AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **31** (2005), Pages 287–298

Splitting balanced incomplete block designs

Beiliang Du

Department of Mathematics
Suzhou University
Suzhou 215006
P.R.China
dubl@suda.edu.cn

Abstract

Splitting balanced incomplete block designs were first formulated by Ogata, Kurosawa, Stinson and Saido in recent investigation of authentication codes. This article investigates the existence of a splitting balanced incomplete block design $(v, 2k, \lambda)$-splitting BIBD, and gives the spectra of $(v, 2k, \lambda)$-splitting BIBDs for (1) $k = 2$, (2) $k = 3$, and (3) k even and $\lambda = 1$. As an application we obtain some infinite classes of k-splitting A-codes.

1 Introduction

In the investigation of authentication codes Ogata, Kurosawa, Stinson and Saido [5] found that the 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* $(v, b, l = uk, \lambda)$-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:

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 splitting balanced incomplete block design $(v, b, l = uk, \lambda)$-splitting BIBD will be displayed in the form $(a_1, a_2, \cdots, a_k; b_1, b_2, \cdots, b_k; \cdots; c_1, c_2, \cdots, c_k)$ in this article.

Let r be the number of blocks which contain a fixed point. We have the following expressions from [5].

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

In this article, we shall restrict our attention to splitting balanced incomplete block designs with $u = 2$, denoted briefly by $(v, 2k, \lambda)$-splitting BIBD. We have the following necessary condition for the existence of a $(v, 2k, \lambda)$-splitting BIBD.

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

$$\lambda(v-1) \equiv 0 \pmod{k}, \qquad v(v-1) \equiv 0 \pmod{2k^2}.$$

This article investigates the existence of $(v, 2k, \lambda)$-splitting BIBDs, and gives the spectra of $(v, 2k, \lambda)$-splitting BIBDs for (1) $k = 2$, (2) $k = 3$, and (3) k is even and $\lambda = 1$. That is, our main objective in this article is to establish the following results.

Theorem 1.2 There exists a $(v, 2k, 1)$-splitting BIBD for any $v \equiv\ 1\ (mod\ 2k^2)$ and $v \geq 2k^2 + 1$. Moreover, the necessary condition in Theorem 1.1 is also sufficient for the case k is even and $\lambda = 1$.

Theorem 1.3 The necessary condition in Theorem 1.1 is also sufficient for the case $k = 2$.

Theorem 1.4 The necessary condition in Theorem 1.1 is also sufficient for the case $k = 3$ with the exceptions of $v = 10$ and $\lambda = 1$, and $v = 6$ and $\lambda \equiv 3 \pmod{6}$.

2 Preliminaries

In this section we shall define some of the auxiliary designs and introduce some of the fundamental results which will be used later. The reader is referred to [4] 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. $\mathcal{G}$ partitions 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 $G \in \mathcal{G}$ 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 notations. 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 if $|B| \in K$ for every block $B \in \mathcal{B}$.

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 a 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. $\mathcal{G}$ partitions 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 exists 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 if $|B| \in K$ for every block $B \in \mathcal{B}$.

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

Lemma 2.2 There exists a 2×3-splitting GDD of type 3^u for any $u \geq 2$.

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

$$(i_1, i_2, i_3; (i+j)_1, (i+j)_2, (i+j)_3), \ 0 \leq i \leq u-2, \ 1 \leq j \leq u-i-1.$$

It is easy to check that the $(X, \mathcal{G}, \mathcal{B})$ is a 2×3-splitting GDD of type 3^u. □

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

Theorem 2.3 Suppose that there is a K-GDD of type $g_1g_2\cdots g_u$ and that for each $k\in K$ there is a 2×3-splitting GDD of type h^k. Then there is a 2×3-splitting GDD of type $(hg_1)(hg_2)\cdots(hg_u)$.

Proof We start with a K-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 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 2×3-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 2×3-splitting GDD of type $(hg_1)(hg_2)\cdots(hg_u)$. □

We are now in a position to give our main construction.

Construction 2.4 Suppose

1. there is a 2×3-splitting GDD of type $g_1g_2\cdots g_u$,
2. there is a $(g_i+w,2\times 3,\lambda)$-splitting BIBD for each $i, 1\le i\le u$, where $w=0$ or 1.

Then there is a $(v,2\times 3,\lambda)$-splitting BIBD, where $v=w+\sum_{1\le i\le u}g_i$.

Proof We start with a 2×3-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, let $(G_i\cup W,\mathcal{A}_i)$ be a $(g_i+w,2\times 3,\lambda)$-splitting BIBD, where $|W|=0$ or 1 and $X\cap W=\emptyset$. Then the design we construct will have point set

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

and the block set

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

where $\mathcal{B}'$ is a block collection obtained by repeating every block of $\mathcal{B}$ λ times. It is easy to check that $(X^*,\mathcal{B}^*)$ is a $(v,2\times 3,\lambda)$-splitting BIBD. □

In particular, we have the following construction.

Lemma 2.5 Let m, u and n be positive integers and $w=0$ or 1. If there exist a $(3m+w,2\times 3,\lambda)$-splitting BIBD and a $(3n+w,2\times 3,\lambda)$-splitting BIBD, then there exists a $(3mu+3n+w,2\times 3,\lambda)$-splitting BIBD.

Proof We begin with a 2-GDD of type $m^u n^1$ (for whose existence, see Lemma 2.1) and give the points weight 3 and apply Theorem 2.3 to obtain a 2×3-splitting GDD of type $(3m)^u(3n)^1$. The input design we need, a 2×3-splitting GDD of type 3^2, 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 $(v, 2\times 3, \lambda_1)$-splitting BIBD and a $(v, 2\times 3, \lambda_2)$-splitting BIBD, then there exists a $(v, 2\times 3, \lambda_1+\lambda_2)$-splitting BIBD.

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

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.

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

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

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: $B^h = B^h_1 \cup B^h_2 \cup \cdots \cup B^h_u$, and the multiset union

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

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

The subsets B^h $(1 \le h \le r)$ are called base blocks. It is easy to see that we can construct from the base blocks a $(mn, b, l = uk, \lambda)$-splitting BIBD $(X, \mathcal{B})$, in which the block set $\mathcal{B}$ is obtained by developing the base blocks mod n.

3 $(v, 2 \times 2, \lambda)$-splitting BIBD

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

- $v \equiv 1 \pmod 8$ when $\lambda \equiv 1,\ 3 \pmod 4$.
- $v \equiv 0,\ 1 \pmod 4$ when $\lambda \equiv 2 \pmod 4$.
- $v \geq 4$ when $\lambda \equiv 0 \pmod 4$.

From Lemma 2.6, we only need to consider the cases $v \equiv 1 \pmod 8$ and $\lambda = 1$, $v \equiv 0,\ 1 \pmod 4$ and $\lambda = 2$, and $v \geq 4$ and $\lambda = 4$.

3.1 The case $\lambda = 1$

In this subsection, we shall investigate the existence of a $(v, 2 \times 2, 1)$-splitting BIBD.

Lemma 3.1.1 There exists a $(v, 2k, 1)$-splitting BIBD for any $v \equiv\ 1 \pmod{2k^2}$ and $v \geq 2k^2 + 1$.

Proof The design we construct will have point set $X = Z_v$. The block set $\mathcal{B}$ is obtained by developing the following blocks mod v:

$$(0, 1, \cdots, k-1; ik^2 + k, ik^2 + 2k, \cdots, (i+1)k^2),\ 0 \leq i < (v-1)/(2k^2).$$

It is easy to check that $(X, \mathcal{B})$ is a $(v, 2k, 1)$-splitting BIBD. □

We are now in a position to prove Theorem 1.2.

The proof of Theorem 1.2: Theorem 1.1 and Lemma 3.1.1 complete the proof of Theorem 1.2. □

3.2 The case $\lambda > 1$

In this subsection, we shall investigate the existence of $(v, 2 \times 2, \lambda)$-splitting BIBD for $\lambda = 2$ and 4. For this purpose we need to introduce the concept of a perfect Mendelsohn design.

Let $S = \{s_1, s_2, \cdots, s_k\}$ be a set of k distinct elements. Then the ordered pair (s_i, s_j) is said to be t-apart in the cycle $(s_1, s_2, \cdots, s_k)$ if $j - i \equiv\ t \pmod k$. Let $v,\ k,\ \lambda$ be positive integers. A *perfect Mendelsohn design* (v, k, λ)-PMD is a pair $(X, \mathcal{B})$ where X is a v-set (of points) and $\mathcal{B}$ is a collection of subsets of X (called blocks) with size k such that for any $x, y \in X,\ x \neq y$ and for any t, $1 \leq t \leq k-1$, there exist exactly λ blocks $B \in \mathcal{B}$ in which the ordered pair (x, y) appears t-apart.

For perfect Mendelsohn designs, we have the following result.

Lemma 3.2.1

(1) ([2], [3], [6]) There exists a $(v, 4, \lambda)$-PMD if and only if $\lambda v(v-1) \equiv 0 \pmod 4$ with the exception of $v = 4$ and λ odd, and $v = 8$ and $\lambda = 1$.

(2) ([1], [7]) There exists a $(v, 6, 3)$-PMD if and only if $v \geq 6$ with the possibly exception of $v \in E$, where $E = \{6, 10, 12, 16, 18, 22, 24, 30, 33, 34, 39, 45, 48, 51, 54, 60\}$.

Perfect Mendelsohn designs provide a method of constructing splitting balanced incomplete block designs.

Lemma 3.2.2 If there exists a $(v, 2k, \lambda)$-PMD and $k = 2$ or 3, then there exists a $(v, 2k, k\lambda)$-splitting BIBD.

Proof Let $(s_1, s_2, \cdots, s_{2k})$ be any block of the $(v, 2k, \lambda)$-PMD $(X, \mathcal{B})$. We rearrange this block as follows:

$$(s_1, s_3, \cdots, s_{2k-1}; s_2, s_4, \cdots, s_{2k}).$$

Performing such rearrangements to every block of the PMD, these rearranged blocks constitute the design we need. Clearly the above rearrangement indicates that for each pair set $\{x, y\}$ of X, there exist exactly 2λ blocks $B = B_1 \cup B_2$ such that $x \in B_1,\ y \in B_2$ from the 1-apart property of a PMD. For the case $k = 3$, the 3-apart property of a PMD provides exactly another λ blocks $B = B_1 \cup B_2$ such that $x \in B_1,\ y \in B_2$. □

Lemma 3.2.3 There exists a $(v, 2 \times 2, 2)$-splitting BIBD for any $v \equiv 0,\ 1 \pmod 4$ and $v \geq 4$.

Proof For the cases $v = 4$ and 8, we construct the designs directly as follows:

$v = 4:\ X = Z_4,$

$\mathcal{B}$: $(0, 1; 2, 3), (0, 2; 1, 3), (0, 3; 1, 2).$

$v = 8:\ X = Z_7 \cup \{x\},$

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

$$(x, 0; 4, 5), (0, 2; 1, 5).$$

For the other values of v, we apply Lemma 3.2.2 with $\lambda = 1$ to obtain the desired designs; the input design we need, $(v, 4, 1)$-PMD, comes from Lemma 3.2.1 (1). □

Lemma 3.2.4 There exists a $(v, 2 \times 2, 4)$-splitting BIBD for any $v \geq 4$.

Proof We apply Lemma 3.2.2 with $\lambda = 2$ to obtain the desired design; the input design we need, $(v, 4, 2)$-PMD, comes from Lemma 3.2.1 (1). □

We are now in a position to prove Theorem 1.3.

The proof of Theorem 1.3: Theorems 1.1 and 1.2 and Lemmas 3.2.3, 3.2.4 and 2.6 complete the proof of Theorem 1.3. □

4 $(v, 2 \times 3, \lambda)$-splitting BIBD

In this section, we shall give the spectrum of $(v, 2 \times 3, \lambda)$-splitting BIBDs. From Theorem 1.1, we have the following necessary conditions for the existence of a $(v, 2 \times 3, \lambda)$-splitting BIBD:

- $v \equiv 1 \pmod 9$ when $\lambda \equiv 1,\ 2 \pmod 3$.
- $v \equiv 0,\ 1 \pmod 3$ when $\lambda \equiv 3,\ 6 \pmod 9$.
- $v \geq 6$ when $\lambda \equiv 0 \pmod 9$.

From Lemma 2.6, we only need to consider the cases $v \equiv 1 \pmod 9$ and $\lambda = 1$, $v \equiv 0,\ 1 \pmod 3$ and $\lambda = 3$, and $v \geq 6$ and $\lambda = 9$.

4.1 The case $\lambda = 1$

In this subsection, we shall investigate the existence of $(v, 2 \times 3, 1)$-splitting BIBDs. From Theorem 1.2 we only need to consider the case $v \equiv 10 \pmod{18}$. There is no $(10, 2 \times 3, 1)$-splitting BIBD by computer search.

Lemma 4.1.1 There exists a $(28, 2 \times 3, 1)$-splitting BIBD.

Proof We construct the design directly as follows:

$X = Z_7 \times \{1, 2, 3, 4\}$,

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

$(0_1, 1_1, 2_1; 3_1, 0_2, 3_2),\ (0_1, 1_1, 2_1; 0_3, 3_3, 0_4),\ (0_1, 0_2, 2_2; 4_2, 4_3, 2_4),$

$(0_1, 0_2, 5_4; 1_4, 3_4, 4_4),\ (0_2, 0_3, 2_3; 6_2, 5_4, 6_4),\ (0_2, 1_3, 0_4; 0_3, 5_3, 6_3).$ □

Lemma 4.1.2 If $v \equiv 10 \pmod{18}$ and $v \geq 46$, then there exists a $(v, 2 \times 3, 1)$-splitting BIBD.

Proof For any $v \equiv 10 \pmod{18}$ and $v \geq 46$, we can write $v = v_0 + 27 + 1$, where $v_0 \equiv 0 \pmod{18}$ and then there exists a $(v_0 + 1, 2 \times 3, 1)$-splitting BIBD by Theorem 1.2. The result then follows from Lemma 2.5 with $w = 1$. □

Combining Theorem 1.2 and Lemmas 4.1.1 and 4.1.2, we have established the following result.

Theorem 4.1.3 There exists a $(v, 2 \times 3, 1)$-splitting BIBD for any $v \equiv\ 1 \pmod 9$ and $v > 10$.

4.2 The case $\lambda > 1$

In this subsection, we shall investigate the existence of $(v, 2 \times 3, \lambda)$-splitting BIBDs for $\lambda = 3$ and 9. We first consider the case $v = 6$.

Lemma 4.2.1 There does not exist a $(6, 2 \times 3, \lambda)$-splitting BIBD for any odd λ.

Proof Let $X = Z_6$ and λ be an odd integer. Suppose that there exists a $(6, 2 \times 3, \lambda)$-splitting BIBD $(X, \mathcal{B})$, where $\mathcal{B}$ is obtained from the following blocks:

$$\begin{aligned} B_1 &= (0,2,3;1,4,5), & B_2 &= (0,2,4;1,3,5), \\ B_3 &= (0,2,5;1,3,4), & B_4 &= (0,3,4;1,2,5), \\ B_5 &= (0,3,5;1,2,4), & B_6 &= (0,4,5;1,2,3), \\ B_7 &= (0,1,5;2,3,4), & B_8 &= (0,1,4;2,3,5), \\ B_9 &= (0,1,3;2,4,5), & B_{10} &= (0,1,2;3,4,5). \end{aligned}$$

Without loss of generality, we can assume that B_i occurs in $\mathcal{B}$ exactly x_i times, $1 \le i \le 10$. From the pair sets $\{0,1\}$, $\{3,4\}$, $\{3,5\}$ and $\{4,5\}$ all occurring in exactly λ blocks, we have the following equalities.

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = \lambda, \tag{1}$$
$$x_1 + x_2 + x_5 + x_6 + x_8 + x_9 = \lambda, \tag{2}$$
$$x_1 + x_3 + x_4 + x_6 + x_7 + x_9 = \lambda, \tag{3}$$
$$x_2 + x_3 + x_4 + x_5 + x_7 + x_8 = \lambda. \tag{4}$$

Combining equalities (1) and (2), (1) and (3), and (1) and (4), respectively, we have:

$$x_3 + x_4 = x_8 + x_9, \quad x_2 + x_5 = x_7 + x_9, \quad x_1 + x_6 = x_7 + x_8.$$

Consequently, $\lambda = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 2(x_7 + x_8 + x_9)$ is even, which is a contradiction. Thus a $(6, 2 \times 3, \lambda)$-splitting BIBD cannot exist for any odd λ. □

Lemma 4.2.2 There exists a $(v, 2 \times 3, 3)$-splitting BIBD for $v \in \{7, 9, 10, 12, 15\}$.

Proof We construct the designs directly as follows:

$X = Z_v$,

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

$v = 7:$ $(0,1,3;2,4,5)$.

$v = 9:$ $(0,3,6;1,4,7)$ (choose the first 3 blocks),
$(0,1,5;4,6,7)$.

$v = 10:$ $(0,1,3;5,6,8)$ (choose the first 5 blocks),
$(0,2,5;1,3,8)$.

$v = 12:$ $(0,4,8;1,5,9)$ (choose the first 4 blocks),
$(0,1,3;6,7,9)$ (choose the first 6 blocks),
$(0,1,4;2,3,8)$.

$v = 15:$ $(0,1,3;8,9,11)$ (choose the first 5 blocks),
$(0,1,2;3,4,7)$,
$(0,1,3;6,8,14)$. □

Lemma 4.2.3 If $v \equiv 0 \pmod 3$ and $v \ge 18$, then there exists a $(v, 2 \times 3, 3)$-splitting BIBD.

Proof For any $v \equiv 0 \pmod 3$ and $v \geq 18$, we can write $v = 9u + 9 + s$ if $v \equiv s \pmod 9$, where $s = 0, 3$ or 6, and then there exists a $(9 + s, 2 \times 3, 3)$-splitting BIBD from Lemma 4.2.2. The result then follows from Lemma 2.5 with $w = 0$. □

Lemma 4.2.4 If $v \equiv 1 \pmod 3$ and $v \geq 13$, then there exists a $(v, 2 \times 3, 3)$-splitting BIBD.

Proof For any $v \equiv 1 \pmod 3$ and $v \geq 13$, we can write $v = 6u + 6 + s + 1$ if $v \equiv s + 1 \pmod 6$, where $s = 0$ or 3, and then there exists a $(6 + s + 1, 2 \times 3, 3)$-splitting BIBD from Lemma 4.2.2. The result then follows from Lemma 2.5 with $w = 1$. □

Combining Lemma 4.2.1 to Lemma 4.2.4, we have established the following result.

Theorem 4.2.5 There exists a $(v, 2 \times 3, 3)$-splitting BIBD for any $v \equiv 0,\ 1 \pmod 3$ and $v > 6$.

We then have the following result for $\lambda = 9$.

Theorem 4.2.6 There exists a $(v, 2 \times 3, 9)$-splitting BIBD for any $v > 6$.

Proof Combining Lemma 3.2.2 and Lemma 3.2.1 (2), we only need to consider the case $v \in E$ (in Lemma 3.2.1 (2)). Noticing that $v \equiv 0,\ 1 \pmod 3$ for $v \in E$, we know that the result is true from Theorem 4.2.5, Lemma 4.2.1 and Lemma 2.6. □

We are now in a position to prove Theorem 1.4.

The proof of Theorem 1.4: Theorems 4.1.3, 4.2.5 and 4.2.6 complete the proof of Theorem 1.4, apart from $v = 6$ and 10. For these cases, we construct directly a $(6, 2 \times 3, 6)$-splitting BIBD and a $(10, 2 \times 3, 2)$-splitting BIBD as follows:

$v = 6:\ X = Z_5 \cup \{x\}$,

$\mathcal{B}$: Develop the following blocks mod 5:

$(x, 0, 1; 2, 3, 4),\ (x, 0, 2; 1, 3, 4)$.

$v = 10:\ X = Z_5 \times \{1, 2\}$,

$\mathcal{B}$: Develop the following blocks mod 5:

$(0_1, 1_1, 0_2; 2_1, 1_2, 2_2),\ (0_1, 1_1, 1_2; 2_1, 0_2, 3_2)$. □

5 k-splitting A-code

An authentication code (A-code) is called splitting if a message m ($\in M$) is not uniquely determined by the source state s ($\in S$) and the key e ($\in E$). In this case, a message m is computed as $m = e(s, r)$, where r is a random chosen from some specified finite set. If we define

$$e(s) = \{m : e(s, r) = m \text{ for some } r\},$$

then splitting means that $|e(s)| > 1$. The concept of splitting is very important in the context of authentication codes with arbitration. We say that a splitting A-code is k-splitting if $|e(s)| = k$ for any $e \in E$ and any $s \in S$. In a k-splitting A-code, we have

$$p_I \geq \frac{k|S|}{|M|}, \quad p_S \geq \frac{(k-1)|S|}{|M|-1},$$

where p_I is the impersonation attack probability and p_S is the substitution attack probability.

Ogata, Kurosawa, Stinson and Saido found that splitting balanced incomplete block designs can be used to construct k-splitting A-codes, whose impersonation attack probabilities p_I and substitution attack probabilities p_S all achieve their information-theoretic lower bounds.

Theorem 5.1 ([5]) If there exists a $(v, b, uk, 1)$-splitting BIBD, then there exists a k-splitting A-code with $|M| = v$, $|E| = b$ and $|S| = u$ such that:

1. $p_I = \frac{uk}{v}$, $p_S = \frac{u(k-1)}{v-1}$,
2. each source state occurs with equal probability.

From Theorem 1.2 we have established the following result.

Theorem 5.2 Let k be a positive integer, $v \equiv 1 \pmod{2k^2}$ and $v \geq 2k^2 + 1$. Then there exists a k-splitting A-code with $|M| = v$, $|E| = \frac{v(v-1)}{2k^2}$ and $|S| = 2$ such that:

1. $p_I = \frac{2k}{v}$, $p_S = \frac{2(k-1)}{v-1}$,
2. each source state occurs with equal probability.

From Theorem 1.4 we have established the following result.

Theorem 5.3 Let $v \equiv 1 \pmod 9$ and $v \geq 19$. Then there exists a 3-splitting A-code with $|M| = v$, $|E| = \frac{v(v-1)}{18}$ and $|S| = 2$ such that:

1. $p_I = \frac{6}{v}$, $p_S = \frac{4}{v-1}$,
2. each source state occurs with equal probability.

Acknowledgment

The author wishes to thank the referee for his/her comments on improving the presentation of the paper. The author also wishes to thank Miao Liang for her work on improving the presentation of the paper.

References

[1] R.J.R. Abel, F.E. Bennett and H. Zhang, Perfect Mendelsohn designs with block size 6, *J. Statist. Plann. Inference* **86** (2000), 287–319.

[2] F.E. Bennett, H. Shen and J. Yin, Incomplete perfect Mendelsohn designs with block size four and hole of size 2 and 3, *J. Combin. Designs* **3** (1994), 171–183.

[3] F.E. Bennett, Z. Xuebin and L. Zhu, Perfect Mendelsohn designs with block size four, *Ars Combin.* **29** (1990), 65–72.

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

[5] 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.

[6] Z. Xuebin, On the existence of $(v, 4, 1)$-PMD, *Ars Combin.* **29** (1990), 3–12.

[7] J. Yin, The existence of $(v, 6, 3)$-PMDs, *Math. Appl.* **6** (1993), 457–462.

(Received 16 June 2003; revised 25 Sep 2003)