Splitting balanced incomplete block designs with block size 2×4*

MIAO LIANG

Department of Foundation
Suzhou Vocational University
Suzhou 215104, P.R.China

Beiliang Du

Department of Mathematics
Suzhou University
Suzhou 215006, P.R.China

Abstract

Splitting balanced incomplete block designs were first formulated by Ogata, Kurosawa, Stinson and Saido recently in the investigation of authentication codes. This article investigates the existence of splitting balanced incomplete block designs, i.e., $(v, 2k, \lambda)$-splitting BIBDs; we give the spectrum of $(v, 2 \times 4, \lambda)$-splitting BIBDs.

Keywords: splitting balanced incomplete design, k-splitting A-code

1 Introduction

In the investigation of authentication codes Ogata, Kurosawa, Stinson and Saido [4] found that splitting balanced incomplete block designs can be used to construct k-splitting A-codes, whose impersonation attack probabilities and substitution attack probabilities all achieve their information-theoretic lower bounds. Let v, b, l, u, k, λ be positive integers. A *splitting balanced incomplete block design*, i.e., a $(v, b, l = uk, \lambda)$-splitting BIBD is a pair $(X, \mathcal{B})$ where X is a v-set (of points) and $\mathcal{B}$ is a collection of b subsets of X (called blocks) with size l such that the following properties are satisfied:

*This work was supported by the National Natural Science Foundation of China (Grant No. 10571133).

Correspondence to: Beiliang Du, Department of Mathematics, Suzhou University, Suzhou 215006, China

1. every $B \in \mathcal{B}$ is expressed as a disjoint union of u subblocks of size k: $B = B_1 \cup B_2 \cup \cdots \cup B_u$,
2. for each pair set $\{x, y\}$ of X, there exist exactly λ blocks $B = B_1 \cup B_2 \cup \cdots \cup B_u$ such that $x \in B_i, y \in B_j (i \neq j)$.

The blocks of a $(v, b, l = uk, \lambda)$-splitting BIBD will be displayed in the form $\{a_1, a_2, \cdots, a_k; b_1, b_2, \cdots, b_k; \cdots; r_1, r_2, \cdots, r_k\}$ in this paper.

Let r be the number of blocks which contain a fixed point. We have the following expressions from [4].

$$r = \frac{\lambda(v-1)}{k(u-1)},$$
$$b = \frac{\lambda v(v-1)}{k^2 u(u-1)}.$$

There has been some work done on splitting balanced incomplete block designs (see, for example, Ogata, Kurosawa, Stinson and Saido [4] and Du [3] and [2]) and there are some known results on the existence of splitting balanced incomplete block designs. They gave the spectra of $(v, b, l = uk, \lambda)$-splitting BIBDs for $(u, k) = (2, 2), (2, 3)$ and $(3, 2)$. In this article, we shall be restricting our attention to splitting balanced incomplete block designs with $u = 2$ and we denote these briefly as $(v, 2k, \lambda)$-splitting BIBDs. We have the following necessary conditions for the existence of $(v, 2k, \lambda)$-splitting BIBDs.

Theorem 1.1 If there exists a $(v, 2k, \lambda)$-splitting $BIBD$, then

$$\lambda(v-1) \equiv 0 \ (mod\ k),$$
$$\lambda v(v-1) \equiv 0 \ (mod\ 2k^2).$$

For the case $k = 4$, the second author of this article in [2] obtained the following result.

Theorem 1.2 ([2]) There exists a $(v, 2 \times 4, 4)$-splitting BIBD for any $v \equiv 0 \pmod 8$ with $v \geq 12928$ and $v \equiv 1 \pmod 8$ with $v \geq 1801$.

This article investigates the existence of $(v, 2k, \lambda)$-splitting BIBDs; we give the spectrum of $(v, 2 \times 4, \lambda)$-splitting BIBDs. That is, our main objective in this article is to establish the following result.

Theorem 1.3 There exists a $(v, 2\times 4, \lambda)$-splitting $BIBD$ if and only if $\lambda(v-1) \equiv 0 \ (mod\ 4)$ and $\lambda v(v-1) \equiv 0 \ (mod\ 32)$.

2 Preliminaries

In this section we shall introduce some of the auxiliary designs and some of the fundamental results which will be used later. The reader is referred to [1] for more information on designs, and, in particular, group divisible designs and splitting group divisible designs.

Let K and M be sets of positive integers. A *group divisible design* (GDD) GD$[K, 1, M; v]$ is a triple $(X, \mathcal{G}, \mathcal{B})$ where X is a v-set (of points), $\mathcal{G}$ is a collection of nonempty subsets of X (called groups) with cardinality in M and $\mathcal{B}$ is a collection of subsets of X (called blocks) with cardinality at least two, in K, such that the following properties are satisfied.

1. $\mathcal{G}$ partition X,
2. no block intersects any group in more than one point,
3. each pair set $\{x, y\}$ of points not contained in a group is contained in exactly one block.

The group-type (or type) of the GDD $(X, \mathcal{G}, \mathcal{B})$ is the multiset of sizes $|G|$ of the group $G \in \mathcal{G}$ and we usually use the "exponential" notation for its description: group-type $1^i 2^j 3^k \cdots$ denotes i occurrences of groups of size 1, j occurrences of groups of size 2, and so on.

We need to establish some more notation. We shall denote by GD$[k, 1, m; v]$ a GD$[\{k\}, 1, \{m\}; v]$. We shall sometimes refer to a GD$[K, 1, M; v]$ $(X, \mathcal{G}, \mathcal{B})$ as a K-GDD.

For group divisible design, we have the following obvious result.

Lemma 2.1 There exists a 2-GDD of type $m^u n^1$ for any positive integers m and n.

For our purpose we need to introduce the concept of splitting group divisible design. Let K and M be sets of positive integers. A *splitting group divisible design* (splitting GDD) splitting GD$[K, 1, M; v]$ is a triple $(X, \mathcal{G}, \mathcal{B})$ where X is a v-set (of points), $\mathcal{G}$ is a collection of nonempty subsets of X (called groups) with cardinality in M and $\mathcal{B}$ is a collection of subsets of X (called blocks) with cardinality at least two, in K, such that the following properties are satisfied.

1. $\mathcal{G}$ partition X,
2. every $B \in \mathcal{B}$ is expressed as a disjoint union of u subblocks of size k: $B = B_1 \cup B_2 \cup \cdots \cup B_u$,
3. no block intersects any group in more than one subblock,
4. for each pair set $\{x, y\}$ of X not contained in a group, there exist exactly one block $B = B_1 \cup B_2 \cup \cdots \cup B_u$ such that $x \in B_i, y \in B_j (i \neq j)$.

The group-type (or type) of the splitting GDD is the same as that of the GDD. We shall sometimes refer to a splitting GD$[K, 1, M; v]$ $(X, \mathcal{G}, \mathcal{B})$ as a K-splitting GDD.

For splitting group divisible design, we can establish the following result which will be used later.

Lemma 2.2 There exists a 2×4-splitting GDD of type 4^u for any $u \geq 2$.

Proof The design we construct will have point set $X = Z_u \times \{1, 2, 3, 4\}$, $\mathcal{G} = \{G_1, G_2, \cdots, G_u\}$, where $G_i = \{i-1\} \times \{1, 2, 3, 4\}$. The block set $\mathcal{B}$ consists of the following blocks:

$$\{(i,1),(i,2),(i,3),(i,4);(i+j,1),(i+j,2),(i+j,3),(i+j,4)\},$$
$$0 \leq i \leq u-2,\ 1 \leq j \leq u-i-1.$$

It is easy to check that the $(X, \mathcal{G}, \mathcal{B})$ is a 2×4-splitting GDD of type 4^u.

∎

We shall illustrate the main technique that will be used throughout the remainder of the article, which is "Filling in Holes" construction. In applying the "Filling in Holes" construction, we require splitting GDD with groups not necessarily all of the same size. To get these splitting GDDs, we use the following construction which is a variant of "Weighting Construction" in [5].

Theorem 2.3 Suppose that there is a K-GDD of type $g_1 g_2 \cdots g_u$ and that for each $k \in K$ there is a $2k$-splitting GDD of type h^k. Then there is a $2k$-splitting GDD of type $(hg_1)(hg_2)\cdots(hg_u)$.

Proof We start with a K-GDD of type $g_1 g_2 \cdots g_u$ $(X, \mathcal{G}, \mathcal{B})$, where $\mathcal{G} = \{G_1, G_2, \cdots, G_u\}$, $|G_i| = g_i$. For each $B \in \mathcal{B}$, let $X_B = \{a_1, a_2, \cdots, a_k\}$ be the set of points of B, and $X_B^* = X_B \times \{1, 2, \cdots, h\}$. Let $(X_B^*, \mathcal{A}_B)$ be a $2k$-splitting GDD of type h^k. Then the design we construct will have point set

$$X^* = X \times \{1, 2, \cdots, h\}$$

and the block set

$$\mathcal{B}^* = \bigcup_{B \in \mathcal{B}} \mathcal{A}_B.$$

It is easy to check that the $(X^*, \mathcal{B}^*)$ is a $2k$-splitting GDD of type $(hg_1)(hg_2)\cdots(hg_u)$. ∎

Finally, as the "Filling in Holes" construction will generally involve adjoining more than one infinite point to a splitting GDD, we will require the notation of a splitting incomplete balanced incomplete block design. A *splitting incomplete balanced incomplete block design*, i.e., a $(v, w; 2k, \lambda)$-splitting IBIBD, is a triple $(X, Y, \mathcal{B})$ where X is a set of v elements, Y is a subset of X of size w (Y is called the hole) and $\mathcal{B}$ is a collection of subsets of X (blocks), such that

1. every $B \in \mathcal{B}$ is expressed as a disjoint union of 2 subblocks of size k: $B = B_1 \cup B_2$,
2. each pair set $\{x, y\}$ of Y do not occur in any block $B = B_1 \cup B_2$ such that $x \in B_i, y \in B_j (i \neq j)$,
3. each pair set $\{x, y\}$ of X occur together either in Y or in exactly λ blocks $B = B_1 \cup B_2$ such that $x \in B_i, y \in B_j (i \neq j)$,

We observe that the existence of a $(v, w; 2k, \lambda)$-splitting IBIBD is equivalent to the existence a $(v, 2k, \lambda)$-splitting BIBD when $w = 0$ and 1. Now we are in a position to give our main construction.

Construction 2.4 Suppose

1. there is a $2k$-splitting GDD of type $g_1g_2\cdots g_u$,
2. there is a $(g_i+w, w; 2k, \lambda)$-splitting IBIBD for each $i, 1 \le i < u$,where $w \ge 0$,
3. there is a $(g_u + w, 2k, \lambda)$-splitting BIBD.

Then there is a $(v, 2k, \lambda)$-splitting BIBD, where $v = w + \sum_{1\le i \le u} g_i$.

Proof We start with a $2 \times k$-splitting GDD of type $g_1g_2\cdots g_u$ $(X, \mathcal{G}, \mathcal{B})$, where $\mathcal{G} = \{G_1, G_2, \cdots, G_u\}$, $|G_i| = g_i$ for $1 \le i \le u$. For each G_i, $1 \le i < u$, let $(G_i \cup W, \mathcal{A}_i)$ be a $(g_i + w, w; 2k, \lambda)$-splitting IBIBD, where $|W| = w$ and $X \cap W = \emptyset$. Let $(G_u \cup W, \mathcal{A}_u)$ be a $(g_u + w, 2k, \lambda)$-splitting BIBD. Then the design we construct will have point set

$$X^* = X \cup W,$$

and the block set

$$\mathcal{B}^* = \mathcal{B}' \cup (\textstyle\bigcup_{1\le i\le u} \mathcal{A}_i),$$

where $\mathcal{B}'$ is a block collection obtained by repeating every block of $\mathcal{B}$ λ times. It is easy to check that the $(X^*, \mathcal{B}^*)$ is a $(v, 2k, \lambda)$-splitting BIBD.

∎

Especially, we have the following construction.

Lemma 2.5 Let m, n, and u be positive integers and $w \ge 0$. If there exist a $(4m + w, w; 2 \times 4, \lambda)$-splitting IBIBD and a $(4n + w, 2 \times 4, \lambda)$-splitting BIBD, then there exists a $(4mu + 4n + w, 2 \times 4, \lambda)$-splitting BIBD.

Proof We begin with a 2-GDD of type $m^u n^1$ (whose existence see Lemma 2.1) and give the points weight 4 and apply Theorem 2.3 to obtain a 2×4-splitting GDD of type $(4m)^u(4n)^1$. The input design we need 2×4-splitting GDD of type 4^2 comes from Lemma 2.2. The result then follows from Construction 2.4. ∎

We also need the following construction whose proof is easy.

Lemma 2.6 If there exist a $(v, 2\times k, \lambda_1)$-splitting BIBD and a $(v, 2\times k, \lambda_2)$-splitting BIBD, then there exists a $(v, 2 \times k, \lambda_1 + \lambda_2)$-splitting BIBD.

3 Direct Constructions

In this section we shall construct some designs of small order, which we will used later.

Lemma 3.1 There exists a $(9, 2 \times 4, 4)$-splitting BIBD.

Proof We construct directly the design as follows:

$$X = Z_9,$$

$$\mathcal{B}: \ \{0,2,5,6;3,4,7,8\},\ \{0,1,7,8;3,4,5,6\},\ \{0,4,5,7;1,2,6,8\},$$
$$\{0,2,4,8;1,3,6,7\},\ \{0,2,3,7;1,4,5,8\},\ \{0,3,6,8;1,2,5,7\},$$
$$\{0,1,4,6;2,3,5,8\},\ \{0,1,3,5;2,4,6,7\},\ \{1,2,3,4;5,6,7,8\}.$$

∎

In the remaining of this section we shall give some cycle constructions, which are variants of cycle construction used to construct balanced incomplete block designs.

The first cycle construction is difference construction based on Abelian group. Let $(X, +)$ be an Abelian group of order v, A $(v, b, l = uk, \lambda)$-*splitting difference family* over X is a collection of r subsets of X, $\{B^1, B^2, \cdots, B^r\}$, such that each B^h is expressed as a disjoint union of u subsets of size k: $B^h = B^h_1 \cup B^h_2 \cup \cdots \cup B^h_u$, and the multiset union

$$\bigcup_{1 \le h \le r} \{x - y : x \in B^h_i, y \in B^h_j \ (i \neq j),\ x \neq y\} = \lambda(X \setminus \{0\}).$$

The subsets B^h $(1 \le h \le r)$ are called based blocks. It is easy to see the existence of a $(v, b, l = uk, \lambda)$-splitting difference family over X implies the existence of a $(v, b, l = uk, \lambda)$-splitting BIBD $(X, \mathcal{B})$, in which the block set $\mathcal{B}$ is obtained by developing the based blocks mod v.

Lemma 3.2 There exists a $(17, 2 \times 4, 2)$-splitting BIBD.

Proof We construct directly the design as follows:

$$X = Z_{17}$$

$\mathcal{B}$: Develop the following blocks mod 17:

$$\{0,1,2,3;4,8,12,16\}. \qquad \blacksquare$$

Lemma 3.3 There exists a $(8, 2 \times 4, 4)$-splitting BIBD.

Proof We construct directly the design as follows:

$X = Z_7 \cup \{x\}$

$\mathcal{B}$: Develop the following blocks mod 7:

$$\{0,1,2,4;3,5,6,x\}. \qquad \blacksquare$$

Lemma 3.4 There exist $(v, 2 \times 4, 8)$-splitting BIBDs for $v = 12$ and 13.

Proof We construct the designs directly in Appendix. $\blacksquare$

Lemma 3.5 There exists a $(v, 2\times4, 16)$-splitting BIBD for $v \in \{10, 11, 14, 15\}$.

Proof We construct the designs directly in Appendix. $\blacksquare$

The second cycle construction is mixed difference construction. Let $(G, +)$ be an Abelian group of order n, $M = \{1, 2, \cdots, m-1\}$, and let $X = G \times M = \{\alpha_s : s \in M\}$. The group G operates on X by the rule

$$\alpha_s + \beta = (\alpha + \beta)_s \quad \text{for all } \beta \in G.$$

For any subset $A \subset X$ the set $A + \beta = \{x + \beta : x \in A\}$ is defined by the above rule. Let $\{B^1, B^2, \cdots, B^r\}$ be a collection of r subsets of X, such that each B^h is expressed as a disjoint union of u subsets of size k: $B^h = B_1^h \cup B_2^h \cup \cdots \cup B_u^h$, and the multiset union

$$\bigcup_{1\le h\le r}\{x - y : x_s \in B_i^h, y_s \in B_j^h \ (i \ne j),\ x \ne y\} = \lambda(G \setminus \{0\}) \ \text{ for all } s \in M,$$

$$\bigcup_{1\le h\le r}\{x - y : x_s \in B_i^h, y_t \in B_j^h \ (i \ne j)\} = \lambda G \ \text{ for all } s, t \in M, s < t.$$

The subsets B^h $(1 \le h \le r)$ are called based blocks. It is easy to see that we can construct from the based blocks a $(mn, b, l = uk, \lambda)$-splitting BIBD

$(X, \mathcal{B})$, in which the block set $\mathcal{B}$ is obtained by developing the based blocks mod n.

Lemma 3.6 There exist a $(10, 2; 2 \times 4, 16)$-splitting IBIBD and a $(11, 3; 2 \times 4, 16)$-splitting IBIBD.

Proof We construct directly the design $(10, 2; 2 \times 4, 16)$-splitting IBIBD as follows:

$X = Z_4 \times \{1, 2\} \cup \{x_1, x_2\}$

$\mathcal{B}$: Develop the following blocks mod 4:

$\{(0,1),(1,1),(2,1),(3,1);(0,2),(1,2),(2,2),(3,2)\}$,

$\{(0,1),(1,1),(0,2),(1,2);(2,1),(3,1),(2,2),(3,2)\}$,

$\{(0,1),(1,1),(0,2),(2,2);(2,1),(3,1),(1,2),(3,2)\}$,

$\{(0,1),(1,1),(0,2),(1,2);(2,1),(3,1),x_1,x_2\}$,

$\{(0,1),(1,1),(0,2),(2,2);(2,1),(3,1),x_1,x_2\}$,

$\{(0,1),(2,1),(0,2),(1,2);(1,1),(3,1),x_1,x_2\}$,

$\{(0,1),(2,1),(0,2),(2,2);(1,1),(3,1),x_1,x_2\}$,

$\{(0,1),(1,1),(2,2),(3,2);(0,2),(1,2),x_1,x_2\}$,

$\{(0,1),(1,1),(3,2),(2,2);(0,2),(1,2),x_1,x_2\}$,

$\{(0,1),(2,1),(1,2),(3,2);(0,2),(2,2),x_1,x_2\}$,

$\{(0,1),(3,1),(1,2),(2,2);(0,2),(3,2),x_1,x_2\}$.

For the $(11, 3; 2 \times 4, 16)$-splitting IBIBD, we construct the design directly in Appendix. ∎

4 $(v, 2 \times 4, \lambda)$-splitting *BIBD*

In this section, we shall give the spectrum of $(v, 2 \times 4, \lambda)$-splitting BIBDs. From Theorem 1.1, we have the following necessary condition for the existence of $(v, 2 \times 4, \lambda)$-splitting BIBD:

- $v \equiv 1 \pmod{32}$ when $\lambda \equiv 1,\ 3 \pmod 4$.
- $v \equiv 1 \pmod{16}$ when $\lambda \equiv 2 \pmod 4$.

- $v \equiv 0,\ 1 \pmod 8$ when $\lambda \equiv 4,\ 12 \pmod{16}$.
- $v \equiv 0,\ 1 \pmod 4$ when $\lambda \equiv 8 \pmod{16}$.
- $v \geq 8$ when $\lambda \equiv 0 \pmod{16}$.

From Lemma 2.6, we only need to consider the cases (1) $v \equiv 1 \pmod{32}$ and $\lambda = 1$, (2) $v \equiv 1 \pmod{16}$ and $\lambda = 2$, (3) $v \equiv 0,\ 1 \pmod 8$ and $\lambda = 4$, (4) $v \equiv 0,\ 1 \pmod 4$ and $\lambda = 8$, and (5) $v \geq 8$ and $\lambda = 16$.

For the case $\lambda = 1$, the second author of this article have obtained the following result.

Lemma 4.1 ([3]) There exists a $(v, 2k, 1)$-splitting BIBD for any $v \equiv 1\ (mod\ 2k^2)$ and $v \geq 2k^2 + 1$.

Then we have

Lemma 4.2 There exists a $(v, 2 \times 4, 1)$-splitting BIBD for any $v \equiv 1\ (mod\ 32)$ and $v \geq 33$.

For the case $\lambda > 1$, we can obtain the desired result by applying our main construction with the input designs constructed in Section 3.

Lemma 4.3 There exists a $(v, 2 \times 4, 2)$-splitting BIBD for any $v \equiv 1\ (mod\ 16)$ and $v \geq 17$.

Proof From Lemmas 3.2 we only need to consider the case $v \geq 33$. For any $v \equiv 1\ (mod\ 16)$ and $v \geq 33$, we can write $v = 16u + 16 + 1$. Notice that there exists a $(17, 2 \times 4, 2)$-splitting BIBD from the above Lemma, the result then follows from Lemma 2.5 with $w = 1$. ∎

Lemma 4.4 There exists a $(v, 2 \times 4, 4)$-splitting BIBD for any $v \equiv 0,\ 1\ (mod\ 8)$ and $v \geq 8$.

Proof From Lemmas 3.1 and 3.3 we only need to consider the case $v \geq 16$. For any $v \equiv 0,\ 1\ (mod\ 8)$ and $v \geq 16$, we can write $v = 8u + 8 + w$, where $w = 0, 1$, and then there exists a $(8 + w, 2 \times 4, 4)$-splitting BIBD from the above Lemmas. The result then follows from Lemma 2.5 with $w = 0$ and 1. ∎

Lemma 4.5 There exists a $(v, 2 \times 4, 8)$-splitting BIBD for any $v \equiv 0,\ 1 \pmod 4$ and $v \geq 8$.

Proof From Lemmas 3.1, 3.3 and 3.4 we only need to consider the case $v \geq 16$. For any $v \equiv 0,\ 1 \pmod 4$ and $v \geq 16$, we can write $v = 8u + (8+s) + w$, where $s = 0, 4$ and $w = 0, 1$, and then there exists a $(8 + s + w, 2 \times 4, 8)$-splitting BIBD from the above Lemmas. The result then follows from Lemma 2.5 with $w = 0$ and 1. ∎

Lemma 4.6 There exists a $(v, 2 \times 4, 16)$-splitting BIBD for any $v \geq 8$.

Proof From Lemma 3.5 and 4.5 we only need to consider the case $v \equiv 2,\ 3 \pmod 4$ and $v \geq 18$. For any $v \equiv 2,\ 3 \pmod 4$ and $v \geq 18$, we can write $v = 8u + (8 + s) + w$, where $s = 0, 4$ and $w = 2, 3$, and then there exist a $(8 + s + w, 2 \times 4, 16)$-splitting BIBD from Lemma 3.5 and a $(8 + w, w; 2 \times 4, 16)$-splitting IBIBD from Lemma 3.6. The result then follows from Lemma 2.5 with $w = 2$ and 3. ∎

Combining Lemma 4.2 to Lemma 4.6, we have established the following result.

Theorem 4.7 if $\lambda(v-1) \equiv 0 \pmod 4$ and $\lambda v(v-1) \equiv 0 \pmod{32}$, there exists a $(v, 2 \times 4, \lambda)$-splitting BIBD.

We are now in a position to prove Theorem 1.3.

The proof of Theorem 1.3: Theorems 1.1 and 4.7 complete the proof of Theorem 1.3. ∎

Appendix: Some Direct Constructions

$(11, 3; 2 \times 4, 16)$-splitting IBIBD

$X = Z_4 \times \{1, 2\} \cup \{x_1, x_2, x_3\}$

$\mathcal{B}$: Develop the following blocks mod 4:

$\{(0,1), (1,1), (2,1), (3,1); (0,2), (1,2), (2,2), (3,2)\}$,

$\{(0,1), (1,1), (0,2), (1,2); (2,1), (3,1), x_1, x_2\}$,

$\{(0,1),(1,1),(0,2),(2,2);(2,1),(3,1),x_1,x_2\}$,

$\{(0,1),(1,1),(0,2),(3,2);(2,1),(3,1),x_1,x_2\}$,

$\{(0,1),(1,1),(1,2),(0,2);(2,1),(3,1),x_1,x_2\}$,

$\{(0,1),(2,1),(0,2),(1,2);(1,1),(3,1),x_2,x_3\}$,

$\{(0,1),(2,1),(0,2),(2,2);(1,1),(3,1),x_2,x_3\}$,

$\{(0,1),(1,1),(0,2),(2,2);(1,2),(3,2),x_2,x_3\}$,

$\{(0,1),(1,1),(1,2),(2,2);(0,2),(3,2),x_2,x_3\}$,

$\{(0,1),(1,1),(2,2),(3,2);(0,2),(1,2),x_3,x_1\}$,

$\{(0,1),(1,1),(3,2),(2,2);(0,2),(1,2),x_3,x_1\}$,

$\{(0,1),(2,1),(0,2),(1,2);(2,2),(3,2),x_3,x_1\}$,

$\{(0,1),(2,1),(1,2),(3,2);(0,2),(2,2),x_3,x_1\}$. ∎

$(12, 2 \times 4, 8)$-splitting BIBD

$X = Z_{11} \cup \{x\}$

$\mathcal{B}$: Develop the following blocks mod 11:

$\{0,1,2,3;4,5,6,7\}$, $\{0,1,2,4;3,5,10,x\}$, $\{0,1,4,6;2,3,10,x\}$.

∎

$(13, 2 \times 4, 8)$-splitting BIBD

$X = Z_{13}$

$\mathcal{B}$: Develop the following blocks mod 13:

$\{0,1,2,3;4,5,6,7\}$, $\{0,1,2,4;3,5,6,7\}$, $\{0,1,3,10;2,7,11,12\}$.

∎

$(10, 2 \times 4, 16)$-splitting BIBD

$X = Z_9 \cup \{x\}$

$\mathcal{B}$: Develop the following blocks mod 9:

$\{0,1,2,3;4,5,6,7\}$, $\{0,1,2,4;3,5,7,x\}$, $\{0,1,3,5;2,4,8,x\}$,

$\{0,1,3,6;2,4,8,x\}$, $\{0,1,4,5;2,3,6,x\}$. ∎

$(11, 2\times 4, 16)$-splitting BIBD

$X = Z_{11}$

$\mathcal{B}$: Develop the following blocks mod 11:

$\{0,1,2,3;4,5,6,7\}$, $\{0,1,2,3;4,5,6,9\}$, $\{0,1,3,5;2,4,6,10\}$,

$\{0,1,3,8;2,4,9,10\}$, $\{0,1,4,5;2,3,6,8\}$. ∎

$(14, 2\times 4, 16)$-splitting BIBD

$X = Z_{13} \cup \{x\}$

$\mathcal{B}$: Develop the following blocks mod 13:

$\{0,1,2,3;4,5,6,7\}$ three times,

$\{0,1,2,3;4,5,7,x\}$, $\{0,1,5,8;6,7,12,x\}$,

$\{0,2,4,6;1,3,5,x\}$, $\{0,1,4,10;2,3,12,x\}$. ∎

$(15, 2\times 4, 16)$-splitting BIBD

$X = Z_{15}$

$\mathcal{B}$: Develop the following blocks mod 15:

$\{0,1,2,3;4,5,6,7\}$ four times,

$\{0,1,5,6;7,8,13,14\}$, $\{0,1,7,8;2,6,9,14\}$, $\{0,2,6,8;1,7,9,14\}$.

∎

References

[1] Th. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Bibliographisches Institut, Zurich, 1985.

[2] B. Du, *Splitting balanced incomplete block designs with block size* 3×2, J. Combin. Designs, **12** (2004), 404-420.

[3] B. Du, *Splitting balanced incomplete block designs*, Australas. J. Combin., **31** (2005), 287-298.

[4] W. Ogata, K. Kurosawa, D.R. Stinson and H. Saido, *New combinatorial designs and their applications to authentication codes and secret sharing schemes* , Discrete Math., **279** (2004), 383-405.

[5] R.M. Wilson, *Constructions and uses of pairwise balanced designs*, Math. Centre Tracts, **55**(1974), 18-41.