Honam Mathematical J. 24(2002), No. 1,pp. 109–119

SUFFICIENT CONDITIONS AND CONSTRUCTION OF SYMMETRIC BIBD

SUNGKWON KANG*, YOON-TAE JUNG, AND JU-HYUN LEE

Dept. of Mathematics.
Chosun University, Kwangju 501-759, Korea,
E-mail: sgkang@mail.chosun.ac.kr
E-mail: ytajung@mail.chosun.ac.kr
E-mail: jh0911@hanmail.net.

Abstract Some sufficient conditions on the existence and uniqueness of certain symmetric balanced incomplete block design are introduced. Also, a construction algorithm for the design and some examples are presented. The algorithm is developed based on the construction of subspaces of the three-dimensional vector space over a field.

1. Introduction

The theory of design of experiments came into being largely through the work of R. A. Fisher and F. Yates in the early 1930's[1]. They were motivated by questions of design of careful field experiments in agriculture. Although the applicability of this theory is now very widespread, much of the terminology still bears the stamp of its origins. Consider an agricultural experiment. Suppose it is desired to compare the yield of v different varieties of grain. It is quite possible that there would be an interaction between the environment (type of soil, rainfall, drainage, etc.) and the variety of grain which would alter the yields. So, b blocks (sets of experimental plots) are chosen in which the environment is fairly consistent throughout the block. In other types of experiments in which the environment might not be a factor, blocks

Received May 6, 2002.
1991 AMS Subject Classification : 51E20.
Key words and phrases : Balanced incomplete block design(BIBD), symmetric BIBD, projective plane.
*This work was supported by Chosun University Research Funds 2001.

could be distinguished as plots which receive a particular treatment (say, are given a particular type of fertilizer). In this way, the classification of the experimental plots into blocks and varieties can be used whenever there are two factors which may influence yield. The obvious technique of growing every variety in a plot in every block may, for large experiments, be too costly or impractical. To deal with this, one would use smaller blocks which did not contain all of the varieties. Now the problem is one of comparison, to minimize the effects of chance due to incomplete blocks, we would want to design the blocks so that the probability of two varieties being compared (i.e., are in the same block) is the same for all pairs. This property would be called *balance* in the design. Statistical techniques, in particular, Analysis of Variance, could then be used to reach conclusions about the experiment[1].

Generation of balanced incomplete block design(BIBD), a special case of block design, is a standard combinatorial problem from design theory, originally used in the design of statistical experiments but since finding other applications such as cryptography. Usually, symmetric BIBDs are used in conference key distribution system[6] and visual cryptographic schemes[3,4]. A conference key distribution system is a scheme to generate a conference key, and then to distribute this key to only paticipants attending at the conference in order to communicate with each other securely. Visual cryptographic scheme is a simple method which can be directly decoded the secret information in human visual system without performing any cryptographic computation. The visual cryptographic schemes using BIBD is better than another ones in relative contrast[4].

One of the main goals of combinatorial design theory is to determine necessary and sufficient conditions for the existence of a BIBD. This is a very difficult problem in general. However, there are many known constructions for some classes of BIBDs with small number of objects, as well as some other necessary conditions[2]. But, there is no known sufficient condition on the existence of a BIBD. Also, it is not easy to construct a BIBD with large(or arbitrary) number of objects. In this paper, we present some sufficient conditions on the existence and unique-

ness of certain symmetric BIBDs. Also, we introduce a practical construction algorithm for a symmetric BIBD in projective plane.

2. Symmetric BIBD and projective plane

Codewords are generated by employing a block design among methods of generation of error-correcting codes. By a block design we mean a selection of the subsets of a given set such that some prescribed conditions are satisfied. In some designs, the elements in each of the subsets are also to be ordered in a certain way. A BIBD is defined as follows[6].

Let $X = \{x_1, x_2, \cdots, x_v\}$ be a set of v objects. A (b, v, r, k, λ)-BIBD of X is a collection of b blocks $B_1, B_2, \cdots, B_b$ which are subsets of X such that the following conditions are satisfied:

(1) Each block contains k objects.
(2) Each object appears in exactly r blocks.
(3) Every two objects appears simultaneously in exactly λ blocks.
(4) $k < v$.

Property (3) is the "balance" property. A BIBD is called an "incomplete block" design because of (4). Also, note a BIBD may contain "repeated blocks" if $\lambda > 1$, which is why we refer to a collection of blocks rather than a set[5]. Since a BIBD is characterized by the five parameters b, v, r, k, and λ, it is also called a (b, v, r, k, λ)-*configuration*. It is known that $bk = vr$ and $r(k-1) = \lambda(v-1)$ in a BIBD[2].

A (b, v, r, k, λ)-BIBD can be described by the *incidence matrix* M which is useful for computer programs. It is a $b \times v$ *zero-one matrix*, i.e., its entries are 0 and 1. The rows and columns of the matrix correspond to the blocks and the objects, respectively. The entry in the $i-th$ row and the $j-th$ column of M is 1 if the block B_i contains the object x_j and is 0 otherwise.

Let I_b be the $b \times b$ identity matrix, J_b the $b \times b$ matrix in which every entry is 1, and u_b(or u_v) be the vector of length b(or v) in which every coordinate is 1. For a matrix M, let M^T be the transpose of M. Then we have the following theorem[2].

THEOREM 2.1. *Let M be a $b \times v$ zero-one matrix. Then M is*

the incidence matrix of a (b, v, r, k, λ)-BIBD if and only if

$$MM^T = \lambda J_b + (r - \lambda) I_b \quad \text{and} \quad u_b M = k u_v.$$

In some special cases of a BIBD, the number of blocks is the same as that of objects. A (b, v, r, k, λ)-BIBD is said to be a *symmetric* (v, k, λ)-BIBD if $b = v$ and $r = k$. The following theorem gives the necessary conditions for the existence of symmetric BIBD with given parameters v, k, and λ[2].

THEOREM 2.2. *(Bruck-Ryser-Chowla Theroem) Suppose there exists a symmetric (v, k, λ)-BIBD. If v is even, then it must be the case that $k - \lambda$ is a perfect square ; and if v is odd, then there must exist integers x, y, and z (not all 0) such that*

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

A *finite projective plane of order* q with $q > 0$ is a collection of $q^2 + q + 1$ lines and $q^2 + q + 1$ points such that

(1) every line contains $q + 1$ points,
(2) every point is on $q + 1$ lines,
(3) any two distinct lines intersect at exactly one point, and
(4) any two distinct points lie on exactly one line(see [7]).

From the definition of finite pojective plane, it becomes a symmetric $(q^2 + q + 1, q + 1, 1)$-BIBD since it has $q^2 + q + 1$ objects, each block contains exactly $q+1$ objects, and every pair of distinct objects is contained in exactly one block.

A finite projective plane exists when the order q is a power of a prime, i.e., $q = p^n$ for $n \geq 1$ and prime p ([2,7]). It is conjectured that these are the only possible projective planes, but proving this remains one of the most important unsolved problems in combinatorics. The first few orders which are powers of primes are 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, $\cdots$. The first few orders which are not of this form are 6, 10, 12, 14, 15, $\cdots$. It is known that there are no finite projective planes of order 6 and 10 ([2,7]).

3. Sufficient conditions of symmetric BIBD

In this section, we present some sufficient conditions.

THEOREM 3.1. *For any v and $k \geq 2$, there exists a symmetric (v, k, λ)-BIBD.*

Proof. Let

$$\begin{aligned}
B_1 &= \{x_1, x_2, \cdots, x_{v-2}, x_{v-1}\}.\\
B_2 &= \{x_1, x_2, \cdots, x_{v-3}, x_{v-2}, x_v\}.\\
&\vdots\\
B_{v-1} &= \{x_1, x_3, x_4, \cdots, x_{v-1}, x_v\}.\\
B_v &= \{x_2, x_3, \cdots, x_{v-1}, x_v\}.
\end{aligned}$$

Then it becomes a symmetric (v, k, λ)-BIBD with $k = v - 1$ and $\lambda = v - 2$. Thus, there always exists a symmetric (v, k, λ)-BIBD for any v and $k \geq 2$. The incidence matrix becomes

$$\begin{array}{c} \\ B_1 \\ B_2 \\ B_3 \\ \vdots \\ B_{v-2} \\ B_{v-1} \\ B_v \end{array}
\begin{array}{c}
\begin{array}{ccccccc} x_1 & x_2 & x_3 & \cdots & x_{v-2} & x_{v-1} & x_v \end{array}\\
\left(\begin{array}{ccccccc}
1 & 1 & 1 & \cdots & 1 & 1 & 0\\
1 & 1 & 1 & \cdots & 1 & 0 & 1\\
1 & 1 & 1 & \cdots & 0 & 1 & 1\\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots\\
1 & 1 & 0 & \cdots & 1 & 1 & 1\\
1 & 0 & 1 & \cdots & 1 & 1 & 1\\
0 & 1 & 1 & \cdots & 1 & 1 & 1
\end{array}\right)
\end{array}.$$

□

We call the BIBD in Theroem 3.1 the *trivial symmetric BIBD.*

THEOREM 3.2. *If $v = p^m + 1$ for a prime p and $m \geq 1$, there is the only one symmetric (v, k, λ) -BIBD. It is the trivial symmetric $(v, v-1, v-2)$-BIBD.*

Proof. Case 1 : $m = 1$.
Suppose that another symmetric (v, k, λ)-BIBD, non-trivial BIBD, exists. Then $k < p$ or $k - 1 < p$ since $k < v$. From the property of BIBD described in Section 2, $r = k$ and $v = p + 1$. $k(k-1) = \lambda p$.

Thus p divides either k or $k-1$ since p is a prime number. If p divides k, $2 \leq k < v-1$ since the given BIBD is not trivial and $k < v$. Therefore, $k < p$, which is a contradiction due to the assumption that p divides k. Similarly, if p divides $k-1$. we have a contradiction.

Case 2 : $m \geq 2$.

Suppose that another symmetric (v, k, λ)-BIBD exists. Then $k < p^m$ or $k-1 < p^m$. Hence, $k(k-1) = \lambda p^m$. Since p is prime, p divides either k or $k-1$. If p divides k, $k = p^l$ for some l, $1 \leq l < m$. Thus $k-1 = \lambda p^{m-l}$. Hence, p divides $k-1$. Since p cannot divide both k and $k-1$, we have a contradiction. Similarly, if p divides $k-1$, then we have a contradiction. Thus, the only one symmetric BIBD exists. □

From the fact that $k(k-1) = \lambda(v-1)$ in symmetric (v, k, λ)-BIBD, we have the following corollary.

COROLLARY 3.3. *If $v = pq + 1$, where p and q are distinct prime numbers $(p, q \geq 3)$, there is no symmetric (v, k, λ)-BIBD for any odd number λ.*

EXAMPLE 3.4. From the above theorems, we can classify symmetric (v, k, λ)-BIBD for each v.

(1) For primes $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, \cdots$,

$$\begin{aligned}
&\text{if } v = p+1, \quad v = 3, 4, 6, 8, 12, 14, 18, 20, 24, \cdots, \\
&\text{if } v = p^2+1, \quad v = 5, 10, 26, 50, \cdots, \\
&\text{if } v = p^3+1, \quad v = 9, 28, 126, \cdots, \\
&\text{if } v = p^4+1, \quad v = 17, 82, \cdots, \\
&\qquad \vdots
\end{aligned}$$

These cases have the unique symmetric with $k = v-1$ and $\lambda = v-2$.

(2) If we consider another BIBDs, for example, in case of $v = 7$, it has three symmetric BIBDs, that is, (7,3,1)-BIBD known as finite projective plane of order 2, (7,4,2)-BIBD, and the trivial (7,6,5)-BIBD. For the case of $v = 11$, it has (11,5,2)-BIBD and the trivial

(11,10,9)-BIBD. For other v, we have the following symmetric BIBDs:

$$\begin{aligned} &v = 13, \quad r = 4, \quad \lambda = 1, \\ &v = 15, \quad r = 7, \quad \lambda = 3, \\ &v = 16, \quad r = 6, \quad \lambda = 2, \\ &v = 19, \quad r = 9, \quad \lambda = 4, \\ &v = 21, \quad r = 5, \quad \lambda = 1, \\ &\quad \vdots \end{aligned}$$

and the trivial BIBD. Another cases may exist for each v.

4. Construction algorithm

To develop our algorithm for constructing the symmetric $(q^2 + q + 1, q + 1, 1)$- BIBD known as projective plane of order q, consider a field $\mathbb{Z}_q = \{0, 1, \cdots, q-1\}$ of order q. Then, in case of prime p, the 3-dimensional vector space V over $\mathbb{Z}_q$ is $(\mathbb{Z}_q)^3 = \{(a, b, c) | a, b, c \in \mathbb{Z}_q\}$. We construct all the 1-dimensional and the 2-dimensional subspaces of V. It is begun by finding bases of 1-dimensional and 2-dimensional subspaces of V as following.

Step 1. Construction of all 1-dimensional subspaces of V.

(1) $x_1 =< (0,0,1) >= \{a(0,0,1) | a \in \mathbb{Z}_q\}$.

(2) For all $i = 0, 1, \cdots, q-1$,
$x_{i+2} =< (0,1,i) >= \{a(0,1,i) \bmod q | a \in \mathbb{Z}_q\}$.

(3) For all $i, j = 0, 1, \cdots, q-1$,
$x_{q(i+1)+(j+2)} =< (1,i,j) >= \{a(1,i,j) \bmod q | a \in \mathbb{Z}_q\}$.

Then each x_i becomes a 1-dimensional subspace of V.
Let $X = \{x_1, x_2, \cdots, x_{q^2+q+1}\}$.
Here, $<$, $>$ denotes a generator.

Step 2. Construction of all 2-dimensional subspaces of V.

(1) $B_1 =< (0,0,1) > + < (0,1,0) >$
$= \{a(0,0,1) + b(0,1,0) | a, b \in \mathbb{Z}_q\}$.

(2) For all $i = 0, 1, \cdots, q-1$,
$B_{i+2} =< (0,0,1) > + < (1,i,0) >$
$= \{a(0,0,1) + b(1,i,0) \bmod q | a, b \in \mathbb{Z}_q\}$.

(3) For all $i, j = 0, 1, \cdots, q-1$,
$B_{q(i+1)+(j+2)} =< (0,1,i) > + < (1,0,j) >$
$= \{a(0,1,i) + b(1,0,j) \bmod q | a, b \in \mathbb{Z}_q\}$.

Let $\mathcal{B} = \{B_1, B_2, \cdots, B_{q^2+q+1}\}$.

Step 3. Construction of blocks.

For $i = 1, \cdots, q^2+q+1$, and for each $B_i \in \mathcal{B}$, let

$$A_{B_i} = \{x \in X | x \subseteq B_i\}.$$

That is, the q^2+q+1 blocks A_{B_i} are represented by the elements of X.

Step 4. Find the incidence matrix.

For $i, j = 1, 2, \cdots, q^2+q+1$, the incidence matrix $M = (m_{ij})$ becomes

$$m_{ij} = \begin{cases} 1, & \text{if } x_j \in A_{B_i}, \\ 0, & \text{if } x_j \notin A_{B_i}. \end{cases}$$

Step 5. Test.

From Theorem 2.1 and the definition of symmetric (v, k, λ)-BIBD, it is easy to see that the incidence matrix M in Step 4 satisfies the following :

$$MM^T = \lambda J_v + (k-\lambda) I_v \quad \text{and} \quad u_v M = k u_v,$$

where $v = q^2+q+1$, $k = q+1$, $\lambda = 1$, and J_v, I_v, and u_v are defined as in the above of Theorem 2.1.

From Step 1, $|X| = 1+q+q^2$ and $|x| = q$ for $x \in X$, i.e., the BIBD has q^2+q+1 objects. Also, from Step 2 and Step 3, $|\mathcal{B}| = 1+q+q^2$ and $|B| = q^2$ for $B \in \mathcal{B}$, i.e., the BIBD has q^2+q+1 bolcks. By the two facts, we know that the number of blocks is the same as that of objects. Also, from Step 3, each block A_{B_i} contains exactly $q+1$ objects. From Steps 1, 2, and 3, there is a unique 2-dimensional subspace containing the 1-dimensional

subspaces x_i and x_j for $i \neq j$. This subspace determines the unique block containing the objects x_i and x_j for $i \neq j$. Therefore, from Steps 1-5, we have the symmetric $(q^2+q+1, q+1, 1)$-BIBD.

The following example is computed under the Matlab environment.

EXAMPLE. Let $q = 3$. Then $\mathbb{F}_3 = \mathbb{Z}_3$. Let the three elements in $\mathbb{F}_3$ be 0, 1, and 2. The 3-dimensional vector space V consists of all the 27 vectors $(0,0,0)$, $(0,0,1)$, $(0,0,2)$, $(0,1,0)$, $(0,1,1)$, $\cdots$, $(2,2,2)$. The 1-dimensional subspaces of V are as follows :

$$x_1 = \{(0,0,0),(0,0,1),(0,0,2)\}, x_2 = \{(0,0,0),(0,1,0),(0,2,0)\},$$
$$x_3 = \{(0,0,0),(0,1,1),(0,2,2)\}, x_4 = \{(0,0,0),(0,1,2),(0,2,1)\},$$
$$x_5 = \{(0,0,0),(1,0,0),(2,0,0)\}, x_6 = \{(0,0,0),(1,0,1),(2,0,2)\},$$
$$x_7 = \{(0,0,0),(1,0,2),(2,0,1)\}, x_8 = \{(0,0,0),(1,1,0),(2,2,0)\},$$
$$x_9 = \{(0,0,0),(1,1,1),(2,2,2)\}, x_{10} = \{(0,0,0),(1,1,2),(2,2,1)\},$$
$$x_{11} = \{(0,0,0),(1,2,0),(2,1,0)\},$$
$$x_{12} = \{(0,0,0),(1,2,1),(2,1,2)\},$$
$$x_{13} = \{(0,0,0),(1,2,2),(2,1,1)\}.$$

The 2-dimensional subspaces of V are as follows:

$$B_1 = \{(0,0,0),(0,1,0),(0,2,0),(0,0,1),(0,1,1),$$
$$(0,2,1),(0,0,2),(0,1,2),(0,2,2)\},$$
$$B_2 = \{(0,0,0),(1,0,0),(2,0,0),(0,0,1),(1,0,1),$$
$$(2,0,1),(0,0,2),(1,0,2),(2,0,2)\},$$
$$B_3 = \{(0,0,0),(1,1,0),(2,2,0),(0,0,1),(1,1,1),$$
$$(2,2,1),(0,0,2),(1,1,2),(2,2,2)\},$$
$$B_4 = \{(0,0,0),(1,2,0),(2,1,0),(0,0,1),(1,2,1),$$
$$(2,1,1),(0,0,2),(1,2,2),(2,1,2)\},$$
$$B_5 = \{(0,0,0),(1,0,0),(2,0,0),(0,1,0),(1,1,0),$$
$$(2,1,0),(0,2,0),(1,2,0),(2,2,0)\},$$
$$B_6 = \{(0,0,0),(1,0,1),(2,0,2),(0,1,0),(1,1,1),$$
$$(2,1,2),(0,2,0),(1,2,1),(2,2,2)\}.$$

$$B_7 = \{(0,0,0),(1,0,2),(2,0,1),(0,1,0),(1,1,2),$$
$$(2,1,1),(0,2,0),(1,2,2),(2,2,1)\},$$
$$B_8 = \{(0,0,0),(1,0,0),(2,0,0),(0,1,1),(1,1,1),$$
$$(2,1,1),(0,2,2),(1,2,2),(2,2,2)\},$$
$$B_9 = \{(0,0,0),(1,0,1),(2,0,2),(0,1,1),(1,1,2),$$
$$(2,1,0),(0,2,2),(1,2,0),(2,2,1)\},$$
$$B_{10} = \{(0,0,0),(1,0,2),(2,0,1),(0,1,1),(1,1,0),$$
$$(2,1,2),(0,2,2),(1,2,1),(2,2,0)\},$$
$$B_{11} = \{(0,0,0),(1,0,0),(2,0,0),(0,1,2),(1,1,2),$$
$$(2,1,2),(0,2,1),(1,2,1),(2,2,1)\},$$
$$B_{12} = \{(0,0,0),(1,0,1),(2,0,2),(0,1,2),(1,1,0),$$
$$(2,1,1),(0,2,1),(1,2,2),(2,2,0)\},$$
$$B_{13} = \{(0,0,0),(1,0,2),(2,0,1),(0,1,2),(1,1,1),$$
$$(2,1,0),(0,2,1),(1,2,0),(2,2,2)\}.$$

The 13 blocks are

$$A_{B_1} = \{x_1, x_2, x_3, x_4\}, \quad A_{B_2} = \{x_1, x_5, x_6, x_7\},$$
$$A_{B_3} = \{x_1, x_8, x_9, x_{10}\}, \quad A_{B_4} = \{x_1, x_{11}, x_{12}, x_{13}\},$$
$$A_{B_5} = \{x_2, x_5, x_8, x_{11}\}, \quad A_{B_6} = \{x_2, x_6, x_9, x_{12}\},$$
$$A_{B_7} = \{x_2, x_7, x_{10}, x_{13}\}, \quad A_{B_8} = \{x_3, x_5, x_9, x_{13}\},$$
$$A_{B_9} = \{x_3, x_6, x_{10}, x_{11}\}, \quad A_{B_{10}} = \{x_3, x_7, x_8, x_{12}\},$$
$$A_{B_{11}} = \{x_4, x_5, x_{10}, x_{12}\}, \quad A_{B_{12}} = \{x_4, x_6, x_8, x_{13}\},$$
$$A_{B_{13}} = \{x_4, x_7, x_9, x_{11}\}.$$

Thus, it becomes a finite projective plane of order 3, a symmetric (13,4,1)-BIBD.

References

[1] B. Cherowitzo, *Block Designs*, Preprint, Department of Mathematics, University of Colorado, 2001.

[2] D. R. Stinson, *An introduction to Combinatorial Designs*, Preprint, Department of Combinatorics and Optimization, University of Waterloo, 1999.

[3] A. Shamir, *How to share a secret*, Comm. of the ACM, **22(1)** (1979), 612-613.

[4] M. Naor and A. Shamir, *Visual cryptography*, Advances in Cryptology-EURO-CRYPTO'94 (1994), 1-12.

[5] D. R. Stinson, *Combinatorial Designs with Selected Applications, Lecture Notes*, Department of Computer Science, University of Manitoba, 1996.

[6] M. Oh and I. Chung, *The conference key distribution system employing a symmetric balanced incomplete block design*, Proceedings of the ICIM' 01 (2001), 231-235.

[7] C. W. H. Lam, *The Search for a Finite Projective Plane of order 10*, Preprint, Department of Computer Science, University of Concordia, 1990.