Further constructions for BIB designs with nested rows and columns

Takaaki HISHIDA
Department of Information Network Engineering
Aichi Institute of Technology
Toyota 470-0392, Japan
hishida@aitech.ac.jp

Masakazu JIMBO Graduate School of Information Science Nagoya University Nagoya 464-8601, Japan jimbo@is.nagoya-u.ac.jp

Miwako MISHIMA*
Information and Multimedia Center
Gifu University
Gifu 501-1193, Japan
miwako@info.gifu-u.ac.jp

Yukiyasu MUTOH
Graduate School of Information Science
Nagoya University
Nagoya 464-8601, Japan
yukiyasu@jim.math.cm.is.nagoya-u.ac.jp

Kazuhiro Ozawa Gifu College of Nursing Hashima 501-6295, Japan ozawa@gifu-cn.ac.jp

Abstract

In this paper, several constructions are presented for balanced incomplete block designs with nested rows and columns. Some of them refine theorems due to Hishida and Jimbo [6] and Uddin and Morgan [17], and some of them give parameters which have not been available before.

^{*}Corresponding author.

1. Introduction

We assume that the reader is familiar with balanced incomplete block (BIB) designs. For any terms used undefined in this article, we refer the reader to [3] and [4] for example. In what follows, the notation $B(v, k, \lambda)$ stands for a BIB design with v points, block size k and index λ .

Let V be a set of v points and A be a collection of b subsets, called blocks, of V, each of which is represented as a $k_1 \times k_2$ array. Further define $\lambda_R(i,j)$ to be the number of rows in blocks in which a pair of distinct points i and j occurs together. $\lambda_C(i,j)$ and $\lambda_B(i,j)$ are defined similarly for columns and blocks. The pair (V,A) is called a balanced incomplete block design with nested rows and columns if the following conditions are satisfied:

- (i) no point occurs more than once in any block of A (said to be binary),
- (ii) each point occurs in exactly $r = bk_1k_2/v$ blocks of A, and
- (iii) for any pair of distinct points i and j,

$$\lambda = k_1 \lambda_R(i,j) + k_2 \lambda_C(i,j) - \lambda_B(i,j) \tag{1.1}$$

is constant not depending on the choice of i and j.

A balanced incomplete block design with nested rows and columns (BIBRC for short) with parameters v, b, r, k_1 , k_2 , λ is denoted by BIBRC(v, b, r, k_1 , k_2 , λ). Furthermore, if the following condition (iv) holds, then the BIBRC is especially said to be *completely balanced* (see Morgan [8]).

(iv) Each of indices $\lambda_R(i,j)$, $\lambda_C(i,j)$ and $\lambda_B(i,j)$ is constant not depending on the choice of pairs (i,j), simply denoted by λ_R , λ_C and λ_B .

The condition (iv) implies that the sets of rows, columns and blocks form a B(v, k_1, λ_R), a B(v, k_2, λ_C) and a B($v, k_1 k_2, \lambda_B$), respectively. A simple counting argument shows that the indices λ_R , λ_C and λ_B are uniquely determined by k_1 , k_2 and λ as follows:

$$\lambda_R=\frac{1}{k_1-1}\lambda,\quad \lambda_C=\frac{1}{k_2-1}\lambda,\quad \lambda_B=\frac{k_1k_2-1}{(k_1-1)(k_2-1)}\lambda.$$

If $v = k_1 k_2$, then (V, A) is called a balanced *complete* block design with nested rows and columns (BCBRC for short), denoted by BCBRC $(v, b, r, k_1, k_2, \lambda)$.

The concept of nested incomplete block designs was first introduced by Preece [12] in 1967 and several related concepts have been derived from [12]. The notion of a balanced incomplete block design with nested rows

and columns was formalized by Singh and Dey [13] in 1979. They gave a construction together with some examples. After that, constructions for BIBRC have been investigated by Agrawal and Prasad [1, 2], Cheng [5], Jimbo and Kuriki [7], Mukerjee and Gupta [10], Sreenath [14], Street [15], Uddin [16], etc. Uddin and Morgan [17] presented constructions for BIBRC which cover most of the known direct constructions before them, and they also put a table of the designs for $v \leq 101$ and $3 \leq k_1 \leq k_2$ constructed by themselves together with the fewest number r of replications that have ever been known in the literature. The statistical analysis of BIBRC was given by Morgan and Uddin [9]. They showed that a BIBRC is universally optimum within the class of binary designs for a random effect model. Morgan surveyed the statistical analysis and known direct and recursive constructions in [8]. Hishida and Jimbo [6] have generalized some constructions due to Uddin and Morgan [17] for BIBRC having completely balanced property. In Nasu et al. [11], we can find some series of BIBRC obtained through affine geometries.

In this paper, several constructions are presented for BIBRC, some of which are the refinement of theorems due to Hishida and Jimbo [6] and Uddin and Morgan [17], and some of which have not been known before.

2. Constructions for BIBRC having completely balanced property

This section is devoted to direct constructions for BIBRC having completely balanced property. For simplicity, a BIBRC having completely balanced property is referred to just as a BIBRC, unless otherwise specified.

To present our constructions, the following lemma is needed, which is a well-known result by Wilson [18]. Throughout this article, α stands for a primitive element of a *Galois field* of prime power order v, denoted by GF(v) = V, and $H_0^n = \{\alpha^i \mid i \equiv 0 \pmod{n}\}$ denotes a multiplicative subgroup of $GF(v) \setminus \{0\}$. Then H_e^n is defined as a coset of H_0^n , i.e., $H_e^n = \alpha^e H_0^n$.

Lemma 2.1 Let v = nk + 1 be a prime power, S_n be a system of distinct representatives for the cosets of $V \setminus \{0\}$ modulo H_0^n and L be a g-subset of S_n .

(i) Let
$$B = \bigcup_{e \in L} H_e^n$$
 and

$$\mathcal{B} = \{sB + x \mid s \in S_n, x \in V\},\$$

where $sB + x = \{sb + x \mid b \in B\}$. Then (V, \mathcal{B}) is a B(v, gk, g(gk-1)).

- (i)' Moreover, if n is even and k is odd, then for $\mathcal{B}' = \{sB + x \mid s \in S_{n/2}, x \in V\}, (V, \mathcal{B}')$ is a B(v, gk, g(gk-1)/2).
- (ii) Let $\bar{B} = \{0\} \cup B$ and

$$\bar{\mathcal{B}} = \{ s\bar{\mathcal{B}} + x \mid s \in S_n, x \in V \}.$$

Then (V, \hat{B}) is a B(v, gk+1, g(gk+1)).

(ii)' Moreover, if n is even and k is odd, then for $\bar{\mathcal{B}}' = \{s\bar{B} + x \mid s \in S_{n/2}, x \in V\}, (V, \bar{\mathcal{B}}')$ is a B(v, gk + 1, g(gk + 1)/2).

The next theorem is the refinement of Theorems 3.1 and 3.2 in [6]. Actually, the range of i for u_i in those theorems is redundant. Note that Theorem 2.2(a)' and (b)' with m even covers Theorem 3.2 in [6].

Theorem 2.2 Let v = mpqf + 1 be a prime power with gcd(p,q) = 1. Write $\alpha^{u_{ij}} = 1 - \alpha^{m(qi+pj)}$ for $0 \le i < pf$ and $0 \le j < qf$ but $(i,j) \ne (0,0)$, where $0 \le u_{ij} < v - 1$.

(a) If $f \le m$ and there exists an integer u such that $u \not\equiv mpqf/2, u_{ij} - u_{-i,0} \pmod{m}$ for any $1 \le i < pf$ and $1 \le j < q$, where $u_{-i,0} = u_{pf-i,0}$, then there exists a BIBRC with parameters

$$v = mpqf + 1, \quad b = mqv, \quad r = k_1k_2mq,$$

 $k_1 = pf, \quad k_2 = qf, \quad \lambda = qf(pf - 1)(qf - 1).$

(b) If f < m and there exists an integer u such that $u \not\equiv mpqf/2, -u_{i0}, u_{ij} - u_{-i,0} \pmod{m}$ for any $1 \le i < pf$ and $1 \le j < q$, then there exists a BIBRC with parameters

$$v = mpqf + 1, \quad b = mqv, \quad r = k_1k_2mq,$$

 $k_1 = pf, \quad k_2 = qf + 1, \quad \lambda = qf(pf - 1)(qf + 1).$

Moreover, if mq is even and pf is odd, then there exist BIBRC with the following parameters corresponding to (a) and (b):

(a)'
$$v = mpqf + 1$$
, $b = mqv/2$, $r = k_1k_2mq/2$, $k_1 = pf$, $k_2 = qf$, $\lambda = qf(pf-1)(qf-1)/2$.

(b)'
$$v = mpqf + 1$$
, $b = mqv/2$, $r = k_1k_2mq/2$, $k_1 = pf$, $k_2 = qf + 1$, $\lambda = qf(pf - 1)(qf + 1)/2$.

Proof. (a) Define a $pf \times qf$ array A by the (i, j)th entry as follows:

$$A = [\alpha^{m(qi+pj)} + \alpha^{mqi+u}], \quad 0 \le i < pf, \quad 0 \le j < qf,$$
 (2.1)

and a collection A of mqv arrays by

$$A = \{ sA + x \mid s \in S_{mq}, \ x \in V \}, \tag{2.2}$$

where V = GF(v). Then (V, A) is the desired BIBRC of (a). In order to prove this, we firstly show that the entries of A are distinct from each other.

It is easy to see that the *i*th row R_i and the *j*th column C_j of the array A can be regarded as the following sets:

$$R_i = \alpha^{mqi}(\alpha^u + H_0^{mp})$$
 and $C_j = (\alpha^u + \alpha^{mpj})H_0^{mq}$.

By flattening out the array A into a block B of size pqf^2 , we have

$$B = \bigcup_{i=0}^{pf-1} R_i = \bigcup_{j=0}^{qf-1} C_j = \bigcup_{j=0}^{qf-1} (\alpha^u + \alpha^{mpj}) H_0^{mq}.$$

This means that we need to prove that the elements of $\bigcup_{j=0}^{qf-1}(\alpha^u + \alpha^{mpj})$ are relatively distinct over S_{mq} . Clearly, $\alpha^u + \alpha^{mpj} \not\equiv 0 \pmod{v}$ for $0 \leq j < qf$ is an indispensable prerequisite, which leads to the condition $u \not\equiv mpqf/2 \pmod{m}$ since $\alpha^{mpqf/2} = -1$.

Now, for some $1 \le i < pf$ and $0 \le j_1 \ne j_2 < qf$, suppose that

$$\alpha^{mqi}(\alpha^u + \alpha^{mpj_1}) = \alpha^u + \alpha^{mpj_2}.$$

This can readily be transformed into

$$\alpha^{mqi+u}(1-\alpha^{-mqi}) = \alpha^{mpj_2}(1-\alpha^{mqi+mp(j_1-j_2)}),$$

which is written as follows by using u_{ij} :

$$\alpha^{mqi+u}\alpha^{u_{-i,0}}=\alpha^{mpj_2}\alpha^{u_{i,j_1-j_2}}.$$

Then we have

$$u = m(pj_2 - qi) + u_{ij} - u_{-i,0}$$
 (2.3)

for $1 \le i < pf$ and $1 \le j < qf$, where $j = j_1 - j_2$. Since $u_{ij} = u_{hl}$ if $pi + qj \equiv ph + ql \pmod{pqf}$, it is sufficient to check for (2.3) in the range of $1 \le i < pf$ and $1 \le j < q$. However, (2.3) readily proves to be impossible from the condition on u. Therefore the entries of A are relatively distinct.

Next, we examine the respective designs generated from sR_i 's, sC_j 's and sB's for $0 \le i < pf$, $0 \le j < qf$ and $s \in S_{mq}$. It follows straightforward from Lemma 2.1(i) that for each j, $\{sC_j + x \mid s \in S_{mq}, x \in V\}$ forms a B(v, pf, pf - 1). Thus $\{sC_j + x \mid 0 \le j < qf, s \in S_{mq}, x \in V\}$ is a B(v, pf, qf(pf - 1)). Similarly, it can easily be proved from Lemma 2.1(i) that $\{sB + x \mid s \in S_{mq}, x \in V\}$ forms a $B(v, pqf^2, qf(pqf^2 - 1))$.

As for the design generated from sR_i 's, by letting $R'_i = \alpha^{mqi}H_0^{mp}$, we have only to examine if

$$\{sR'_i + x \mid 0 \le i < pf, \ s \in S_{mg}, \ x \in V\}$$
 (2.4)

forms a BIB design. This is the same thing as examining $\{sR_i + x \mid 0 \le i < pf, s \in S_{mq}, x \in V\}$ since the differences from R'_i are the same as those from R_i . Note that $\{qi \pmod{p} \mid 0 \le i < p\} = \mathbb{Z}_p$ holds because of the assumption $\gcd(p,q) = 1$. Then it follows that

$$\{s\alpha^{mqi} \mid 0 \le i < p, \ s \in S_m\} = \{s\alpha^{mi} \mid 0 \le i < p, \ s \in S_m\} = S_{mp},$$

whence (2.4) can be regarded as qf copies of

$$\{tH_0^{mp} + x \mid t \in S_{mp}, \ x \in V\}.$$
 (2.5)

Lemma 2.1(i) guarantees that (2.5) forms a B(v, qf, qf-1). Therefore (2.4) becomes a B(v, qf, qf(qf-1)).

For case (a)', we take $A = \{sA + x \mid s \in S_{mq/2}, x \in V\}$, instead of (2.2). Then it can readily be proved from Lemma 2.1(i)' that the respective designs generated by sC_j 's and sB's for $0 \le j < qf$ and $s \in S_{mq/2}$ are a B(v, pf, qf(pf-1)/2) and a $B(v, pqf^2, qf(pqf^2-1)/2)$.

As for the design formed by the rows, i.e.,

$$\{sR'_i + x \mid 0 \le i < pf, \ s \in S_{ma/2}, \ x \in V\},$$
 (2.6)

we need to consider two cases depending on the parity of q.

(i) When q is odd (thus m is even and pqf is odd). In this case, since

$$S_{m/2} = S_m/\{1, -1\} \subset S_{mp}/\{1, -1\} = S_{mp/2},$$

by replacing the range of t in (2.5) with $t \in S_{mp/2}$, the set (2.6) of rows is proved to be a B(v, qf, qf(qf-1)/2).

(ii) When q is even. In this case, the parity of m does not make any difference. Since $S_m = S_m/\{1,-1\} \subset S_{mq}/\{1,-1\} = S_{mq/2}$, (2.6) can be considered as qf/2 copies of (2.5). Then it turns out that (2.6) is a B(v, qf, qf(qf-1)/2).

(b) Using A of (2.1), we newly define a $pf \times (qf+1)$ array by $A^* = [\alpha^u \mu | A]$, where $\mu^T = H_0^{mq}$, and a collection A^* of mqv arrays by $A^* = \{sA^* + x \mid s \in S_{mq}, x \in V\}$. Then, in a manner similar to case (a), we can prove that (V, A^*) is the desired BIBRC of (b). It is easy to see that the further condition $u \not\equiv -u_{i0} \pmod{m}$ is required for the elements of $\alpha^u \mu$ and those of A to be distinct from each other. Case (b)' can also be proved in the same way as (a)'.

Remark. By counting the number of no-good values as an integer u, it is easy to see that there does exist the required u for Theorem 2.2(a) and (a)' as long as $m \ge pqf^2$. Similarly, if $m \ge pf(qf+1)$, an integer u for Theorem 2.2(b) and (b)' definitely exists. Of course, there are still a number of designs generated by Theorem 2.2 which do not fulfill these sufficient conditions for existence. For example, when $(p, q, m, f; \alpha) = (3, 2, 3, 1; 2)$, we can take u = 2 for any cases of Theorem 2.2, and when $(p, q, m, f; \alpha) = (3, 2, 8, 2; 5)$, u = 2 is admissible for any cases of the theorem.

Here is another refinement of a theorem in [6]. By replacing m with 2m, Theorem 2.3 becomes Theorem 3.3 in [6].

Theorem 2.3 Let v = mpqf + 1 be a prime power and let gcd(p,q) = 1. Write $\alpha^{w_i} = 1 - \alpha^{mqi}$ for $1 \le i < pf$ and $\alpha^{u_j} = 1 - \alpha^{mpj}$ for $1 \le j < qf$, where $0 \le w_i, u_j < v - 1$.

(a) If $f \le m$ and there exists an integer u such that $u \not\equiv mpqf/2, u_j - w_i \pmod{m}$ for any i and j, then there exists a BIBRC with parameters

$$v = mpqf + 1, \quad b = mpqv, \quad r = k_1k_2mpq,$$

 $k_1 = pf, \quad k_2 = qf, \quad \lambda = pqf(pf - 1)(qf - 1).$

(b) If f < m and there exists an integer u such that $u \not\equiv mpqf/2, -w_i, u_j - w_i \pmod{m}$ for any i and j, then there exists a BIBRC with parameters

$$v = mpqf + 1, \quad b = mpqv, \quad r = k_1k_2mpq,$$

 $k_1 = pf, \quad k_2 = qf + 1, \quad \lambda = pqf(pf - 1)(qf + 1).$

(c) If f < m and there exists an integer u such that $u \not\equiv mpqf/2, u_j, -w_i, u_j - w_i \pmod{m}$ for any i and j, then there exists a BIBRC with parameters

$$v = mpqf + 1, \quad b = mpqv, \quad r = pk_1k_2mq,$$

 $k_1 = pf + 1, \quad k_2 = qf + 1, \quad \lambda = pqf(pf + 1)(qf + 1).$

Moreover, if mpq is even and f is odd, then there exist BIBRC with the following parameters corresponding to (a), (b) and (c):

(a)'
$$v = mpqf + 1$$
, $b = mpqv/2$, $r = k_1k_2mpq/2$, $k_1 = pf$, $k_2 = qf$, $\lambda = pqf(pf-1)(qf-1)/2$.

(b)'
$$v = mpqf + 1$$
, $b = mpqv/2$, $r = k_1k_2mpq/2$, $k_1 = pf$, $k_2 = qf + 1$, $\lambda = pqf(pf - 1)(qf + 1)/2$.

(c)'
$$v = mpqf + 1$$
, $b = mpqv/2$, $r = k_1k_2mpq/2$, $k_1 = pf + 1$, $k_2 = qf + 1$, $\lambda = pqf(pf + 1)(qf + 1)/2$.

Proof. (a) Define a $pf \times qf$ array A by the (i, j)th entry as follows:

$$A = [\alpha^{mqi+u} + \alpha^{mpj}], \quad 0 \le i < pf, \ 0 \le j < qf, \tag{2.7}$$

and a collection A of mpqv arrays by $A = \{sA + x \mid s \in S_{mpq}, x \in V\}$. Then the *i*th row R_i and the *j*th column C_j of A can be regarded respectively as

$$R_i = \alpha^{mqi+u} + H_0^{mp}$$
 and $C_j = \alpha^{mpj} + \alpha^u H_0^{mq}$.

Then it is readily confirmed by Lemma 2.1(i) that

$$\{sR_i + x \mid 0 \le i < pf, \ s \in S_{mpq}, \ x \in V\}$$

and

$$\{sC_j + x \mid 0 \le i < qf, \ s \in S_{mpq}, \ x \in V\}$$

become a B(v, qf, pqf(qf-1)) and a B(v, pf, pqf(pf-1)), respectively. Considering the array A as a block B of size pqf^2 , we can represent an arbitrary element of B as the (pr+i', q(r+t)+j')th entry

$$\alpha^{mq(pr+i')+u} + \alpha^{mp(q(r+t)+j')} = \alpha^{mpqr} \beta_{i',i'}$$

of A, where $\beta_{i'j't} = \alpha^{mqi'+u} + \alpha^{mp(qt+j')}$, for $0 \le r, t < f$, $0 \le i' < p$ and $0 \le j' < q$. In order to prove the elements of B to be distinct from each other, we need to show that the elements in

$$\{\beta_{i'j't} \mid 0 \le i' < p, \ 0 \le j' < q, \ 0 \le t < f\}$$

are relatively distinct over S_{mpq} . Note that because of the fact that $\alpha^{mpqf/2} = -1$ and the assumption that $u \not\equiv mpqf/2 \pmod{m}$, $\beta_{i'j't} \neq 0$ is guaranteed for any i', j' and t. Now, suppose that two of the entries in A are in the same coset of H_0^{mpq} , i.e.,

$$\alpha^{mpqr}(\alpha^{mqi_1+u} + \alpha^{mp(qt_1+j_1)}) = \alpha^{mqi_2+u} + \alpha^{mp(qt_2+j_2)}.$$

With some deformations, we have

$$u = m\{p(qt_2 + j_2) - pqr - qi_1\} + u_j - w_i,$$

where $i = i_2 - i_1 - pr$ and $j = q(t_1 - t_2 + r) + j_1 - j_2$. However this is impossible because of the condition $u \not\equiv u_j - w_i \pmod{m}$. Thus the elements of B (equivalently the entries of A) are relatively distinct. Since B can be considered as a union of distinct pqf cosets of H_0^{mpq} , $\{sB + x \mid s \in S_{mpq}, x \in V\}$ becomes a $B(v, pqf^2, pqf(pqf^2 - 1))$. Thus (V, A) is the desired BIBRC of (a).

- (b) Define a $pf \times (qf+1)$ array A^* by $A^* = [\alpha^u \mu | A]$, where $\mu^T = H_0^{mq}$ and A is as defined by (2.7), and let $A^* = \{sA^* + x \mid s \in S_{mpq}, x \in V\}$. Then case (b) can be proved by using Lemma 2.1(i) and (ii). The condition on u is required for the entries of A^* to be distinct from each other.
- (c) Consider a $(pf+1) \times (qf+1)$ array by concatenating $\{0\} \cup H_0^{mp}$, as a new row, to A^* in the proof of case (b). Then Lemma 2.1(ii) ensures the existence of the desired BIBRC of (c).
- (a)', (b)' and (c)' can be proved by Lemma 2.1(i)' and (ii)' straightforwardly. □

Remark. A sufficient condition for the existence of an integer u required for Theorem 2.3(a) and (a)' is $m \ge (pf-1)(qf-1)+2$, that for (b) and (b)' is $m \ge qf(pf-1)+2$, and that for (c) and (c)' is $m \ge pqf^2+1$. Note that there are still a number of designs generated by Theorem 2.3 even if those conditions are not satisfied. For example, when when $(p,q,m,f;\alpha)=(5,2,5,2;2)$, we can take u=3 for any cases of Theorem 2.3, when $(p,q,m,f;\alpha)=(3,4,7,4;10)$, u=5 is admissible for any cases of the theorem.

As listed below, several constructions by Uddin and Morgan [17] are considered as special cases of Theorems 2.3.

- (i) Theorem 2.3(c) with p = q = 1 and f = 2t becomes Theorem 1(b) of [17].
- (ii) Theorem 2.3(b)' with p = 1, q = 2 and f = t becomes Theorem 3(b) of [17].
- (iii) Theorem 2.3(c)' with p = 1, q = 2 and f = t becomes Theorem 3(d) of [17].

Eventually our constructions make up for designs with parameters which cannot be obtained through the constructions due to Hishida and Jimbo [6], and generalize Theorems 1, 2 and 3 in Uddin and Morgan [17].

3. Constructions for BIBRC not having completely balanced property

In this section, as an extension of Theorems 4 and 5 in [17], two direct constructions for BIBRC both of which are not completely balanced are presented. Though resultant designs would not have fewer replications than the designs which have been known previously, the constructions are meaningful in the sense that those can provide a BIBRC (v, b, r, k, k, λ) or a BIBRC $(v, b', r', k + 1, k + 1, \lambda')$ such that v - 1 is divisible by neither k nor k - 1.

Theorem 3.1 Let v = 4mf + 1 be a prime power and S_m be a system of distinct representatives for the cosets of $V \setminus \{0\}$ modulo H_0^m .

(a) If there exist $n \leq \sqrt{m/f}$ distinct integers e_i , $0 \leq i < n$, such that the elements in

$$\{\alpha^{e_j}(1 + \alpha^{e_i - e_j + m(2t+1)}) \mid 0 \le i, j < n, \ 0 \le t < f\}$$
 (3.1)

are relatively distinct over S_m , then there exists a BIBRC with parameters

$$v = 4mf + 1$$
, $b = mv$, $r = 4mn^2f^2$,
 $k_1 = k_2 = 2nf$, $\lambda = n^2f(2nf - 1)^2$.

(b) For some integer n satisfying $n(nf+1) \le m$, if there exist n distinct integers e_i , $1 \le i \le n$, such that the elements in

$$\{\alpha^{e_i} \mid 0 \leq i < n\} \cup \{\alpha^{e_j}(1 + \alpha^{e_i - e_j + m(2t+1)}) \mid 0 \leq i, j < n, \ 0 \leq t < f\}$$
 are relatively distinct over S_m , then there exists a BIBRC with pa-

are relatively distinct over S_m , then there exists a BIBRC with parameters

$$v = 4mf + 1$$
, $b = mv$, $r = m(2nf + 1)^2$,
 $k_1 = k_2 = 2nf + 1$, $\lambda = n^2 f(2nf + 1)^2$.

Proof. (a) Define a $2nf \times 2nf$ array A by the (2fi + h, 2fj + l)th entry as follows:

$$A = \left[\alpha^{e_i + m(2h+1)} + \alpha^{e_j + 2ml}\right], \quad 0 \le i, j < n, \ 0 \le h, l < 2f, \tag{3.2}$$

and a collection A of mv arrays by $A = \{sA + x \mid s \in S_m, x \in V\}$. Then we can represent any row and column of A by the (2fi + h)th row R_{2fi+h} and the (2fj + l)th column C_{2fj+l} which are regarded as

$$R_{2fi+h} = \alpha^{e_i + m(2h+1)} + \bigcup_{j=0}^{n-1} \alpha^{e_j} H_0^{2m}$$

and

$$C_{2fj+l} = \alpha^{e_j + 2ml} + \bigcup_{i=0}^{n-1} \alpha^{e_i + m} H_0^{2m}.$$

Note that the sets of differences from R_{2fi+h} and C_{2fj+l} are the same as those from

$$R'_{2fi+h} = \bigcup_{j=0}^{n-1} \alpha^{e_j} H_0^{2m}$$
 and $C'_{2fj+l} = \bigcup_{i=0}^{n-1} \alpha^{e_i+m} H_0^{2m}$,

respectively. This means that examining the design generated from sR_{2fi+h} 's and sC_{2fj+l} 's for $s \in S_m$ equates to examining the design generated from sR'_{2fi+h} 's and sC'_{2fj+l} 's. Since

$$\begin{aligned} & \{ sR'_{2fi+h} + x \mid s \in S_m, x \in V \} \cup \{ sC'_{2fi+h} + x \mid s \in S_m, x \in V \} \\ &= \{ sR'_{2fi+h} + x \mid s \in S_{2m}, x \in V \}, \end{aligned}$$

by using Lemma 2.1(i) it turns out that $\{sR_{2fi+h} + x \mid s \in S_m, x \in V\} \cup \{sC_{2fi+h} + x \mid s \in S_m, x \in V\}$ becomes a B(v, 2nf, n(2nf-1)). Thus the set of rows and columns of sA's for $s \in S_m$ generates a $B(v, 2nf, 2n^2f(2nf-1))$.

By flattening out the array A into a block B of size $4n^2f^2$, we have

$$\begin{split} B &= \{\alpha^{e_i + m(2h + 1)} + \alpha^{e_j + 2ml} \mid 0 \le i, j < n, \ 0 \le h, l < 2f\} \\ &= \{\alpha^{e_j + 2ml} (1 + \alpha^{e_i - e_j + m} H_0^{2m}) \mid 0 \le i, j < n, \ 0 \le l < 2f\} \\ &= \{\alpha^{e_j} (1 + \alpha^{e_i - e_j + m} H_0^{2m}) \otimes H_0^{2m} \mid 0 \le i, j < n\}. \end{split}$$

Here, by noting that for $f \leq t < 2f$,

$$\alpha^{e_j}(1+\alpha^{e_i-e_j+m(2t+1)})=\alpha^{e_i+m(2t+1)}(1+\alpha^{e_j-e_i+m(2t'+1)})$$

holds, where t' = 2f - t - 1 (and then $0 \le t' < f$), the block B can be further transformed as follows:

$$B = \{\alpha^{e_j}(1 + \alpha^{e_i - e_j + m(2t+1)}) \otimes H_0^m \mid 0 \le i, j < n, \ 0 \le t < f\}.$$
 (3.3)

As obvious from (3.3), the condition on e_j ($0 \le j < n$) is necessary for the elements of B (thus the entries of A) to be distinct from each other. Then it is readily shown from Lemma 2.1(i) that $\{sB + x \mid s \in S_m, x \in V\}$ is a $B(v, 4n^2f^2, n^2f(4n^2f^2 - 1))$. Thus (V, A) is the desired BIBRC of (a).

(b) For case (b), we take a $(2nf+1) \times (2nf+1)$ array A^* as follows:

$$A^* = \left[\begin{array}{cc} 0 & \boldsymbol{\mu}^{\mathrm{T}} \\ \alpha^m \boldsymbol{\mu} & A \end{array} \right],$$

where $\mu^{T} = \bigcup_{j=0}^{n-1} \alpha^{e_j} H_0^{2m}$ and A is as defined by (3.2). Then, in a manner similar to case (a), we can verify that the set of rows and columns of sA^* 's for $s \in S_m$ generates a $B(v, 2nf + 1, n(2nf + 1)^2)$.

Now, let B^* be a block of size $(2nf+1)^2$ obtained by flattening out the array A^* . Since B^* can be written as

$$B^* = \{0\} \cup (\bigcup_{i=0}^{n-1} \alpha^{e_i} H_0^m) \cup B,$$

by using Lemma 2.1(ii) it is verified that sB^* 's generate a $B(v, (2nf + 1)^2, n(nf + 1)(2nf + 1)^2)$. Thus case (b) has also been proved.

Example. When v=53, m=13, f=1 and n=3. Take $\alpha=2$ as a primitive element of GF(53). In this case, a system of distinct representatives for the cosets of GF(53) \ {0} modulo H_0^{13} is given by $S_{13}=\{1,2,4,8,16,32,11,22,44,35,17,34,15\}$. In Theorem 3.1(a), if we set $e_0=0$, $e_1=1$ and $e_2=2$, then (3.1) will be $\{31,8,15,32,9,16,34,11,18\}\subset S_{13}$, which satisfies the required condition. An array A defined by (3.2) is given as follows:

Then the design generated from sA's for $s \in S_{13}$ is a BIBRC with parameters v=53, b=689, r=468, $k_1=k_2=6$ and $\lambda=225$, denoted by BIBRC(53,689,468,6,6,225). Furthermore, a BIBRC(53,689,637,7,7,441) can be obtained from Theorem 3.1(b) since $\{1,2,4\} \cup \{31,8,15,32,9,16,34,11,18\} \subset S_{13}$.

There are much more parameter sets which satisfy the conditions of Theorem 3.1(a) and (b) other than the example above, e.g., $(m, f; n, \alpha) = (14, 2; 2, 3), (15, 3; 2, 3), (16, 3; 2, 5), (17, 2; 2, 3)$ with $\{e_0, e_1\} = \{0, 1\}$ in common.

Theorem 3.2 Let v = 4mf + 1 be a prime power with f odd and S_{4m} be a system of distinct representatives for the cosets of $V \setminus \{0\}$ modulo H_0^{4m} .

(a) If there exist $n \ (\leq 2\sqrt{m/f})$ distinct integers e_i , $1 \leq i \leq n$, such that the elements in

$$\{\alpha^{e_i} + \alpha^{e_j + m} H_0^{4m} \mid 0 \le i, j < n\}$$
 (3.4)

are relatively distinct over S_{4m} , then there exists a BIBRC with parameters

$$v = 4mf + 1$$
, $b = mv$, $r = mn^2f^2$,
 $k_1 = k_2 = nf$, $\lambda = n^2f(nf - 1)^2/4$.

(b) For some integer n satisfying $n(nf+2) \le 4m$, if there exist n distinct integers e_i , $1 \le i \le n$, such that the elements in

$$(\{1,\alpha^m\} \otimes \{\alpha^{e_i} \mid 0 \le i < n\}) \cup \{\alpha^{e_i} + \alpha^{e_j + m} H_0^{4m} \mid 0 \le i, j < n\}$$
 (3.5)

are relatively distinct over S_{4m} , then there exists a BIBRC with parameters

$$v = 4mf + 1$$
, $b = mv$, $r = m(nf + 1)^2$,
 $k_1 = k_2 = nf + 1$, $\lambda = n^2 f(nf + 1)^2/4$.

Proof. (a) Define an $nf \times nf$ array A by the (fi + h, fj + l)th entry as follows:

$$A = \left[\alpha^{e_i + m(4h+1)} + \alpha^{e_j + 4ml}\right], \quad 0 \le i, j < n, \ 0 \le h, l < f, \tag{3.6}$$

and a collection A of mv arrays by $A = \{sA + x \mid s \in S_m, x \in V\}$. In this case, the (fi + h)th row R_{fi+h} and the (fj + l)th column C_{fj+l} of A can be regarded as

$$R_{fi+h} = \alpha^{e_i + m(4h+1)} + \bigcup_{j=0}^{n-1} \alpha^{e_j} H_0^{4m} \text{ and } C_{fj+l} = \alpha^{e_j + 4ml} + \bigcup_{i=0}^{n-1} \alpha^{e_i + m} H_0^{4m}.$$

By an analogous argument to that in the proof of Theorem 3.1, we first examine the design generated from sR'_{fi+h} 's and sC'_{fj+l} 's for $s \in S_m$, where

$$R'_{fi+h} = \bigcup_{j=0}^{n-1} \alpha^{e_j} H_0^{4m}$$
 and $C'_{fj+l} = \bigcup_{i=0}^{n-1} \alpha^{e_i+m} H_0^{4m}$.

It is easy to see that

$$\left\{ sR'_{fi+h} + x \mid s \in S_m, x \in V \right\} \cup \left\{ sC'_{fi+h} + x \mid s \in S_m, x \in V \right\} \\
 = \left\{ sR'_{fi+h} + x \mid s \in S_{2m}, x \in V \right\}.
 \tag{3.7}$$

With the assumption that f is odd, Lemma 2.1(i)' assures that (3.7) (equally $\{sR_{fi+h} + x \mid s \in S_m, x \in V\} \cup \{sC_{fi+h} + x \mid s \in S_m, x \in V\}$) is a

B(v, nf, n(nf-1)/2). Thus the set of rows and columns of sA's for $s \in S_m$ generates a $B(v, nf, n^2f(nf-1)/2)$.

Next, we examine the differences arising from a block B of size n^2f which is obtained by flattening out the array A. By noting that an arbitrary pair from A is in the same row, in the same column, or neither of the cases, the differences are classified into nf ΔR_0 's, nf ΔC_0 's and the entries in the addition table of ΔR_0 and $\Delta C_0 = \alpha^m \Delta R_0$ modulo v, where

$$\Delta R_0 = \Delta \cup_{j=0}^{n-1} \alpha^{e_j} H_0^{4m}
= \{ \alpha^{e_j} (1 - \alpha^{e_{j'} - e_j} H_0^{4m}) \otimes H_0^{2m} \mid 0 \le j < j' < n, \ j \ne j' \}
\cup \{ \alpha^{e_j} (1 - H_0^{4m} \setminus \{1\}) \otimes H_0^{4m} \mid 0 \le j < n \}.$$
(3.8)

Since

$$1 - H_0^{4m} \setminus \{1\} = \{(1 - \alpha^{4mt})\{1, -\alpha^{4m(f-t)}\} \mid 1 \le t \le (f-1)/2\}$$

and $-1 \in \alpha^{2m} H_0^{4m}$,

$$(1 - H_0^{4m} \setminus \{1\}) \otimes H_0^{4m} = \{(1 - \alpha^{4mt})H_0^{2m} \mid 1 \le t \le (f - 1)/2\}$$

holds, whence (3.8) can be transformed as follows:

$$\Delta R_0 = \{ \alpha^{e_j} (1 - \alpha^{e_{j'} - e_j} H_0^{4m}) \otimes H_0^{2m} \mid 0 \le j < j' < n, \ j \ne j' \}$$

$$\cup \{ \alpha^{e_j} (1 - \alpha^{4mt}) H_0^{2m} \setminus \{1\}) \mid 0 \le j < n, \ 1 \le t \le (f - 1)/2 \}.$$

By letting $\alpha^{e_i} - \alpha^{e_j + 4mk} = \alpha^{u_{ijk}}$ for some integer $0 \le u_{ijk} \le v - 2$, we have

$$\Delta R_0 = \{ \alpha^{u_{ijk}} H_0^{2m} \mid 1 \le i < j \le n, \ 0 \le k \le f - 1 \}$$

$$\cup \{ \alpha^{u_{iit}} H_0^{2m} \mid 1 < i < n, \ 1 < t < (f - 1)/2 \}.$$
(3.9)

Now, let $L(\Delta R_0, \Delta C_0)$ be the list of the entries in the addition table of ΔR_0 and ΔC_0 . Then $L(\Delta R_0, \Delta C_0)$ can be considered as a collection of the following four sets:

(i)
$$\{L(\alpha^{u_{ijk}}H_0^{2m}, \alpha^{u_{i'j'k'}+m}H_0^{2m}) \mid 1 \le i < j \le n, \ 1 \le i' < j' \le n, \ 0 \le k, k' \le f-1\};$$

(ii)
$$\{L(\alpha^{u_{ijk}}H_0^{2m},\alpha^{u_{i'i'k}+m}H_0^{2m}) \mid 1 \le i < j \le n, \ 1 \le i' \le n, \ 0 \le k \le f-1, \ 1 \le t \le (f-1)/2\};$$

(iii)
$$\{L(\alpha^{u_{i'i'}}H_0^{2m}, \alpha^{u_{ijk}+m}H_0^{2m}) \mid 1 \le i < j \le n, \ 1 \le i' \le n, \ 0 \le k \le f-1, \ 1 \le t \le (f-1)/2\};$$

$$(\text{iv}) \ \{L(\alpha^{u_{iii}}H_0^{2m},\alpha^{u_{i'i'i'}+m}H_0^{2m}) \mid 1 \leq i,i' \leq n, \ 1 \leq t,t' \leq (f-1)/2\}.$$

Note that $L(\alpha^{x_1}H_0^y, \alpha^{x_2}H_0^y) = \alpha^{x_1}H_0^y \otimes (1 + \alpha^{x_2-x_1}H_0^y) = \alpha^{x_2}H_0^y \otimes (1 + \alpha^{x_1-x_2}H_0^y)$ and $\alpha^{-m}H_0^{2m} = \alpha^mH_0^{2m}$. Then taking a union of the sets (ii) and (iii), we have

$$\begin{aligned} \{\alpha^{u_{ijk}}(1 + \alpha^{u_{i'i'}} - u_{ijk} + m H_0^{2m}) \otimes H_0^m \mid 1 \le i < j \le n, \ 1 \le i' \le n, \\ 0 \le k \le f - 1, \ 1 \le t \le (f - 1)/2 \}. \end{aligned}$$

On the other hand, by noting that for $f \leq t < 2f$,

$$\alpha^{u_{ijk}}(1+\alpha^{u_{i'j'k'}-u_{ijk}+m(2t+1)})=\alpha^{u_{i'j'k'}+m(2t+1)}(1+\alpha^{u_{ijk}-u_{i'j'k'}+m(2t'+1)})$$

holds, where t' = 2f - t - 1 (and then $0 \le t' < f$), we can calculate the set (i) as follows:

$$\begin{split} \{\alpha^{u_{ijk}}(1+\alpha^{u_{i'j'k'}-u_{ijk}+m}H_0^{2m})\otimes H_0^{2m}\mid 1\leq i< j\leq n,\ 1\leq i'< j'\leq n,\\ 0\leq k,k'\leq f-1\}\\ &=\{\alpha^{u_{ijk}}(1+\alpha^{u_{i'j'k'}-u_{ijk}+m(2t+1)})\otimes H_0^m\mid i< i',j\neq j',\ 1\leq i< j\leq n,\\ 1< i'< j'< n,\ 0< k< k'< f-1,\ 0< t< f\} \end{split}$$

Also the set (iv) is reduced to

$$\begin{split} &\{\alpha^{u_{ii\ell}}(1+\alpha^{u_{i'i'\ell'}-u_{ii\ell}+m}H_0^{2m})\otimes H_0^{2m}\mid 1\leq i,i'\leq n,\ 0\leq \ell,\ell'\leq (f-1)/2\}\\ &=\{\alpha^{u_{ii\ell}}(1+\alpha^{u_{i'i'\ell'}-u_{ii\ell}+m(2t+1)})\otimes H_0^m\mid 1\leq i< i'\leq n,\\ &\qquad 0\leq \ell,\ell'\leq (f-1)/2,\ 0\leq t< f\}. \end{split}$$

Then $\{sL(\Delta R_0, \Delta C_0) \mid s \in S_m\} = (n^2f(nf-1)^2/4)(\mathrm{GF}(v) \setminus \{0\})$ holds, which implies that sB's generate a $\mathrm{B}(v, n^2f^2, n^2f(nf-1)^2/4)$. Thus case (a) has been proved.

(b) For case (b), let

$$A^* = \left[\begin{array}{cc} 0 & \boldsymbol{\mu}^{\mathrm{T}} \\ \boldsymbol{\alpha}^m \boldsymbol{\mu} & A \end{array} \right]$$

be an $(nf+1) \times (nf+1)$ array, where $\mu^{T} = \bigcup_{j=0}^{n-1} \alpha^{e_j} H_0^{4m}$ and A is as defined by (3.6). By flattening out the array A^* into a block B^* of size $(nf+1)^2$, we have

$$B^* = \{0\} \cup (\{1,\alpha^m\} \otimes \bigcup_{i=0}^{n-1} \alpha^{e_i} H_0^{4m}) \cup B.$$

Then it is turned out that the condition on e_j is necessary for the elements of B^* (equivalently, the entries of A) to be distinct from each other.

By noting that $\Delta(\{0\} \cup \mu^{T}) = \Delta(\{0\} \cup R_0) = \mp R_0 \cup \Delta R_0$, where $\mp R_0 = \bigcup_{j=0}^{n-1} \alpha^{e_j} H_0^{2m}$ and ΔR_0 is given by (3.9), it is easily verified that the set of rows and columns of sA^* 's generates a $B(v, nf+1, n(nf+1)^2/2)$.

Next, we examine the design generated by sB's. The differences arising from B are classified into nf+1 $\Delta(\{0\}\cup R_0)$'s, nf+1 $\Delta(\{0\}\cup C_0)$'s and the elements in the addition table of $\Delta(\{0\}\cup R_0)$ and $\Delta(\{0\}\cup C_0)$. Let $L(\Delta(\{0\}\cup R_0),\Delta(\{0\}\cup C_0))$ be the list of the entries in the addition table of $\Delta(\{0\}\cup R_0)$ and $\Delta(\{0\}\cup C_0)$. Then $L(\Delta(\{0\}\cup R_0),\Delta(\{0\}\cup C_0))$ can be further divided into $L(\Delta R_0,\Delta C_0)$ and the following five sets:

(i)
$$\{L(\alpha^{e_i}H_0^{2m}, \alpha^{e_j+m}H_0^{2m}) \mid 1 \leq i, j \leq n\};$$

(ii)
$$\{L(\alpha^{e_i}H_0^{2m}, \alpha^{u_{i'j'k'}+m}H_0^{2m}) \mid 1 \le i \le n, \ 1 \le i' < j' \le n, \ 0 \le k' \le f-1\};$$

(iii)
$$\{L(\alpha^{e_i+m}H_0^{2m}, \alpha^{u_{i'j'k'}}H_0^{2m}) \mid 1 \le i \le n, \ 1 \le i' < j' \le n, \ 0 \le k' \le f-1\};$$

(iv)
$$\{L(\alpha^{e_i}H_0^{2m}, \alpha^{u_{i'i't}+m}H_0^{2m}) \mid 1 \le i, i' \le n, \ 1 \le t \le (f-1)/2\};$$

(v)
$$\{L(\alpha^{e_i+m}H_0^{2m}, \alpha^{u_{i'i'}}H_0^{2m}) \mid 1 \leq i, i' \leq n, 1 \leq t \leq (f-1)/2\}.$$

Taking unions of the sets (ii) and (iii), and the sets (iv) and (v), we have

$$\{\alpha^{e_i}(1+\alpha^{u_{i'j'k'}-e_j+m}H_0^{2m})\otimes H_0^m\mid 1\leq i\leq n,\ 1\leq i'< j'\leq n,\ 0\leq k'\leq f-1\},$$

and

$$\{\alpha^{e_i}(1+\alpha^{u_{i'i'}}e^{-e_i+m}H_0^{2m})\otimes H_0^m\mid 1\leq i,i'\leq n,\ 1\leq t\leq (f-1)/2\},$$

respectively. Meanwhile, the set (i) is just the same as (3.3). Then

$$\{sL(\Delta(\{0\} \cup R_0), \Delta(\{0\} \cup C_0)) \mid s \in S_m\} = (n^2 f(nf+1)^2/4)(GF(v) \setminus \{0\})$$

holds, which implies that sB^* 's generate a $B(v, n^2f^2, n^2f(nf+1)^2/4)$. Thus $A^* = \{sA^* + x \mid s \in S_m, x \in V\}$ is the desired BIBRC of (b).

The followings are examples of parameter sets which satisfy the conditions of Theorem 3.2(a) and (b).

$$(m, f; n, \alpha) = (13, 3; 2, 5)$$
 and $\{e_0, e_1\} = \{0, 1\},$
 $(m, f; n, \alpha) = (14, 5; 2, 3)$ and $\{e_0, e_1\} = \{0, 5\}.$

Theorems 4 and 5 in [17] are considered as special cases of Theorems 3.1 and 3.2, i.e., Theorems 3.1 and 3.2 with n = 1 and $e_0 = 0$.

Acknowledgments

The work was supported in part by JSPS Grant-in-Aid for Scientific Research (B)15340035 to M. Jimbo, by Ministry of Education, Culture, Sports, Science and Technology of Japan, Grant-in-Aid for Young Scientists (B)1570023 to M. Mishima, and by JSPS Research Fellow 09978 to Y. Mutoh.

References

- H.L. Agrawal and J. Prasad, Some methods of construction of balanced incomplete block designs with nested rows and columns, *Biometrika* 69 (1982), 481–483.
- [2] H.L. Agrawal and J. Prasad, On construction of balanced incomplete block designs with nested rows and columns, Sankhyā B 45 (1983), 345–350.
- [3] I. Anderson, Combinatorial Designs, Ellis Horwood, Chichester, 1990.
- [4] T. Beth, D. Jungnickel and H. Lenz, Design Theory (Second ed.), Cambridge Univ. Press, Cambridge, 1999.
- [5] C.-S. Cheng, A method for constructing balanced incomplete-block designs with nested rows and columns, *Biometrika* 73 (1986), 695-700.
- [6] T. Hishida and M. Jimbo, Constructions of balanced incomplete block designs with nested rows and columns, J. Statist. Plann. Inference 106 (2002), 47-56.
- [7] M. Jimbo and S. Kuriki, Constructions of nested designs, Ars Combin. 16 (1983), 275–285.
- [8] J.P. Morgan, Nested Designs, in: S. Ghosh and C.R. Rao, eds., Handbook of Statistics 13, North-Holland, 1996, 939-976.
- [9] J.P. Morgan and N. Uddin, Optimality and construction of nested row and column designs, J. Statist. Plann. Inference 37 (1993), 81-93.
- [10] R. Mukerjee and S. Gupta, Geometric construction of balanced block designs with nested rows and columns, *Discrete Math.* 91 (1991), 105– 108.
- [11] K. Nasu, Y. Mutoh and M. Jimbo, Constructions of nested designs by affine geometries, submitted.

- [12] D.A. Preece, Nested balanced incomplete block designs, *Biometrika* 54 (1967), 479–486.
- [13] M. Singh and A. Dey, Block designs with nested rows and columns, *Biometrika* 66 (1979), 321-326.
- [14] P.R. Sreenath, Construction of some balanced incomplete block designs with nested rows and columns, *Biometrika* 76 (1989), 399-402.
- [15] D.J. Street, Graeco-Latin and nested row and column designs, in: K.L. McAvaney, ed., Combinatorial Mathematics 8, Lecture Notes in Mathematics 884, 1983, 301-313.
- [16] N. Uddin, On a recursive construction for balanced incomplete block designs with nested rows and columns, Metrika 42 (1995), 341-345.
- [17] N. Uddin and J.P. Morgan, Some constructions for balanced incomplete block designs with nested rows and columns, *Biometrika* 77 (1990), 193-202.
- [18] R.M. Wilson, Cyclotomy and difference families in elementary abelian groups, J. Number Theory 4 (1972), 17-47.