Discrete Mathematics 92 (1991) 321–328
North-Holland

Row-column directed block designs

D.G. Sarvate and R.C. Hamm

Department of Mathematics, College of Charleston, SC 29424, USA

Received 20 December 1988
Revised 19 April 1989

Dedicated to Professor R.G. Stanton on the occasion of his 68th birthday.

Abstract

Sarvate, D.G. and R.C. Hamm, Row-column directed block designs, Discrete Mathematics 92 (1991) 321–328.

A balanced incomplete block design (BIBD) is called a row-column directed BIBD (RCDBIBD) if:

(i) it is directed in the usual sense, i.e., each ordered pair of points occurs an equal number of times in the blocks (directed column wise), and

(ii) the blocks are arranged in such a way that (a) each point occurs an equal number of times in each row, and (b) each ordered pair of distinct points occurs an almost equal number of times in the rows.

The present paper gives construction techniques for RCDBIBDs and proves that the necessary conditions are sufficient for the existence of RCDBIBDs with block size 2. Existence of RCDBIBDs with block size 3 and $v \equiv 1 \bmod 6$ is shown and it is proved that an RCDBIBD$(7, 7, 4, 4, 1^*)$ does not exist.

1. Introduction

A *balanced incomplete block design* BIBD(v, b, r, k, λ) is an arrangement of v points into blocks of size k such that each point occurs r times and each pair of points occurs in exactly λ blocks. For example, see Street and Street [11]. We will use BIBD(v, b, r, k, λ) and BIBD(v, k, λ) interchangeably. A directed BIBD, DBIBD(v, b, r, k, λ^*) is a BIBD$(v, k, 2\lambda)$ in which points in each block are arranged so that each ordered pair occurs a total of λ times. A block $a_1, a_2, \ldots, a_k$ of a DBIBD is said to have $k(k-1)/2$ ordered pairs (a_i, a_j) $i = 1, 2, \ldots, k-1; j = i+1, \ldots, k$. Directed designs have been studied by many authors. See for example, Colbourn and Harms [1], Dawson, Seberry and Skillicorn [2], Hamm, Lindner and Rodger [3], Hung and Mendelsohn [5], Seberry and Skillicorn [8], Street and Seberry [10] and Street and Wilson [12].

Consider the BIBD(4, 3, 2),

B_1	B_2	B_3	B_4
1	1	1	2
2	2	3	3
3	4	4	4

where the blocks are written vertically as columns. In each block the points can be ordered to get a DBIBD(4, 3, 1*) as follows:

B_1	B_2	B_3	B_4
1	2	3	4
2	4	1	3
3	1	4	2.

We can consider the above arrangement as a 3×4 matrix, where the columns form a DBIBD(4, 3, 1*) and each point occurs exactly once in each row. We also observe that each ordered pair (a, b) of points occurs at least once in the rows.

The above properties suggest the study of the following configuration.

Definition. A BIBD(v, b, $r = sk$, k, 2λ) is said to be *row-column directed* if:

(i) the BIBD is a DBIBD(v, k, λ^*),

(ii) the blocks are so arranged that each point occurs s times in each row, and

(iii) each ordered pair of disjoint points occurs $\lfloor ks^2/2 \rfloor$ times in the rows.

Recall that for any positive integer n, $\lfloor n/2 \rfloor = n/2$ if n is even and $(n-1)/2$ if n is odd.

A row-column directed BIBD with the parameters v, b, $r = ks$, k and 2λ will be denoted by RCDBIBD(v, k, λ^*).

2. Justification for the condition (ii)

In view of the condition (iii), a natural question may be whether we should let each point occur almost s times in each row. For example in the case $r = 3s + 2$ and $k = 3$, we could let each point occur $(s+1)$ times in two of the rows and s times in one row. We will show that such an arrangement is not possible for $k = 3$ and $\lambda = 2$.

If $v \equiv 0 \bmod 3$ then $v - 1 \equiv 2 \bmod 3$, i.e., $r \equiv 2 \bmod 3$. Let $r = 3s + 2$. Now any point, say a, can occur:

(i) $(s+1)$ times in the first and second rows and s times in the third row,

(ii) $(s+1)$ times in the first and third rows and s times in the second row, or

(iii) $(s+1)$ times in the second and third rows and s times in the first row.

Now we know that there are $v-1=3s+2$ pairs in the columns with a as the first entry. The only way we can have $3s+2$ such pairs is to arrange a in the first row $s+1$ times and in the second row s times. It is not possible for all the points to appear in the first row $(s+1)$ times and in the second row s times. In other words, if we relax the second condition in the definition, we get non-existence of such an arrangement for $k=3$ and $\lambda=2$.

3. Constructions of RCDBIBDs

Construction 1. If a difference set solution without extra starter blocks for a BIBD(v, k, λ) exists then a RCDBIBD(v, k, λ^*) can be constructed as follows: Write the blocks first, in any order, then write the blocks in the reverse order, reversing the points of the blocks as well, to get a RCDBIBD(v, k, λ^*). Proof of this construction will appear elsewhere in a paper by Hamm and Sarvate.

Example 1.1. Consider the BIBD$(7,3,1)$ generated by the starter block $(1,2,4)$. We obtain a RCDBIBD$(7,3,1^*)$ as follows:

$$\begin{array}{ccccccc@{\quad}ccccccc}
1&2&3&4&5&6&7&3&2&1&7&6&5&4\\
2&3&4&5&6&7&1&1&7&6&5&4&3&2\\
4&5&6&7&1&2&3&7&6&5&4&3&2&1.
\end{array}$$

Construction 2. If a RCDBIBD(v, k, λ^*), X, exists, then a RCDBIBD$(v, k, c\lambda^*)$ can be constructed for any positive integer c as follows: Let Y be the RCDBIBD(v, k, λ^*) obtained by writing the blocks of X in the reverse order. (Not the elements in the blocks.) Write the pair XY $c/2$ times if c is even and write the pair XY $(c-1)/2$ times followed by X once if c is odd. The resulting arrangement will be a RCDBIBD$(v, k, c\lambda^*)$. Observe that the only condition to check is the third condition. If $r=ks$ then each ordered pair (a, b) occurs $ks^2=\lceil ks^2/2\rceil+\lfloor ks^2/2\rfloor$ times in the pair XY. Therefore (a, b) occurs in the rows at least

$$((c-1)+(c-2)+\cdots+1)ks^2+(c/2)ks^2$$

times if c is even and

$$((c-1)+(c-2)+\cdots+1)ks^2+((c-1)/2)ks^2+\lfloor ks^2/2\rfloor$$

times if c is odd.

But this means that when c is even the ordered pair (a, b) occurs $kc^2s^2/2$ times, and when c is odd it occurs $\lfloor kc^2s^2/2\rfloor$ times. That is, the ordered pair (a, b) occurs in the design the required number of times.

Construction 3. RCDBIBD($2n, 2n, 2n, 2n, n^*$) can be constructed as follows.

Let L be the $2n \times 2n$ latin square defined as follows:

$$a_{ij} = \begin{cases} j-i+1 & i \leqslant n, j \leqslant n, \\ i+j-n & i > n, j \leqslant n, \\ 2+n-(i+j) & i \leqslant n, j > n, \\ i-j+1 & i > n, j > n, \end{cases}$$

where all operations are taken modulo $2n$. It is easy to see that L is a RCDBIBD($2n, 2n, 2n, 2n, n^*$). Notice that L can be subdivided into four $n \times n$ squares L_{11}, L_{12}, L_{21}, L_{22} as follows:

$$\begin{array}{ccccc|ccccc}
1 & 2 & \cdot & \cdots & n & 2n & 2n-1 & \cdots & n+2 & n+1 \\
2n & 1 & 2 & \cdots & n-1 & 2n-1 & \cdot & \cdots & & n \\
\vdots & & \ddots & & \vdots & \vdots & & \ddots & & \vdots \\
n+3 & & & 1 & 2 & n+2 & & & \cdot & 3 \\
n+2 & \cdot & \cdots & 2n & 1 & n+1 & n & \cdots & 3 & 2 \\
\hline
2 & 3 & \cdot & \cdots & \cdot\, n+1 & 1 & 2n & \cdots & \cdot & n+2 \\
3 & \cdot & & & n+2 & 2 & 1 & & & n+3 \\
\vdots & & \ddots & & \vdots & \vdots & & \ddots & & \vdots \\
n & & & & \cdot\, 2n-1 & n-1 & n & & \cdot & 2n \\
n+1 & \cdot & & \cdots & 2n & n & n-1 & \cdots & 2 & 1
\end{array}$$

where L_{22} is the transpose of L_{11} and L_{12} and L_{21} are reflections of each other through the reverse diagonal. The ordered pair (a, b) appears in the first n rows of L exactly the same number of times (b, a) appears in the last n rows. Since exactly one of (a, b) and (b, a) appears in every row we have (a, b) and (b, a) each appearing in n rows. Similarly (a, b) and (b, a) each appear in n columns.

Note that L can be constructed as follows:

(1) Cycle the row $(1, 2, \ldots, 2n)$ to generate a latin square,

(2) Reverse the order of the last n rows,

(3) Reverse the order of the last n columns.

Example 3.1. For $2n = 6$, we proceed as follows:

Step 1:
$$\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
6 & 1 & 2 & 3 & 4 & 5 \\
5 & 6 & 1 & 2 & 3 & 4 \\
4 & 5 & 6 & 1 & 2 & 3 \\
3 & 4 & 5 & 6 & 1 & 2 \\
2 & 3 & 4 & 5 & 6 & 1.
\end{array}$$

Step 2:

1	2	3	4	5	6
6	1	2	3	4	5
5	6	1	2	3	4
2	3	4	5	6	1
3	4	5	6	1	2
4	5	6	1	2	3.

Step 3:

1	2	3	6	5	4
6	1	2	5	4	3
5	6	1	4	3	2
2	3	4	1	6	5
3	4	5	2	1	6
4	5	6	3	2	1.

Construction 4. A RCDBIBD($2n$, $2n$, $2n-1$, $2n-1$, $(n-1)^*$) can be constructed by a method similar to the above construction.

Construct a BIBD($2n$, $2n$, $2n-1$, $2n-1$, $2n-2$) by writing the blocks generated by $1, 2, \ldots, 2n$ and then deleting the last row. Now write the last n columns in the reverse order and then write the last n rows in the reverse order. It can be checked that the resulting configuration is the required RCDBIBD.

Example 4.1.

1 6 5	2 3 4
2 1 6	3 4 5
5 4 3	6 1 2
4 3 2	5 6 1
3 2 1	4 5 6.

4. Existence of a RCDBIBD(v, 2, λ^*)

RCDBIBD(v, 2, λ^*) exists for any v and any λ. We use part of Construction 1 for the existence of RCDBIBD(v, 2, 1^*). Write all the $v(v-1)/2$ pairs in any order to get BIBD(v, 2, 1). Now write the pairs in the reverse order, reversing the points in each pair as well. We obtain the required design. Now apply Construction 2 to obtain RCDBIBD(v, 2, λ^*).

5. Existence of a RCDBIBD(v, 3, λ^*) for $v \equiv 1 \bmod 6$

The necessary condition for the existence of RCDBIBD(v, 3, 1*) is $v \equiv 1 \bmod 3$, i.e. $v \equiv 1 \bmod 6$ or $v \equiv 4 \bmod 6$. If $v \equiv 1 \bmod 6$ then it is well known (for example, see [9]) that a cyclic BIBD(v, 3, 1) exists, therefore by Construction 1 a RCDBIBD(v, 3, 1*) exists for $v \equiv 1 \bmod 6$. Hence RCDBIBD(v, 3, λ^*) exists for all λ and $v \equiv 1 \bmod 6$.

Remark. Not much is known about the existence of RCDBIBDs(v, 3, λ^*) for $v \equiv 4 \bmod 6$. We have presented a RCDBIBD(4, 3, 1*) in the introduction. A RCDBIBD(10, 3, 1*) is given below.

$$\begin{array}{cccccccccccccc}
6&7&8&9&5&0&4&3&2&1&6&7&8&9&5\\
0&1&2&3&4&1&0&4&3&2&9&8&6&7&8\\
3&4&0&1&2&5&9&8&7&6&4&0&1&2&3\\
\\
9&8&7&6&5&2&3&4&0&1&2&1&0&4&3\\
8&7&6&5&9&1&2&3&4&0&8&7&6&5&9\\
5&9&8&7&6&9&5&6&7&8&4&3&2&1&0.
\end{array}$$

6. Non-existence of RCDBIBD(7, 4, 1*)

Assume that a RCDBIBD(7, 4, 1*) exists. Each element i will appear as the first entry in twelve of the ordered pairs from the rows. Without loss of generality let $\{1, 2, 3, 4\}$ be the first block. If t_{ij} denotes the number of pairs of the type $(i, .)$ in the jth row for $i = 1, 2, 3, 4$ and $j = 1, 2, 3, 4$, then we have the following situation:

(a) $t_{ii} = 6$,

(b) $t_{12} + t_{13} + t_{14} = 6, \qquad t_{21} + t_{23} + t_{24} = 6,$

$t_{31} + t_{32} + t_{34} = 6, \qquad t_{41} + t_{42} + t_{43} = 6.$

Now $x + y + z = 6$ has 6 possible solutions, namely $\{6, 0, 0\}$, $\{5, 1, 0\}$, $\{4, 1, 1\}$, $\{4, 2, 0\}$, $\{3, 2, 1\}$ and $\{3, 3, 0\}$. But for our purposes a possible solution cannot have a repeated value because a point cannot occur twice in the same block. Therefore the only possible solutions are $\{5, 1, 0\}$, $\{4, 2, 0\}$ and $\{3, 2, 1\}$. This means that two of the four equations in (b) above have the same solution thereby putting the corresponding two elements in the same columns. Thus two of the four elements $\{1, 2, 3, 4\}$ occur together in three blocks in addition to the first block. But in the underlying BIBD each pair occurs together in $2\lambda = 2$ blocks, a contradiction.

This example suggests the following: If the number of partitions of $(k-1)(v-1)/2$ as a sum of $(k-1)$ distinct integers is less than k then no RCDBIBD$(v, k, 1^*)$ exists.

7. Applications

The structure of the RCDBIBD permits us to use them whenever we can use a directed design and/or a block design. For example, they can be used for the construction of rows of orthogonal designs using the techniques in Kharaghani [6] or Hammer, Sarvate and Seberry [4]. A more interesting application may be to use it in encryption in which we can use different pairs of symbols to represent the same pair of message alphabets as follows: Label the $b(b-2)/2+k(k-1)/2$ ways of selecting a pair from a given row and a block. Now a pair of alphabets can be transmitted by using two symbols. The first being the row or column (block) number, depending on the key, and the second symbol will be one of the labels corresponding to the position of the pair in the row or in the column. A natural generalization of the RCDBIBDs to t-RCDBIBDs can be used to compress the message because then we can transmit a t-tuple of alphabets by using two symbols. The usual random number generator and permutation techniques can be applied to further strengthen the complexity of the algorithm. For similar encryption methods see, for example, Sarvate and Seberry [7]. One of the referees has suggested that further applications can be found in the paper Undiminished residual effects designs and their suggested applications by E. Lakatos and D. Raghavarao, Communications in statistics—theory and methods 16 (1987) 1345–1359.

Acknowledgement

We would like to thank Dr. Warwick de Launey for raising the question of directing designs row-wise in a conversation.

References

[1] C.J. Colbourn and J.J. Harms, Directing triple systems, Ars Combin. 15 (1983) 261–266.

[2] J.E. Dawson, J. Seberry and D.B. Skillicorn, The directed packing numbers DD(t, v, v), $t \geq 4$, Combinatorica 4 (2–3) (1984) 121–130.

[3] R.C. Hamm, C.C. Lindner and C.A. Rodger, Linear embeddings of partial directed triple systems with $\lambda=1$ and partial triple systems with $\lambda=2$, Ars Combin. 16 (1983) 11–16.

[4] J. Hammer, D.G. Sarvate and J. Seberry, A note on orthogonal designs, Ars Combin. 24 (1987) 93–100.

[5] S.H.Y. Hung and N.S. Mendelsohn, Directed triple systems, J. Combin. Theory Ser. A 14 (1973) 310–318.

[6] H. Kharaghani, New class of weighing matrices, Ars Combin. 19 (1985) 69–73.
[7] D.G. Sarvate and J. Seberry, Encryption methods based on combinatorial designs, Ars Combin. 21 A (1986) 237–246.
[8] J. Seberry and D.B. Skillicorn, All directed designs with $k = 3$ exist, J. Combin. Theory Ser. A 29 (1980) 244–248.
[9] R.G. Stanton and I.P. Goulden, Graph factorization, general triple systems and cyclic triple systems, Aequationes Math. 22 (1981) 1–28.
[10] D.J. Street and J. Seberry, All DBIBDs with block size four exist, Utilitas Math. 18 (1980) 161–174.
[11] A.P. Street and D.J. Street, Combinatorics of Experimental Designs (Clarendon Press, Oxford, 1987).
[12] D.J. Street and W. Wilson, On directed balanced incomplete block designs with block size 5, Utilitas Math. 18 (1980) 161–174.