positions available over the total number of blocks. Thus, $bk = vr$.

To prove equation (2), a similar argument is used as in the proof of equation (1). This time we are going to fix an element, x, and count the total number of pairs x makes with the other elements contained within the blocks x is an element of (this means counting all pairs, even those made with the same element in different blocks). In the first method of counting, count the number of pairs x makes in one block, $k-1$, and then multiply this number by the number of blocks x is an element of, r. Under the second method, take the total number of elements x makes a pair with, $v-1$, and multiply this number by the number of pairs x makes with each of these elements individually, λ. These two different methods count the same number of pairs, therefore $r(k-1) = \lambda(v-1)$.

Q.E.D.

Although a set of parameters may satisfy equations (1) and (2) and be admissable, this does not imply a BIBD of these parameters actually exists. For example, the set of parameters $b = v = 43$, $k = r = 7$, $\lambda = 1$ are admissable, yet only some exhaustive experimentation disproves the existence of such a BIBD [**?**].

Another condition for the existence of a BIBD follows directly from theorem 1.1:

$$r = \frac{\lambda(v-1)}{k-1} \tag{3}$$

In order for a BIBD to exist, equation (3) must yield an integer value for r. Notice that equations (3) and (1) allow us to determine all parameters of a BIBD with the knowledge of only the three parameters $\{v, k, \lambda\}$. Thus, it is a common practice to refer to a $\{v, b, k, r, \lambda\}$ design simply as a $\{v, k, \lambda\}$ design.

Example Suppose we are given the set, $V = \{1, 2, 3, 4, 5, 6, 7\}$ and we want to form a number of blocks, each of order 3, such that each pair of elements in V is contained in exactly one block. In order to complete the structure of the design, we use equations (3) and (1) and the given information to find that $b = 7$ and $r = 3$. With this information (and because of the relatively small size of the parameters) we can easily construct a family of blocks for the parameters:

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

Definition Given a BIBD $(V, \mathcal{B})$ where $\mathcal{B} = \{B_1, \ldots, B_b\}$, the *complement* of $(V, \mathcal{B})$ is $(V, \bar{\mathcal{B}})$, where $\bar{\mathcal{B}} = \{V \backslash B : B \in \mathcal{B}\}$.

Remark The complement of a BIBD with parameters $\{v, b, k, r, \lambda\}$ is a BIBD with parameters $\{v, b, b-r, v-k, b-2r+\lambda\}$.

1.1 Fisher's Inequality

One of the most famous and most basic results concerning the structure of a BIBD is Fisher's Inequality. Fisher first proved his inequality in 1940 and it has been of the utmost importance in the sutdy of BIBDs.

Theorem 1.2 *(Fisher's Inequality)* For every $\{v, k, \lambda\}$ design, we have the necessary condition that

$$b \geq v. \tag{4}$$

Although Fisher's Inequality seems like an elementary result, the proof is more complex and we will have to first introduce the concept of an *incidence matrix* and then give one of the fundamental results concerning incidence matrices.

Definition If the pair $(V, \mathcal{B})$ is a BIBD such that $V = \{x_1, x_2, ..., x_v\}$ and $\mathcal{B} = \{B_1, B_2, ..., B_b\}$, then the *incidence matrix* of such a BIBD is a $v \times b$ matrix $\mathbf{A} = (a_{ij})$ such that if $x_i \in B_j$, then $a_{ij} = 1$ and if $x_i \notin B_j$, then $a_{ij} = 0$.

Example Referring to the previous example of this section, the incidence matrix of the given $\{7, 7, 3, 3, 1\}$ design is,

$$\mathbf{A} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{array} \begin{array}{c} \begin{array}{ccccccc} B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Theorem 1.3 For $\mathbf{A}$, the incidence matrix of a given $\{v, k, \lambda\}$ design, we have

$$\mathbf{A}\mathbf{A}^T = (r - \lambda)\mathbf{I} + \lambda\mathbf{J}, \tag{5}$$

where $\mathbf{I}$ is the $v \times v$ identity matrix and $\mathbf{J}$ is a $v \times v$ matrix of all 1's.

Proof [**?**] For the proof of this result, we must first notice that because every element is found in exactly r blocks, the sum of the entries along any row of an incidence matrix will be equal to the value of r for the given design. Furthermore, the inner product of the i^{th} row of $\mathbf{A}$ and the i^{th} column of $\mathbf{A}^T$ is equal to $\sum_{s=1}^{b} a_{is}a_{is}$ and because $a_{is} = 0$ or $a_{is} = 1$, $\sum_{s=1}^{b} a_{is}a_{is} = \sum_{s=1}^{b} a_{is} = r$. Therfore, the entries along the main diagonal of the matrix $\mathbf{A}\mathbf{A}^T$ are equal to r.

Now, notice the product of entries a_{ij} and a_{kj} in matrix $\mathbf{A}$ will be 1 if and only if elements i and k are found together in block B_j. This implies that the inner product of the i^{th} row of $\mathbf{A}$ with the k^{th} column of $\mathbf{A}^T$ (really the k^{th} row

of $\mathbf{A}$) will be equal to the number of blocks i and k are common elements of, i.e., λ. Therefore, all entries not along the main diagonal of the matrix $\mathbf{AA}^T$ will be λ. From here it is clear that $\mathbf{AA}^T = (r-\lambda)\mathbf{I} + \lambda\mathbf{J}$.

Q.E.D.

.

Now, with this knowledge in mind, the use of theorem 1.3 and some linear algebra, we are ready to prove Fisher's Inequality.

Proof of Fisher's Inequality [**?**] The proof of Fisher's Inequality will done by contradiction. Hence, we begin with the assumption that $b < v$ and, if this be the case, we may add $v - b$ columns of 0's to the $v \times b$ incidence matrix $\mathbf{A}$ to create a $v \times v$ matrix $\mathbf{B}$. However, because we added only columns of 0's to $\mathbf{A}$ in order to create $\mathbf{B}$, it is clear that

$$\mathbf{AA}^T = \mathbf{BB}^T.$$

Furthermore, by the laws of determinants, $\det(\mathbf{AA}^T) = \det(\mathbf{BB}^T)$ and, because $\mathbf{B}$ contains a column of 0's, we may further state that

$$\det(\mathbf{AA}^T) = \det(\mathbf{BB}^T) = 0.$$

At this point, we apply theorem 1.3 to obtain

$$\det(\mathbf{AA}^T) = \det\begin{bmatrix} r & \lambda & \lambda & \lambda & \dots & \lambda \\ \lambda & r & \lambda & \lambda & \dots & \lambda \\ \lambda & \lambda & r & \lambda & \dots & \lambda \\ \lambda & \lambda & \lambda & r & \dots & \lambda \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \lambda & \dots & \lambda \\ \lambda & \lambda & \lambda & \lambda & \dots & r \end{bmatrix}.$$

We will now compute the determinant of this matrix. In our effort to do this it is important to remember that by the laws of determinants we may perform any number of row and column transformations without changing the value of the determinant. Thus, we will begin by subtracting the first column of the matrix from all others. The result of this transformation is

$$\det(\mathbf{AA}^T) = \det\begin{bmatrix} r & \lambda - r & \lambda - r & \lambda - r & \dots & \lambda - r \\ \lambda & r - \lambda & 0 & 0 & \dots & 0 \\ \lambda & 0 & r - \lambda & 0 & \dots & 0 \\ \lambda & 0 & 0 & r - \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & 0 & \dots & 0 \\ \lambda & 0 & 0 & 0 & \dots & r - \lambda \end{bmatrix}.$$

We will now add every row to the first row to obtain the following:

$$\det(\mathbf{A}\mathbf{A}^T) = \det \begin{bmatrix} r+(v-1)\lambda & 0 & 0 & 0 & \dots & 0 \\ \lambda & r-\lambda & 0 & 0 & \dots & 0 \\ \lambda & 0 & r-\lambda & 0 & \dots & 0 \\ \lambda & 0 & 0 & r-\lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & 0 & \dots & 0 \\ \lambda & 0 & 0 & 0 & \dots & r-\lambda \end{bmatrix}.$$

Now the matrix in question contains all 0's in the upper-triangle and its determinant may be computed directly by taking the product of the entries along its main diagonal,

$$\det(\mathbf{A}\mathbf{A}^T) = (r+(v-1)\lambda)(r-\lambda)^{v-1}.$$

Now, if $\det(\mathbf{A}\mathbf{A}^T) = 0$, then either $(r+(v-1)\lambda) = 0$ or $(r-\lambda) = 0$. However, the initial assumptions about BIBDs state that $r > 0, \lambda > 0$, and $v \geq 2$. Therefore,

$$(r+(v-1)\lambda) > 0.$$

As for $(r-\lambda)$, our initial assumptions about BIBDs also state that $v > k$, which implies by equation (2) that $r > \lambda$. Hence,

$$(r-\lambda) > 0$$

and $\det(\mathbf{A}\mathbf{A}^T) \neq 0$, a contradiction.

Q.E.D.

1.2 An Introduction to Finite Projective Planes

Some BIBDs can be described alternatively using geometry. If the parameter $\lambda = 1$ is set, then a BIBD can be described using a number of points and lines in a plane. Each element of the v-element set will correspond to a point on the plane and every block will correspond to a line which connects a fixed number of points. Thus, the same number of points will lie along each line and every point will lie on exactly r lines. Further, given that $\lambda = 1$, between every pair of points there will be a unique line.

Definition A *finite projective plane* is a finite set of points and lines such that,

(P_1) through any two points there is a unique line, and

(P_2) any two lines have exactly one intersection point.

From this definition it is somewhat obvious that these conditions will be trivially satisfied by a single line with any number of points on it. Other trivial constructions also exist, however, to avoid these situations a third condition will be introduced:

(P_3) in any finite projective plane there exist four points, of which no three

lie on the same line
A finite projective plane that satisfies (P_3) is called *nondegenerate* and it is finite projective planes of this kind that will be considered in this text.

Definition For a finite projective plane with $m + 1$ points on each line, m is the *order* of the given projective plane.

Example The most famous example of a finite projective plane is the Fano plane (see Figure 1). The plane consists of seven points and seven lines, six straight and one circular. Three points lie along each of the lines (i.e., the Fano plane has an order of two) and each pair of lines intersect at exactly one point.

Figure 1: The Fano plane. Line intersections occur only where there are large points.

It is possible to describe a BIBD with $\lambda > 1$ geometrically, however, the geometric object will not be in two dimensions. For further reading on such geometries, see [**?**].

There are a number of important theorems that describe projective planes and, later on, these theorems will be very useful in describing situations in which BIBDs exist.

Theorem 1.4 For any finite projective plane, the number of lines through each point is equal to the number of points on each line.

Proof [**?**] The three conditions which describe a finite projective plane will provide the proof for this theorem. Take any line within a finite projective plane, L. By (P_3) there is a point x that does not lie on L. Further, by (P_1) for every point y on L there exists a through x that intersects the point y, call these lines L_y. Now, assume there is a line L' through x that does not intersect any point y on L. However, this is a contradiction by (P_2). Hence, L' is a line L_y through some point y on L and the lines through x form a one-to-one correspondence with the points on any given line L. In other words, the number of lines through each point in a finite projective plane is equal to the number of points on each line.

Q.E.D.

In terms of a BIBD, this theorem implies the condition $r = k$. Theorem 1.1 further implies that if $r = k$, then $b = v$. Therefore, any BIBD that may be represented by a finite projective plane will have the condition $r = k$ and $b = v$. This concept will be discussed further in section 3.2.

Corollary 1.4.1 A finite projective plane with $m + 1$ points on each line has $m^2 + m + 1$ points and $m^2 + m + 1$ lines.

Proof By theorem 1.4, a finite projective plane with $m + 1$ points on each line will have $m + 1$ lines through each point. Now, take any point x. There are $m + 1$ lines through x and each of these lines has m points on it other than x. Now we can simply count the total number of points by multiplying the total number of lines through x times the number of points on each of these lines other than x, and adding x to the total:

$$m(m + 1) + 1 = m^2 + m + 1$$

This same argument can be made to count the total number of lines in a finite projective plane.

Q.E.D.

This corollary may also be explained through an application of theorem 1.1. A plane with $m + 1$ points on each line implies $k = m + 1$ and from theorem 1.4 we have seen that $r = k$ in such a situation. Therefore, equation (2) implies the following relation:

$$\begin{aligned} v - 1 &= (m + 1)m, \quad or \\ v &= m^2 + m + 1. \end{aligned}$$

It follows from our discussion of theorem 1.4 that $b = v = m^2 + m + 1$, the result given (in different terms) by the above corollary.

1.3 Orthogonal Latin Squares [1]

Definition A *Latin square* is a $k \times k$ matrix whose elements are chosen from a set of n elements ($S = \{a_1, a_2, \ldots, a_n\}$, for example) such that every row and every column of the matrix contains each of these n elements exactly once.

In many cases we identify the n elements set with the set of the first n positive integers, i.e., $S = \{1, 2, \ldots, n\}$. With this identification an example of an orthogonal Latin square is shown below:

[1] This section has been closely adapted from a text prepared by Miklos[**?**]

$$\begin{bmatrix} 1 & 2 & 3 & \cdots & k-1 & k \\ 2 & 3 & 4 & \dots & k & 1 \\ 3 & 4 & 5 & \dots & 1 & 2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ k-1 & k & 1 & \dots & k-3 & k-2 \\ k & 1 & 2 & \cdots & k-2 & k-1 \end{bmatrix}$$

Definition Similar to a Latin square, a *Latin rectangle* is an $\ell \times k$ matrix ($k \geq \ell$) whose elements are chosed from a k element set (again, normally identified with the set $\{1, 2, \dots, k\}$) such that every row of the matrix contains each of these elements (each of $1 \leq i \leq k$) exactly once and every column of the matrix contains each of these element (each of $1 \leq i \leq k$) at most once.

Example An example of a Latin rectangle is shown below:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \\ 6 & 4 & 5 & 3 & 1 & 2 \\ 5 & 1 & 2 & 6 & 3 & 4 \end{bmatrix}$$

Definition Two distinct Latin squares $A = (a_{ij})$ and $B = (b_{ij})$ are called *orthogonal* if and only if the n^2 ordered pairs (a_{ij}, b_{ij}) are all different.

Example It follows from the definition that the two 4×4 Latin squares below are orthogonal:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} \qquad \begin{bmatrix} 4 & 1 & 2 & 3 \\ 3 & 2 & 1 & 4 \\ 1 & 4 & 3 & 2 \\ 2 & 3 & 4 & 1 \end{bmatrix}$$

On the other hand, the two 4×4 Latin squares below are not orthogonal:

$$\begin{bmatrix} 2 & 1 & 4 & 3 \\ 3 & 2 & 1 & 4 \\ 4 & 3 & 2 & 1 \\ 1 & 4 & 3 & 2 \end{bmatrix} \qquad \begin{bmatrix} 2 & 3 & 1 & 4 \\ 1 & 4 & 2 & 3 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \end{bmatrix}$$

since the pair $(2, 4)$ appears twice, at positions 2,2 and 3,3.

More generally, if $A^{(1)}, A^{(2)}, \dots, A^{(r)}$ are distinct $n \times n$ Latin squares, they are said to form an *orthogonal family* if every pair of them is orthogonal.

There are three main questions in the study of orthogonal Latin squares:

1. Does there exist a pair of orthogonal Latin squares for every k,
2. In general, how large is the orthogonal family of Latin squares for a given size k, and
3. Is it always possible to augment a Latin rectangle into Latin square?

We will skip the last question here, since the graph theoretical background needed to examine this question will not be discussed in this paper.

As for the first question, it is easy to see that the only Latin squares of order two are

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \qquad \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

and they are not orthogonal.[2]

On the other hand, we have previously seen a pair of 4×4 orthogonal Latin squares and the following two Latin squares make an orthogonal pair of order three,

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$$

Theorem 1.5 If there is an orthogonal family of r Latin squares of order n, then $r \leq n - 1$.

Proof Assume $A^{(1)}, A^{(2)}, \ldots, A^{(r)}$ is a family of orthogonal Latin squares of order n. Let the elements of the squares be the set of numbers $\{1, 2, .., n\}$ and perform the following operation on exactly one of the r squares: for a fixed pair i and j $(1 \leq i < j \leq n)$ exchange each i^{th} element of the square with the j^{th} element and vice versa. This operation will permute the elements of the square but the resulting square will be isomorphic to its predecessor and the family of Latin squares will remain a family of r orthogonal Latin squares.

Using this operation, first change $A^{(1)}$ such that its first row becomes $1, 2, \ldots, n$, then change $A^{(2)}$ the same way, and so on. Finally, we will get another family $B^{(1)}, B^{(2)}, \ldots, B^{(r)}$ of Latin squares such that each square in this family will have its first row equal to $1, 2, \ldots, n$. Now, when the elements of any two squares in this new family are grouped in pairs, all the pairs $(i, i),\ 1 \leq i \leq n$ will occur in the first row. Therefore, except for in the first row, no pair of these r matrices may have the same element in the same position. Clearly then, it follows that the first element in the second row of each of these matrices is different and is chosen from the set $\{2, 3, \ldots, n\}$. Therefore, the number of matrices is at most $n - 1$.

Q.E.D.

In the case that there exists an orthogonal family of $r = n - 1$ Latin squares of order n, this is referred to as the *complete orthogonal family* of Latin squares of order n.

Theorem 1.6 For every prime factor $n = p^k$ there is a complete orthogonal family of Latin squares of order n.

[2] In some conventions a single 2×2 Latin square is allowed to represent an orthogonal family.

Sketch of Proof It is a well known algebraic result that for every prime power $n = p^k$ (and only for prime powers) there is a unique so called *field*, an algebraic structure which behaves with respects to the operations addition and multiplication (and their inverses, subtractions and division). Essentially it is a set which behaves like the field of rational numbers. The fields of order $n = p^k$ are called *Galois fields* and are denoted by $\mathrm{GF}(p^k)$.

With the help of this Galois field we will define the $n-1$ orthogonal Latin squares. Let the elements of the field be $b_1, b_2, \ldots, b_n$, where b_1 is the multiplicative identity of the field (think of 1 in the field of the rational numbers) and b_n is the additive identity (think of 0 of the field of the rational numbers). Now define for every $e = 1, 2, \ldots, n-1$ a Latin square $A^{(e)} = \left(a_{ij}^{(e)}\right)$ by $a_{ij}^{(e)} = (b_e \times b_i) + b_j$. One can check that the family of matrices obtained this way form a family of $n-1$ orthogonal Latin squares of size $n = p^k$.

Theorem 1.7 Given an orthogonal family of r Latin squares of order n and another orthogonal family of r Latin squares of order m, there is another orthogonal family of r Latin squares of order nm.

Proof Let $A^{(1)}, A^{(2)}, \ldots, A^{(r)}$ be the orthogonal family of Latin squares of order n and $B^{(1)}, B^{(2)}, \ldots, B^{(r)}$ be the orthogonal family of Latin squares of order m. For a given element $a_{ij}^{(e)}$ of $A^{(e)}$, let $\left(a_{ij}^{(e)}, B^{(e)}\right)$ be a $m \times m$ matrix whose (k,l) entry is the pair (note that this Latin square will consist of pairs, rather than single numbers) $\left(a_{ij}^{(e)}, b_{kl}^{(e)}\right)$. From these $m \times m$ matrices form an $nm \times nm$ matrix by assembling them together according to the arrangement,

$$C^{(e)} = \begin{bmatrix} \left(a_{11}^{(e)}, B^{(e)}\right) & \left(a_{12}^{(e)}, B^{(e)}\right) & \cdots & \left(a_{1n}^{(e)}, B^{(e)}\right) \\ \left(a_{21}^{(e)}, B^{(e)}\right) & \left(a_{22}^{(e)}, B^{(e)}\right) & \cdots & \left(a_{2n}^{(e)}, B^{(e)}\right) \\ \vdots & \vdots & \ddots & \vdots \\ \left(a_{n1}^{(e)}, B^{(e)}\right) & \left(a_{n2}^{(e)}, B^{(e)}\right) & \cdots & \left(a_{nn}^{(e)}, B^{(e)}\right) \end{bmatrix}$$

The matrices $C^{(1)}, C^{(2)}, \ldots, C^{(r)}$ now form an orthogonal family of r Latin squares of order nm.

Q.E.D.

Corollary 1.7.1 If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ is the prime power decomposition of the integer $n > 1$, then there is an orthogonal family of Latin squares of order n of size $\min\left\{\left(p_1^{\alpha_1} - 1\right), \left(p_2^{\alpha_2} - 1\right), \ldots, \left(p_n^{\alpha_n} - 1\right)\right\}$.

Proof For every prime power p^{α_i} we have a family of $p^{\alpha_i} - 1$ orthogonal Latin squares of order p^{α_i}. Then the repeated application of theorem 1.7 finishes the proof of the corollary.

Corollary 1.7.2 For some $n > 1$, if n is not divisible by two or some higher power of two, then there is at least one pair of orthogonal Latin squares of order n.

The proof of this corollary is immediate by the previous result.

By the above theorems only numbers of the form $n = 2k$ where k is odd are we not able to decide if there is a pair of orthogonal Latin squares of the given size. As it turns out, it has been shown that for $n = 2$ and $n = 6$ there is no pair of orthogonal Latin squares, while for all other numbers there is.

1.4 Orthogonal Latin Squares and Finite Projective Planes

The existence of an orthogonal family of Latin squares is closely related to the existence of a finite projective plane. Indeed, the following theorem and corollary will describe a relation among the existence of an orthogonal family of Latin squares, the existence of a finite projective plane, and possible values for the order of a finite projective plane.

Theorem 1.8 If $m \geq 2$, then a finite projective plane of order m exists if and only if a complete orthogonal family of $m \times m$ Latin squares exists.[3]

Sketch of Proof [**?**] We will show the proof of this theorem in one direction and outline the proof of the opposite statement. Let P be a finite projective plane of order m. Designate a line L of P as the *line at infinity*. This line will connect the $m+1$ points $\{u, v, w_1, w_2, \ldots, w_{m-1}\}$ and there will be m lines other than L through each of these points. Let the lines through each point be designated as follows:

$$\begin{aligned} \text{lines through } u: &\quad L, U_1, U_2, \ldots, U_m, \\ \text{lines through } v: &\quad L, V_1, V_2, \ldots, L_m, \\ \text{lines through } w_j: &\quad L, W_{j1}, W_{j2}, \ldots, W_{jm}. \end{aligned}$$

Every point x that does lie on L, there is a unique line connecting every point on L to the point x. For u and x, let this line be U_h, for v and x let it be V_i, and for w_j and x let this line be W_{jk_j}. Using this notation, we can associate every point x with the $(m+1)$-tuple $(h, i, k_1, k_2, \ldots, k_{m-1})$. Further, the correspondence between points not on line L and couples (h, i) will constitute a one-to-one relationship. If two points not on line L both lie on the line represented by h, then the i coordinate for each point must be different by the second condition (P_2) of the definition of a finite projective plane. We can now construct a family of matrices using this set of ordered pairs. Let $a_{hi}^{(j)} = k_j$ if the point x corresponding to the pair (h, i) also corresponds to the $(m+1)$-tuple

[3] In the instance that $m = 2$, allow a single 2×2 Latin square to constitute an orthogonal family.

$(h, i, k_1, \ldots, k_m - 1)$ and let $\mathbf{A}^{(j)} = a_{hi}^{(j)}$ for $j = 1, 2, \ldots, m-1$. We will now show that each of these matrices is indeed a Latin square. If $a_{hi}^{(j)} = a_{hi'}^{(j)}$, then both the line U_h and the line W_{jk_j} will connect the two points corresponding to (h, i) and (h, i'), a contradiction. The same can be if the two points in question correspond to (h, i) and (h', i). To finish this portion of the proof, see that for any two Latin squares $\mathbf{A}^{(p)}$ and $\mathbf{A}^{(q)}$ of this family, where $p \neq q$, all the pairs $(a_{hi}^{(p)}, a_{hi}^{(q)})$ must be different. If two pairs we have $(a_{hi}^{(p)}, a_{hi}^{(q)}) = (a_{h'i'}^{(p)}, a_{h'i'}^{(q)})$, then the points corresponding to (h, i) and (h', i') will be connected by the lines W_{pk_p} and W_{qk_q}, an obvious contradiction.

The proof is completed by showing a finite projetive plane of order m exists given a complete orthogonal family of Latin squares $\mathbf{A}^{(1)}, \mathbf{A}^{(2)}, \ldots, \mathbf{A}^{(m-1)}$. For this let the pair (h, i), where $h = 1, \ldots, m,\ i = 1, \ldots, m$, correspond to m^2 points. Also, assign each point an $(m+1)$-tuple $(h, i, k_1, \ldots, k_{m-1}$ where $k_j = a_{hi}^{(j)}$. Then form $m^2 + m$ lines W_{jk} by letting W_{jk} correspond to the set of all points (h, i) such that $a_{hi}^{(j)} = k_j$. One more line is then constructed with $m+1$ points so that every previously non-intersecting pair of lines will intersect at a point along this line. Basically, this is the construction that will yield a finite projective plane from a complete orthogonal family of Latin squares and it can be verified that this construction does indeed produce a finite projective plane.

Corollary 1.8.1 If $m = p^k$, where p is a prime number and k is a positive integer, then there exists a finite projective plane of order m.

The proof of this corollary is immediate by the above result and theorem 1.6.

2 Steiner Triple Systems

We previously mentioned that for $k = 2$ there is only one acceptable BIBD for each value of v. Thus, we begin with the next smallest value, $k = 3$. Specifically, we will begin with an investigation of designs with parameters $k = 3$ and $\lambda = 1$, which are of particular interest and have been given a special title.

Definition A *Steiner triple system* (*STS*) is a BIBD such that $k = 3$ and $\lambda = 1$ (a $\{v, 3, 1\}$ design).

Remark The Fano plane mentioned in the previous section is the geometric characterization of a STS over 7 elements. Each line (block) is defined by three points (elements) and for every two points there exists a unique line through them (every pair of elements appears in only one block).

Definition If the pair $(V, \mathcal{B})$ defines a STS, $W \subseteq V$, $\mathcal{D} = \{B \in \mathcal{B} | B \subset W\}$, and $(W, \mathcal{D})$ is a STS, then $(W, \mathcal{D})$ is called a *subsystem* of $(V, \mathcal{B})$.

Steiner triple systems are of such great interest for a number of reasons. Primarily, they are of intereset because their small size makes them quite manageable to work with and because k and λ are fixed we are able to determine necessary requirements for the other parameters of the design. This allows us to give a more concrete description of when a STS actually exists. Indeed, from theorem 1.1 it follows that for a STS

$$r = \frac{v-1}{2}, \tag{6}$$

and it follows that v must be odd.

From theorem 1.1 it can also be seen that for a STS $3b = vr$, or after an application of equation (6),

$$b = \frac{v(v-1)}{6}. \tag{7}$$

Although triple systems such that $\lambda = 1$ have been named for Steiner, it was actually Kirkman who originally began studying them in the 1840's. In fact, it was Kirkman who in 1847 proved the most fundamental result about the existence of a Steiner triple system over v elements.

Theorem 2.1 *(Kirkman 1847)* A Steiner triple system over v elements exists if and only if $v \equiv 1, 3 \ (mod\ 6)$ for $k \geq 1$ and $v \geq 3$.

For each value $v = \{3, 7, 9\}$ there is a unique STS, up to isomorphism. For $v = 13$ there are two solutions and 80 different STSs have been found for $v = 15$. For all values $v > 15$ it is not known how many STSs exist, however, the following theorems will show that is easy to determine whether or not a STS of larger or smaller order exists given the existence of one or two initial systems. Furthermore, these theorems will be necessary in order to sketch the proof of Kirkman's theorem in section 2.1.

Theorem 2.2 Given a STS $(V, \mathcal{B})$, if there exists a set $X \subset V$ such that $|X| = \frac{v-1}{2}$ and at least one element from each block of $\mathcal{B}$ is contained in X, then a STS exists over the set X.

Proof [**?**] Let $\mathcal{D}$ be the set of blocks over X. The set $\mathcal{D}$ will consist of all the blocks of $\mathcal{B}$ that contain only elements of the set X. Now we must show that the pair $(X, \mathcal{D})$ constitutes a STS. Because we have chosen blocks from an already existing STS, each block will have three elements and no pair of elements will be found in more than one block. Therefore, all that remains to prove is that every pair of elements in X is contained in a block of $\mathcal{D}$. Consider two elements $x_i, x_j \in X$. If x_i and x_j are not found together in a block of $\mathcal{D}$, they will be found in a block of the original STS. Furthermore, the third element of this block will not be an element of X, otherwise the block in question would be contained in $\mathcal{D}$. Now let us consider this third element. This element is contained in $\frac{v-1}{2}$ total blocks of the original STS and each of these blocks

must have at least one element contained in X. However, one of these blocks has both x_i and x_j contained in X. This implies the number of elements in X is,

$$\frac{v-1}{2} + 1 = \frac{v+1}{2}$$

a contradiction. Hence, two elements $x_i, x_j \in X$ will be contained in a block of $\mathcal{D}$ and $(X, \mathcal{D})$ will constitute a STS.

Q.E.D.

Theorem 2.3 If there is a STS S_1 over v_1 elements and a STS S_2 over v_2 elements, then there exists a STS S over $v_1 v_2$ elements.

Proof [**?**] The proof of this theorem will be done by construction. Let the STS S_1 be over the elements $\{a_1, \ldots, a_{v_1}\}$ and let S_2 be over the elements $\{b_1, \ldots, b_{v_2}\}$, then S will have elements c_{ij} where $1 \leq i \leq v_1, 1 \leq j \leq v_2$ and each element c_{ij} represents the pair $\{a_i, b_j\}$. The triple $\{c_{ir}, c_{js}, c_{kt}\}$ will define a block in the STS S if and only if

(1) $i = j = k$ and $\{b_r, b_s, b_t\}$ defines a block in S_2, or if
(2) $r = s = t$ and $\{a_i, a_j, a_k\}$ defines a block in S_1, or if
(3) $\{a_i, a_j, a_k\}$ defines a block in S_1 and $\{b_r, b_s, b_t\}$ defines a block in S_2.

To finish the proof we must show this construction defines a STS. Clearly each block in S will contain 3 elements, so $k = 3$ is satisfied. Now, to show the construction satisfies $\lambda = 1$ we will show in every case that the pair $\{c_{ir}, c_{js}\}$ will be contained in only one block. If for the pair $\{c_{ir}, c_{js}\}$ both $\{a_i, a_j\}$ and $\{b_r, b_s\}$ are contained in a block in S_1 and S_2, respectively, then for $\{c_{ir}, c_{js}\}$ to be contained in a second block, either $\{a_i, a_j\}$ would have to be in a second block in S_1 or $\{b_r, b_s\}$ would have to be found in a second block in S_2, a contradiction. Similarly, if $i = j$ and $\{c_{ir}, c_{js}\}$ is found in more than one block in S, then the pair $\{b_r, b_s\}$ would have to be contained in more than one block in S_2, another contradiction based on our knowledge of the STS S_2. The same argument may be used if we assume $r = s$.

Q.E.D.

Theorem 2.4 If there is a STS of order v_2 containing a subsystem of order v_3 (or if we take $v_3 = 1$) and if a STS can be taken over a set of order v_1, then we can construct another STS of order $v = v_3 + v_1(v_2 - v_3)$ containing $v1$ subsystems of order v_2, one of order v_1, and one of order v_3.

Proof [**?**] The proof of this theorem is by construction. We will begin with an array of v elements in $(v_1 + 1)$ sets. Among these sets, there will be one of order v_3 and v_1 of order $s = (v_2 - v_3)$:

$$\begin{array}{rcccc} S_0 = & (a_1, & a_2, & \dots & a_{v_3}) \\ S_1 = & (b_{11}, & b_{12}, & \dots & b_{1s}) \\ S_2 = & (b_{21}, & b_{22}, & \dots & b_{2s}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ S_{v_1} = & (b_{v_1 1}, & b_{v_1 2}, & \dots & b_{v_1 s}) \end{array}$$

This array constitutes the elements of the STS of order v and the triples of this STS will be formed according to the following three rules:

(a) Let the given STS of order v_3 be taken over the set S_0 and take all triples $\{a_i, a_j, a_k\}$ of this STS to be triples of the new STS of order v.

(b) Make $S_0 \cup S_i$, $i = 1, ..., v_1$ correspond to a STS of order v_2. Each of these systems will contain triples $\{a_i, a_j, a_k\}$ that have already been defined by rule (a) and because no pair $\{a_i, a_j\}$ may appear in another triple, the remaining triples will have at most one element of the type a_m. Therefore, the remaining triples will be of the form $\{a_m, b_{ij}, b_{ik}\}$ or $\{b_{ij}, b_{ir}, b_{it}\}$ and all of these triples will be added to the new STS under construction.

(c) Finally, write a STS over the set of integers $\{1, ..., v_1\}$ and if $\{j, k, r\}$ is a triple of this system, then $\{b_{jx}, b_{ky}, b_{rz}\}$ will be a triple of the new system if $x + y + z \equiv 0 \ (mod\ s)$.

These rules form the triples of a STS over v elements. Notice that (a) gives all triples containing three a's and that no other triple contains more than one a, therefore every pair of a's is found in only one triple. By rule (b), all pairs of b's from the same row will be placed with an a in one triple and triples of all b's will contain three elements from the same row but will not repeat pairs from the triples of the form $\{a_m, b_{ij}, b_{ik}\}$. Now, by rule (c) every pair $\{b_{jx}, b_{ky}\}$ will appear in a unique triple with an element b_{rz} where r is determined by the triple $\{j, k, r\}$ and z is determined by the relation $x + y + z \equiv 0 \ (mod\ s)$. Further, it is clear that this STS contains a subdesign of order v_3 (the triples taken over S_0) and v_1 subdesigns of order v_2 (the triples taken over $S_0 \cup S_i, i = 1, ..., v_1$). Another subdesign of order v_1 is found among the triples taken over the set $\{b_{1s}, b_{2s}, ..., b_{v_1 s}\}$, which proves the theorem.

Q.E.D.

2.1 Proof of Kirkman's Theorem

Here we will sketch the proof of Kirkman's theorem of 1847. The first task is to show a STS does not exist unless $v \equiv 1, 3 \ (mod\ 6)$. This can be done with the simple application of equations (6) and (7). It is clear from equation (6) that v must be odd. Moreover, equation (7) implies that either v, $v - 1$, or the product $v(v - 1)$ must be divisible by six. Now, with these conditions in mind, some careful calculation will show that $v \equiv 1, 3 \ (mod\ 6)$ is a necessary condition in order for b and r to be integers.

The next challenge is to show that a STS exists for every $v \equiv 1, 3 \ (mod\ 6)$. This is shown using a recursive construction that applies theorem 2.4 to construct a number of recursive rules to build larger and larger STSs from a small

number of initial values. Here is an example of such a recursive rule,

$$v_1 = v',\ v_2 = 3,\ v_3 = 1,\ v = 2v' + 1,\ v' \geq 3. \tag{8}$$

This is just one of a number of rules that can be used to show the existence of a STS for almost every value $v = 1, 3\ (mod\ 6)$. In some cases these constructions will not produce a STS for some value $v \equiv 1, 3\ (mod\ 6)$. In the case of such an exception, theorems 2.3 and 2.4 can be applied directly to show an STS does exist for such a value. For more on this proof see Hall [**?**]. A proof of Kirkman's theorem which uses a direct construction is known from Skolem sequences (for a full discussion of Skolem sequences see [**?**]).

3 Symmetric BIBDs

Because there are so many variables to be considered in the study of BIBDs, of main interest are types of BIBDs with a number of fixed or otherwise manipulated parameters. As previously stated, Steiner triple systems deal with BIBDs that have two fixed parameters. Another class of BIBDs lie at the lower bound of Fisher's inequality, those BIBDs with $b = v$.

Definition A *symmetric* BIBD (or simply a *symmetric design*) is a BIBD such that $b = v$.

From theorem 1.1 we know that for every BIBD the relation $bk = vr$ holds. Hence,

$$b = v \iff r = k \tag{9}$$

and it is clear that we may equivalently define a symmetric BIBD as a BIBD such that $r = k$. This alternative definition may now be applied to equation (2) of theorem 1.1 to come up with the following relation which holds for every symmetric BIBD:

$$\lambda(v - 1) = k(k - 1). \tag{10}$$

Definition The *order* of a symmetric design is the value $n = k - \lambda$.

For every symmetric design the parameter v will satisfy the following inequality:

$$4n - 1 \leq v \leq n^2 + n + 1. \tag{11}$$

We will see in the following sections that the designs found at the upper bound of this inequality correspond to a projective plane of order n and will have parameters $v = b = n^2 + n + 1, k = r = n + 1,\ and\ \lambda = 1$. The designs at the lower bound, on the other hand, correspond to a *Hadamard design* of dimension n and will have parameters $v = b = 4n - 1, k = r = 2n - 1,\ and\ \lambda = n - 1$. The relation of symmetric designs to each of these topics will be explored further in the upcoming sections.

3.1 Symmetric Designs and Finite Projective Geometry

A perfect example of a symmetric BIBD is once again provided by the Fano plane, which represents a symmetric design with $b = v = 7$, $r = k = 3$, and $\lambda = 1$. In fact, every finite projective plane is a representation of a symmetric BIBD. In section 1.3 it has been described how a finite projective plane can represent a BIBD. It follows from theorem 1.4 and corollary 1.4.1 that any projective plane will correspond to the conditions $b = v$ and $r = k$. Hence, the question of whether or not a symmetric BIBD exists can be asked: does a finite projective plane of a given number of points exist?

Theorem 3.1 If $m \geq 2$, a $\left\{m^2 + m + 1, m + 1, 1\right\}$ symmetric design exists if and only if a projective plane of order m exists.

The proof of this theorem follows from corollary 1.4.1 and the correspondence between a finite projective plane and a BIBD. A trivial corollary to this theorem due to theorem 1.5 is as follows.

Corollary 3.1.1 There are $\left\{m^2 + m + 1, m + 1, 1\right\}$ symmetric designs whenever $m = p^k$, where p is a prime and k is a positive integer.

With this result and theorem 1.6, we are now able to present an important corollary relating the existence of a finite projective plane, a symmetric BIBD, and a complete orthogonal family of Latin squares.

Corollary 3.1.2 For $m \geq 2$ the following three statements are equivalent:

1. There exists a finite projective plane of order m.
2. There exists a complete orthogonal family of Latin squares of order m.
3. There exists an $(m^2 + m + 1, m + 1, 1)$ symmetric BIBD.

3.2 The Bruck-Ryser-Chowla Theorem

The most fundamental necessary condition for the existence of a symmetric BIBD is due to the Bruck-Ryser-Chowla theorem. This result was first proved for $\lambda = 1$ by Ryser and Bruck in 1949 and in generality by Ryser and Chowla in 1950.

Theorem 3.2 *(The Bruck-Ryser-Chowla Theorem)* In order for a symmetric BIBD to exist, the following conditions must be satisfied:

1. If v is even, then $k - \lambda$ is the square of an integer.
2. If v is odd, then the equation

$$z^2 = (k - \lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2 \tag{12}$$

has a solution for integer values of x, y, and z not all equal to zero.

This theorem is an extremely powerful result and until quite recently it was conjectured that any set of parameters that satisfied both equation (10) and the Bruck-Ryser-Chowla theorem would produce a symmetric design. This conjecture, however, has been proven false by an extensive computer search that showed a $\{111, 11, 1\}$ symmetric design cannot exist [**?**]. For a full proof of this theorem consult Hall [**?**] or Ryser [**?**].

3.3 Existence Problems for $m \neq p^k$

By corollary 3.2.1 it is clear that a $\{m^2 + m + 1, m + 1, 1\}$ symmetric design exists when m is a power of a prime, but what happens when m is not a power of a prime? Let us check first the integer that is not a power of a prime, six. For $m = 6$ we will have to check for the existence of a $\{43, 7, 1\}$ design, and because v is odd the parameters of this design must produce a solution to equation (12) of the Bruck-Ryser-Chowla theorem. Thus, there must be a solution to the equation

$$\begin{aligned} z^2 &= 6x^2 + (-1)^{21}y^2, \quad or \\ 6x^2 &= z^2 + y^2 \end{aligned}$$

in x, y, and z, not all zero.

Consider the following, $6x^2$ is divisible by three, so $z^2 + y^2$ must also be divisible by three. If the sum $z^2 + y^2$ is divisible by three, then z^2 and y^2 must each be divisible by three. Further, if z^2 and y^2 are each divisible by three, they will each be divisible by nine. This implies that z and y will each be divisible by three. Now, because six is clearly not divisible by nine but is divisible by three, x^2 must be divisible by three, which implies that x^2 must be divisible by nine and x must be divisible by three. Let i_x be the highest power of three which divides x. Likewise, let i_y and i_z denote the highest powers of three that divide y and z, respectively. If we assume $i_y \geq i_z$, it follows that the highest power of three which divides $z^2 + y^2$ will be an even power of three, $2i_z$. On the other hand, the highest power of three that divides $6x^2$ will be $2i_x + 1$. This contradiction proves no solution in integers x, y, and z (not all zero) exists for the equation $6x^2 = z^2 + y^2$ and a $\{m^2 + m + 1, m + 1, 1\}$ symmetric design will not exist for $m = 6$.

The next integer which is not a power of a prime is ten. In this case we have previously mentioned that $\{111, 11, 1\}$ does not exist, but this result was not so easy to show. In fact, for all $m \geq 12$ where $m \neq p^k$ it is not known if $\{m^2 + m + 1, m + 1, 1\}$ symmetric design exists or not.

3.4 Hadamard Designs and Matrices

Hadamard designs are a specific form of symmetric BIBDs found when the parameter v lies at the lower bound of inequality (11). Moreover, Hadamard

designs are particularly useful in the theory of error correcting coding.

Definition A *Hadamard design of dimension* m is a $\{4m-1, 2m-1, m-1\}$ symmetric BIBD.

Definition A *Hadamard matrix* is a matrix $\mathbf{H}$ whose entries are 1's and -1's such that $\mathbf{H}\mathbf{H}^T = n\mathbf{I}$, where $\mathbf{I}$ is the $n \times n$ identity matrix. A *normalized* Hadamard matrix has only 1's in its first row and column.

Hadamard matrices will be a useful tool in the proof of a fundamental result concerning the existence of a Hadamard design. However, it is necessary to show a few results describing Hadamard matrices.

Theorem 3.3 If $\mathbf{H}$ is a Hadamard matrix, so is $\mathbf{H}^T$.

Proof If $\mathbf{H}\mathbf{H}^T = n\mathbf{I}$, then

$$\frac{\mathbf{H}}{\sqrt{n}}\frac{\mathbf{H}^T}{\sqrt{n}} = \mathbf{I} \tag{13}$$

Now, from linear algebra it is true that if $\mathbf{A}\mathbf{B} = \mathbf{I}$ for square matrices $\mathbf{A}$ and $\mathbf{B}$, then $\mathbf{B}\mathbf{A} = \mathbf{I}$. Therefore,

$$\frac{\mathbf{H}^T}{\sqrt{n}}\frac{\mathbf{H}}{\sqrt{n}} = \mathbf{I}, \tag{14}$$

or $\mathbf{H}^T\mathbf{H} = \mathbf{I}$. Since $(\mathbf{H}^T)^T = \mathbf{H}$, $\mathbf{H}^T$ is also a Hadamard matrix.

Q.E.D.

Theorem 3.4 If $\mathbf{H}$ is a normalized Hadamard matrix of order $n > 2$, then $n = 4m$, for some m. Furthermore, exactly $2m$ entries of each row (column) except the first are 1's, exactly $2m$ are -1's, and for every two rows (columns) other than the first, there are exactly m columns (rows) in which both rows (columns) have a 1.

Proof [**?**] By Theorem 3.3, the results for columns will follow directly from the results for rows. Therefore, here will we only show the result for rows. Let $\mathbf{H}$ be a normalized Hadamard matrix of order n. Since $\mathbf{H}\mathbf{H}^T = n\mathbf{I}$, the inner product of the i^th row of $\mathbf{H}$ with itself will be 1, the inner product of rows i and j $(i \neq j)$ is 0, and the first row and column of $\mathbf{H}$ will be all 1's. This implies that every row except the first must have an equal number of 1's and -1's. Thus, n must be even and $n/2$ entries of each row are 1 and $n/2$ are -1.

Rearrange the columns of $\mathbf{H}$ so that the second row has all 1's in the first half and all -1's in the second half. The first two rows now look like this:

$$\begin{array}{cccccccc} 1 & 1 & \dots & 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 & -1 & \dots & -1 \end{array}$$

By switching the columns to manipulate the first two rows none of the properties of the matrix have been changed and the inner product of each row with another will still be 0.

Consider the inner product of row i, $i \neq 1, 2$, with row 2. The first half of row i will have u entries that are 1 and $n/2 - u$ that are -1, in the second half it will have v 1's and $n/2 - v$ -1's. Now, because the inner product of row i and row 2 must be 0, exactly half of the entries of row i must be 1. Therefore,

$$u + v = \frac{n}{2}. \tag{15}$$

We can now give the equation to compute the inner product of row 2 with row i,

$$u - (\frac{n}{2} - u) - v + (\frac{n}{2} - v) = 0. \tag{16}$$

From here it follows that $u - v = 0$. After an application of equation (15) we have $2u = n/2$, which implies

$$n = 4u. \tag{17}$$

This proves the first part of the theorem. Moreover, $n/2 = 2u$ entries are 1 and the same number are -1, which proves the second part of the theorem. Finally, it is clear the second and i^{th} rows in our construction have u columns with a 1 in common and the same can be shown for any pair of rows by interchanging a number of columns to make this clear.

Q.E.D.

We are now ready to apply this knowledge of Hadamard matrices to prove one of the key results about the existence of Hadamard designs.

Theorem 3.5 For arbitrarily large values of m, and in particular for $m = 2^k$, $k \geq 1$, a Hadamard design of dimension m exists.

Proof [**?**] Given a normalized Hadamard matrix, we can define a $\{v, k, \lambda\}$ symmetric design. This is done by deleting the first row and column from the matrix. Then, every position where there is a -1 is changed to a 0, creating an incidence matrix, $\mathbf{A}$, of a $\{v, k, \lambda\}$ design. Now, to show this design will always be a Hadamard design, notice that by theorem 3.4 $\mathbf{A}$ will have $4m - 1$ rows and $4m - 1$ columns. Thus, $b = v = 4m - 1$. Moreover, because one 1 has been removed from every row and column of the Hadamard matrix, theorem 3.4 implies every row and column of the matrix $\mathbf{A}$ will have $2m - 1$ 1's. So, $k = r = 2m - 1$. Finally, notice that because $\mathbf{A}$ has one less column of 1's than the previous Hadamard matrix, every pair of rows in $\mathbf{A}$ will have exactly $m-1$ columns with a common 1. Hence, $\mathbf{A}$ will yield a $\{4m - 1, 2m - 1, m - 1\}$ symmetric design, a Hadamard design of dimension m.

Now to prove the theorem we will show how to construct a normalized Hadamard matrix of order $4m$ for some arbitrarily large m. Let $\mathbf{H}$ be a Hadamard matrix of order n and define $\mathbf{K}$ as follows:

$$\mathbf{K} = \begin{bmatrix} \mathbf{H} & \mathbf{H} \\ \mathbf{H} & -\mathbf{H} \end{bmatrix}.$$

Clearly, if **H** is a Hadamard matrix of order n, **K** will be a Hadamard matrix of order $2n$. All the entries of **K** will be 1's and -1's and it is easy to show that the inner product of a row with itself will be $2n$ and the inner product of two different rows will be zero. Furthermore, if **H** is a normalized Hadamard matrix, it is clear that **K** will also be a normalized Hadamard matrix. This shows the existence of Hadamard matrices of arbitrarily large orders and, in particular, for $n = 2^p$ where $p \geq 1$. We have previously shown that a Hadamard matrix of order $4m$ will correspond to a Hadamard design and from theorem 3.4 we have $n = 4m$ for some m. Thus, we can say that a Hadamard design exists for $4m = 2^p$, where $m \geq 2$, or equivalently, a Hadamard design of dimension m exists for $m = 2^k$, where $k \geq 1$.

Q.E.D.

4 Resolvable BIBDs

We have already discussed two classes of BIBDs, we now look to a third class, *resolvable* BIBDs. In order to understand the concept of a resolvable BIBD, we must first define what is known as a *parallel class*.

Definition If the pair $(V, \mathcal{B})$ is a BIBD, a *parallel class* (or *resolution class*) in $(V, \mathcal{B})$ is a set of blocks in $\mathcal{B}$ that partition the point set V. A *partial parallel class* is a set of blocks that contain no element of V more than once.

Definition A *resolvable* BIBD (or simply a *resolvable design*) is a BIBD whose blocks may be partitioned into parallel classes. The notation *RBIBD* is also commonly used.

Example The following is an example of a $\{9, 3, 1\}$ RBIBD over the point set $\{1, 2, \ldots, 9\}$ (each column represents a parallel class).

$$\begin{array}{ccc} \{1,2,3\} & \{1,4,7\} & \{1,6,8\} \\ \{4,5,6\} & \{2,5,8\} & \{2,4,9\} \\ \{7,8,9\} & \{3,6,9\} & \{3,5,7\} \end{array}$$

Definition A *near resolvable design* is a BIBD with the property that the blocks may be partitioned into partial parallel classes, each of which lacks a single point. Furthermore, each point of the design is missing in exactly one partial parallel class. The parameters of a near resolvable design will be $\{v, k, k-1\}$.

Example Here is an example of a $\{7, 3, 2\}$ near resolvable design over the set $\{0, 1, \ldots, 6\}$ (each column is a partial parallel class),

$$\begin{array}{rccccccc} \textit{missing point}: & \{0\} & \{1\} & \{2\} & \{3\} & \{4\} & \{5\} & \{6\} \\ \textit{blocks}: & \{1,2,4\} & \{2,3,5\} & \{3,4,6\} & \{4,5,0\} & \{5,6,1\} & \{6,0,2\} & \{0,1,3\} \\ & \{3,5,6\} & \{4,6,0\} & \{5,0,1\} & \{6,1,2\} & \{0,2,3\} & \{1,3,4\} & \{2,4,5\} \end{array}$$

The following theorem is similar to Fisher's inequality, yet is specific to RBIBDs.

Theorem 4.1 (*Bose's Condition*) If a $\{v, k, \lambda\}$ RBIBD exists, then $b \geq v+r-1$.

4.1 Kirkman Triple Systems

Suppose you have 15 schoolgirls, and each day the girls are to walk to and from school in groups of three. Is it possible to arrange the girls in groups of three so that no pair of girls walk with eachother twice over a period of one week? This question was posed by Kirkman in 1850 and is known as the Kirkman schoolgirl problem.

This question is put more simply in terms of resolvable BIBDs: how many resolution classes exist for a $\{15, 3, 1\}$ resolvable design? Kirkman found a solution with seven resolution classes and, in fact, exactly seven distinct solutions with seven resolution classes have been found. Here is a table including two of the seven solutions to the problem. The girls are represented by the set $\{a, b, c, \ldots, o\}$ and blocks are signified by the rows of three elements.

	Day Number						
	1	2	3	4	5	6	7
Solution 1	a,b,c	a,h,i	a,j,k	a,d,e	a,f,g	a,l,m	a,n,o
	d,j,n	b,e,g	b,m,o	b,l,n	b,h,j	b,i,k	b,d,f
	e,h,m	c,m,n	c,e,f	c,i,j	c,l,o	c,d,g	c,h,k
	f,i,o	d,k,o	d,h,l	f,k,m	d,i,m	e,j,o	e,i,l
	g,k,l	f,j,l	g,i,n	g,h,o	e,k,n	f,h,n	g,j,m
Solution 2	a,b,c	a,h,i	a,j,k	a,d,e	a,f,g	a,l,m	a,n,o
	d,j,n	b,e,g	b,m,o	b,i,k	b,l,n	b,d,f	b,h,j
	e,h,m	c,m,n	c,e,f	c,l,o	c,h,k	c,i,j	c,d,g
	f,i,o	d,k,o	d,h,l	f,h,n	d,i,m	e,k,n	e,i,l
	g,k,l	f,j,l	g,i,n	g,j,m	e,j,o	g,h,o	f,k,m

Table 1: Two Distinct Solutions to the Kirkman Schoolgirl Problem[**?**]

As the first to question the existence of designs of this type, RBIBDs with $k = 3$ and $\lambda = 1$ have been named for Kirkman.

Definition A *Kirkman triple system* (*KTS*) of order v is a $\{v, 3, 1\}$ RBIBD together with a resolution of its blocks into parallel classes.

The following theorem follows from Kirkman's theorem of 1847 and some further analysis, but will be given without proof.

Theorem 4.2 A KTS of order v exists if and only if $v \equiv 3 \,(mod\, 6)$.

5 Building New BIBDs from Existing Symmetric Designs

There are a number of easy constructions which can create new BIBDs once given the existence of a symmetric design. Two such constructions will be examined here, but first we must present the following theorem.

Theorem 5.1 For every symmetric BIBD, any two blocks have exactly λ elements in common.

Proof [**?**] Let $\mathbf{A}$ be an incidence matrix of a symmetric design (this will be a $v \times v$ incidence matrix). We know the following about $\mathbf{A}$:
(1) Any row of $\mathbf{A}$ contains k 1's,
(2) Any column of $\mathbf{A}$ contains k 1's, and
(3) Any pair of columns of $\mathbf{A}$ have 1's in exactly λ rows.
For the proof of this theorem, we will show that:
(4) Any pair of rows of $\mathbf{A}$ have 1's in common in exactly λ columns.

Let $\mathbf{J}$ be the $v \times v$ matrix of all 1's. With this in mind it is clear that every position in the matrix $\mathbf{AJ}$ will be the sum of the entries along any row of $\mathbf{A}$. Therefore, we have $\mathbf{AJ} = k\mathbf{J}$. Previously we have also shown in the proof of Fisher's inequality that theorem 1.3 implies $\det \mathbf{A} \neq 0$. Hence, we know that $\mathbf{A}^{-1}$ exists. The matrix $\mathbf{A}^{-1}$ can now be used to show that if $\mathbf{AJ} = k\mathbf{J}$, then

$$\mathbf{A^{-1}AJ} = k\mathbf{A^{-1}J} \quad or \quad k^{-1}\mathbf{J} = \mathbf{A^{-1}J}. \tag{18}$$

From theorem 1.3 we have the relation, $\mathbf{A}\mathbf{A}^T = (r-\lambda)\mathbf{I} + \lambda\mathbf{J}$ for any incidence matrix $\mathbf{A}$. With the above results, however, the following is also true:

$$\begin{aligned} \mathbf{A}^{-1}\mathbf{A}\mathbf{A}^T\mathbf{A} &= \mathbf{A}^{-1}\left((k-\lambda)\mathbf{I} + \lambda\mathbf{J}\right)\mathbf{A}, \quad or \\ \mathbf{A}^T\mathbf{A} &= (k-\lambda)\mathbf{I} + \lambda\mathbf{A}^{-1}\mathbf{J}\mathbf{A} \end{aligned}$$

At this point we may apply equation (18) to come up with this result:

$$\mathbf{A}^T\mathbf{A} = (k-\lambda)\mathbf{I} + \lambda k^{-1}\mathbf{J}\mathbf{A} \tag{19}$$

A number of applications of linear algebra on this result will now finish the proof.

$$\begin{aligned} \mathbf{A}^T\mathbf{A}\mathbf{A}^{-1}\mathbf{J} &= ((k-\lambda)\mathbf{I} + \lambda k^{-1}\mathbf{J}\mathbf{A})\mathbf{A}^{-1}\mathbf{J}, \quad or \\ \mathbf{A}^T\mathbf{J} &= ((k-\lambda)A^{-1}\mathbf{J} + k^{-1}\lambda\mathbf{J}\mathbf{J} \end{aligned}$$

Notice that the inner product of any two rows of $\mathbf{J}$ will yield the sum of the entries along one row of $\mathbf{J}$. Therefore, $\mathbf{JJ} = v\mathbf{J}$ because $\mathbf{J}$ is a $v \times v$ matrix. We now apply this fact and equation (18) to above equation.

$$\mathbf{A}^T\mathbf{J} = k^{-1}(k-\lambda)\mathbf{J} + k^{-1}\lambda v\mathbf{J}$$

Notice that $\mathbf{J}^T = \mathbf{J}$ because $\mathbf{J}$ is a symmetric matrix. With this in mind, we take the transpose of each side of the above equation to get

$$\mathbf{JA} = k^{-1}(k + \lambda v - \lambda)\mathbf{J} = k^{-1}(k + \lambda(v-1))\mathbf{J}. \tag{20}$$

From equation (10) we have $\lambda(v-1) = k(k-1)$. Hence,

$$\mathbf{JA} = k^{-1}(k + k(k-1))\mathbf{J}, \quad \textit{or} \tag{21}$$

$$\mathbf{JA} = k\mathbf{J} = \mathbf{AJ} \tag{22}$$

which implies condition (4) from the beginning of the proof.

Q.E.D.

We may now use this result to present the following constructions. Note that for any two sets U and V, the notation $U - V$ will denote the set $U \cap V^c$, where V^c denotes the complement of the set V.

Theorem 5.2 Let $(V, \mathcal{B})$ be a symmetric BIBD with $\mathcal{B} = \{B_1, B_2, \ldots, B_v\}$ and $V = \{x_1, \ldots, x_v\}$. Then for any i,

$$B_1 - B_i,\ B_2 - B_i, \ldots,\ B_{i-1} - B_i,\ B_{i+1} - B_i, \ldots,\ B_v - B_i$$

are the blocks of a $\{v-k, v-1, k-\lambda, k, \lambda\}$ BIBD over the point set $X - B_i$.

Proof [**?**] Clearly, removing the elements of one block will remove k elements from the set. Therefore, there $v - k$ elements remain in the point set. It is also quite clear that the removal of one block leaves $v - 1$ remaining blocks. By theorem 5.1, every block has λ elements in common. Thus, the construction will leave $k - \lambda$ elements in each block. The remaining elements of the design will be unaffected by the construction. Each remaining element was found in k blocks and will still be found in k blocks. Furthermore, each pair of remaining elements was found in λ blocks together and this value will also remain unchanged. Hence, it is clear a new BIBD has been created through this construction.

Q.E.D.

The design resulting from this previous construction is known as a *residual* design.

Theorem 5.3 Let $(V, \mathcal{B})$ be a symmetric BIBD with $\mathcal{B} = \{B_1, B_2, \ldots, B_v\}$ and $V = \{x_1, \ldots, x_v\}$. Then for any i,

$$B_1 \cap B_i,\ B_2 \cap B_i, \ldots,\ B_{i-1} \cap B_i,\ B_{i+1} \cap B_i, \ldots,\ B_v \cap B_i$$

are the blocks of a $\{k, v-1, \lambda, k-1, \lambda-1\}$ BIBD over the point set B_i.

Proof [**?**] This construction will clearly yield a k-element point set. Also, the

deletion of one block from the design trivially implies the remaining number of blocks will be $v - 1$ and an application of theorem 5.1 implies the number of elements in each of these blocks will be λ. In the original design, an element of the block B_i could be found in k different blocks:

$$B_{j_1}, B_{j_2}, \ldots, B_{j_{k-1}}, B_i.$$

This same element will now be found in only $k - 1$ blocks:

$$B_{j_1} \cap B_i, B_{j_2} \cap B_i, \ldots, B_{j_{k-1}} \cap B_i.$$

Similarly, a pair of elements in the block B_i was originally found in λ blocks:

$$B_{j_1}, B_{j_2}, \ldots, B_{j_{\lambda-1}}, B_i.$$

Now the same pair will be found in the following $\lambda - 1$ blocks:

$$B_{j_1} \cap B_i, B_{j_2} \cap B_i, \ldots, B_{j_{\lambda-1}} \cap B_i.$$

Q.E.D.

References