THEORY OF COMBINATORIAL DESIGNS WITH APPLICATIONS TO ENCRYPTION AND THE DESIGN OF EXPERIMENTS

by
Dinesh Gopalrao Sarvate

A thesis submitted in fulfilment of
the requirements for the degree of
Doctor of Philosophy

in the

Department of Applied Mathematics
The University of Sydney
March 1987

Dedicated to my grandparents

Mr. Laxman N. Golwalkar

Mr. Ramchandra D. Sarvate

and

Mrs. Saraswatibai Golwalkar

Mrs. Sumatibai Sarvate

This thesis is my own work, except where specifically acknowledged. I have not previously submitted any part of this work for a degree at this or any other university.

D. G. Sarvate

(Dinesh G. Sarvate)

ACKNOWLEDGEMENTS

It is a great pleasure for me to acknowledge the encouragement, guidance and support - financial, emotional and above all, educational - which Dr. Jennifer Seberry has extended towards me, from the day I first met her.

Thank you, Jennie, for your now well-known enthusiasm and constructive guidance to your students in general and to me, in particular.

One of the best things to happen to me in Sydney was my introduction to Mr. J. Hammer, with whom I have had numerous discussions, to my great benefit. I sincerely thank him for his help.

I am indebted to Professor Anne Penfold Street in more than one way. I take this opportunity to gratefully thank her.

I am thankful to my co-supervisor, Associate Professor D. E. Winch, for his support and cooperation.

Dr. Elizabeth J. Billington and Dr. D. R. Breach very kindly reviewed the manuscript. Their helpful suggestions and remarks have greatly improved the thesis.

I wish to thank Mr. Warwick de Launey and Dr. Jeremy E. Dawson for their help, particularly in the early stages of the work.

Thanks are due to Mr. John Limnios, Mrs. Swati Sarvate and Mr. David Sim for their help in the preparation of the thesis.

PUBLICATIONS

1. "All directed GDDs with block size three, $\lambda_1=0$, exist", *Utilitas Mathematica*, 26, 1984, 311-317.

2. "A note on equi-neighboured block designs", *Utilitas Mathematica*, 28, 1985, 91-98.

3. "Some results on directed and cyclic designs", *Ars Combinatoria*, 19A, 1985, 179-190.

4. "All simple BIBDs with block size 3 exist", *Ars Combinatoria*, 21A, 1986, 257-270.

5. "Block designs without repeated blocks", *Ars Combinatoria*, 21, 1986, 71-87.

6. "On a BIBD construction", *Ars Combinatoria*, 22, 1986, 165-169.

7. "Non-existence of certain GBRD's", *Ars Combinatoria*, 18, 1984, 5-20, with W. de Launey.

8. "Generalised Bhaskar Rao designs with block size 3 over Z_4", *Ars Combinatoria*, 19A, 1985, 273-286, with W. de Launey and J. Seberry.

9. "Encryption using Hungarian rings", *Discrete Applied Mathematics*, 16, 1987, 151-155, with J. Hammer.

10. "On the introduction of block designs by graphs", submitted, with J. Hammer.

11. "A note on orthogonal designs", *Ars Combinatoria*, to appear, with J. Hammer and J. Seberry.

12. "Colourable designs, new group divisible designs and pairwise balanced designs", *J. of Stat. Plan. and Inf.*, 15, 1987, 379-389, with C.A. Roger and J. Seberry.

13. "Encryption methods based on combinatorial designs", *Ars Combinatoria*, 21A, 1986, 237-246, with J. Seberry.

Table of contents

INTRODUCTION

A *pairwise balanced design*, PBD [K, λ ; v], is a pair (S, β) where S is a v-set (of points), β is a class of subsets of S (called blocks) such that for any block B in β, $|B| \in K$ and any pair of distinct points of S is contained in exactly λ of the blocks of β. If $K = \{ k \}$ then the design is called a *balanced incomplete block design*, BIBD (v, k, λ). The constant λ is called the index of the design. If any t-set of distinct points of S is contained in exactly λ of the blocks of β, then the design is called a *t-design*. The necessary conditions for the existence of BIBD(v, k, λ) are

$$vr = bk$$

$$\lambda(v-1) = r(k-1),$$

and $$b \geq v.$$

An *association scheme* with m associate classes on a v-set S is a family of m symmetric anti-reflexive binary relations on S, such that:

(i) any two distinct elements of S are i^{th} associates for exactly one value of i, where $1 \leq i \leq m$;

(ii) each element of S has n_i i^{th} associates, $1 \leq i \leq m$;

(iii) for each, $1 \leq i \leq m$, if x and y are i^{th} associates then there are P^i_{jk} elements of S which are both j^{th} associates of x and k^{th} associates of y. The numbers v, n_i ($1 \leq i \leq m$), and P^i_{jk} ($1 \leq i, j, k \leq m$) are called the parameters of the association scheme.

From the above definition, we see that $P^i_{jk} = P^i_{kj}$.

A *partially balanced incomplete block design* with m associate classes (PBIBD(m)) is a design based on a v-set S, with b blocks each of

size k and replication number r, such that there is an association scheme with m classes on S satisfying the following: if elements x and y are i^{th} associates, $1 \le i \le m$, then they occur together in λ_i blocks. The numbers v, b, r, k, λ_i $(1 \le i \le m)$ are called the parameters of the PBIBD(m).

The *association matrices* $B_i = (\overset{i}{b}_{jk})$, $1 \le i \le m$, $1 \le j, k \le v$, of a PBIBD(m) are defined by

$$\overset{i}{b}_{jk} = \begin{cases} 1 & \text{if } j \text{ and } k \text{ are } i^{th} \text{ associates,} \\ 0 & \text{otherwise.} \end{cases}$$

The *incidence matrix* N of a design (e.g. a BIBD) is a $v \times b$ matrix where v is the number of points of the design and b is the number of blocks of the designs. The rows of the matrix correspond to the points s_i, $1 \le i \le v$ and the columns correspond to the blocks B_i, $1 \le i \le b$. The $(i, j)^{th}$ entry a_{ij} is determined as follows:

$$a_{ij} = \begin{cases} 1 \text{ if } s_i \in B_j \\ 0 \text{ otherwise.} \end{cases}$$

If N is the incidence matrix of a PBIBD(m) then it is well known that

$$NN^T = rI + \sum_{i=1}^{m} \lambda_i B_i,$$

We define group divisible designs as in Hanani(1975). Let S be a v-set and let $G_1, G_2, \ldots G_n$ be a disjoint partition of S where each G_i is of size m. The sets G_i's are called groups. A *group divisible design*, GD[k, λ, m; v], is a collection of k-subsets (called blocks) of the v-set S such that each block intersects each group in at most one element and a pair of elements from different groups occurs in exactly λ blocks. In a similar way we define a GD[K, λ, M; v], where the size of each block is an element of K and the size of each group is an element of M.

These designs have interesting applications in different areas in industry (see e.g. Roberts (1984)). An extra effect can be obtained if we consider the block as an ordered set and/or consider that a block contains a particular number of pairs, which occur in a particular way. For example, we may think of a block, say, {a, b, c, d} as an ordered set which contains only the ordered pairs (a, b), (a, c), (a, d), (b, c), (b, d) and (c, d) instead of the six unordered pairs (a, b), (a, c), (a, d), (b, c), (b, d) and (c, d). Such a design is called a *directed design* These designs have applications in computer networks (Skillicorn (1981)), in experimental design theory and medical experiments where the order of treatments (points) in time is significant (Street (1981)). In a *cyclic design* we think of the block as an ordered set which contains only the ordered pairs (a, b), (b, c), (c, d) and (d, a), whereas in an *equi-neighboured design* we think of the block as an ordered set which contains only the pairs (a, b), (b, c) and (c, d).

Let $W = [w_{ij}]$ be a matrix of order n with $w_{ij} \in \{0, 1, -1\}$. W is called a *weighing matrix* of weight p and order n, if $WW^T = W^TW = pI_n$, where I_n denotes the identity matrix of order n. Such a matrix is denoted by W(n,p). If squaring all its entries gives an incidence matrix of a SBIBD then W is called a *balanced* weighing matrix.

An *orthogonal design*, (OD), say A, of order n and type $(s_1, s_2, ..., s_t)$ on the commuting variables $(\pm x_1, ..., \pm x_t)$ and 0, is a square matrix of order n with entries from $(\pm x_1, ..., \pm x_t)$ and 0. Each row and column of A contains s_k entries equal to x_k in absolute value, the remaining entries in each row and column being equal to 0. Any two distinct rows of A are orthogonal. In other words

$$AA^T = (s_1x_1^2 + ... + s_tx_t^2) I_n .$$

An Hadamard matrix $A = [a_{ij}]$ is a W(n, n), i.e. it is a square matrix of order n with entries $a_{ij} \in \{1, -1\}$, which satisfies

$$AA^T = A^T A = n I_n .$$

Suppose we have a matrix W with elements from an abelian group $G = \{h_1, h_2, ..., h_g\}$ where $W = h_1A_1 + h_2A_2 + ... + h_gA_g$; here $A_1, ..., A_g$ are $v \times b$ (0, 1) matrices, and the Hadamard product $A_i * A_j$ $(i \neq j)$ is zero. Suppose $(a_{i1}, ..., a_{ib})$ and $(b_{j1}, ..., b_{jb})$ are the i^{th} and j^{th} rows of W; then we define WW^+ by

$$(WW^+)_{ij} = (a_{i1}, ..., a_{ib}) \cdot (b_{j1}^{-1}, ..., b_{jb}^{-1})$$

with "." designating the scalar product. Then W is a generalized Bhaskar Rao design or GBRD over G if:

$$\text{(i) } WW^+ = rI + \sum_{i=1}^{m} (c_iG)B_i;$$

$$\text{(ii) } N = A_1 + ... + A_g \text{ satisfies}$$

$$NN^T = rI + \sum_{i=1}^{m} \lambda_iB_i,$$

that is, N is the incidence matrix of a PBIBD(m), and (c_iG) gives the number of times a complete copy of the group G occurs.

Such a matrix is denoted by $GBRD_G(v, b, r, k; \lambda_1, ..., \lambda_m; c_1, ..., c_m)$. When $m = 1$, $c = \lambda/g$ and $B_1 = J - I$, N is the incidence matrix of a BIBD. In this case W is a $GBRD_G(v, b, r, k; \lambda)$ or $GBRD_G(v, k, \lambda)$.

In Chapter 1 some elementary theory of designs using graph theory is introduced. A construction of PBIBDs using complete bipartite graphs is given (joint work with Hammer).

In Chapter 2 it is proved that the necessary conditions are sufficient for the existence of:

(i) directed group divisible designs with block size 3;

(ii) directed group divisible designs with block size 4;

(iii) cyclic group divisible designs with block size 3 except $v = 6$ and group size 1;

(iv) cyclic BIBD$(v, b, r, 4, (4t)^*)$ for $v > 4$

and it is proved that a cyclic BIBD$(v, b, r, 4, (4t+2)^*)$ exists for $v \equiv 0, 1 \pmod 4$.

The "*" on $(4t)$ and $(4t+2)$ indicates that we count the occurrence of the ordered pairs.

In Chapter 3 recursive constructions for equi-neighboured BIBDs of block size 3 are given and it is proved that every group divisible design of block size 3 with $\lambda = 3t$ underlies an equi-neighboured group divisible design, i.e. every group divisible design of block size 3 and $\lambda = 3t$ can be ordered in such a way that it becomes an equi-neighboured group divisible design.

In Chapter 4, a new proof is given that the necessary conditions are sufficient for the existence of *simple*, (without repeated blocks), balanced incomplete block designs with block size 3. Some embedding theorems for simple balanced incomplete block designs with block size 3, based on a method of graph factorization, are given.

In Chapter 5 crypto designs and colourable designs are defined. A *crypto or colourable design* is an incidence matrix of a block design where the non zero entries of the incidence matrix are labeled by a set of symbols called colours. An application of colourable designs to construct group divisible designs is given. The edge colouring of bipartite graphs is used, in the proof of the main existence theorem of colourable designs, which says that every block design is colourable. This theorem does not tell us how to do the colouring and hence the rest of the chapter is devoted to the methods and constructions for colourable designs (joint work with Rodger and Seberry).

Chapter 6 gives constructions for families of BIBDs and PBIBDs. These constructions are based on directed graphs and t-designs.

Chapter 7 (joint work with de Launey, Hammer and Seberry) deals with orthogonal designs. In particular, Chapter 7 deals with the non-existence of GBRD(7, 4, 4, $Z_2 \times Z_2$) (with de Launey), the existence of GBRDs with block size 3 over Z_4 (with de Launey and Seberry) and a construction for weighing designs extended to orthogonal designs (joint work with Hammer and Seberry).

Chapter 8 explores the use of combinatorial designs in encryption. A systematic method to permute the message block, while scrambling in the message, a number of arbitrary message symbols, is given (joint work with Hammer and Seberry).

Preprints and slightly modified reprints of papers, some written by the author and some as a joint author have been used, to form the main body of the present thesis. This has reduced the manual work involved in the thesis but it has some drawbacks, viz. the lack of uniform notation; for example the use of BIBD(v, k, λ), BIBD[k, λ; v] and $S_\lambda(2, k, v)$ to denote a BIBD and repetition of some definitions and known theorems. Please note that reference numbers contained in papers included in this thesis indicate the references at the end of the each individual paper.

CHAPTER 1

INTRODUCTION OF BLOCK DESIGNS BY GRAPHS

A graph (V, E) is a non-empty finite set V of points and a finite set E of edges consisting of pairs of distinct points. Graphs can be used as very effective tools to prove theorems in the theory of block designs and to give existence theorems and constructions for block designs. Such applications will be seen in the present Chapter and in Chapters 3, 4, 5 and 6. Hence, a preprint of a joint paper with J. Hammer is attached here. This paper contains many known results. The construction of partially balanced incomplete block designs found by this author is a modification of that of Alltop (1966) and is new. The paper has been submitted to The Mathematical Gazette.

ON THE INTRODUCTION OF BLOCK DESIGNS BY GRAPHS

Joseph Hammer and Dinesh G. Sarvate

Introduction

The history of combinatorial designs has remarkably humble beginnings. In 1781 Euler encountered the following problem which led to the development of Latin squares:

There are thirty six officers, six officers of six different ranks from each of six regiments. The officers wish to parade in a 6 × 6 square formation such that each row and each column contains one and only one officer of each rank and one and only one officer from each regiment. Can this be done?

Euler conjectured that there does not exist such an arrangement. This conjecture was proved as late as 1901 by Terry (14). Much later in 1850 Kirkman (8) also encountered a "marching" problem (probably influenced by Euler's problem) which led to the development of the block designs:

A school-mistress wishes to take fifteen girls on a daily walk for seven successive days, three girls in each row: to avoid boredom she wants to arrange them so that no two girls shall walk in the same row more than once. Can this be done?

Unlike the Euler's problem, this arrangement does exist. In fact there are 845 essentially different solutions to the problem. Curiously Kirkman published this problem as a puzzle in the obscure magazine, Lady's and Gentleman's Diary among such queries as this: What is the origin of the custom of making fools on the first day of April?

A few years later, in 1853, Steiner (12) proposed a similar problem and these types of designs are called todays *Steiner triple systems*. Interestingly some people (see e.g. Erdos (5)) suspect that Steiner did

know about Kirkman's problem. Moreover in 1844 Woolhouse (17) also proposed a similar problem.

These seemingly light-hearted problems are the origin of a huge and fertile area of combinatorics, generally called *design theory* They arise in many parts of combinatorial mathematics; from group theory to finite geometries, from number theory to coding theory. The problems also have useful important applications in various areas of industry. Apparently the first such application was done in 1926 by Sir Ronald Fisher (6) who applied Latin squares for the very practical purpose of statistical experimentation in agriculture. Subsequently Frank Yates (18) in 1936 introduced balanced incomplete block designs for similar purpose. It turned out that this latter design became probably the most interesting and influential in the development of design theory. It also has a wide range of applications in a surprising number of different areas in industry. For example, psychology (see, e.g. Durbin (4)), virus research (see, e.g. Youden (19)), agriculture (see, e.g., Wellhausen (17)). A formal definition of a balanced incomplete block design is the following:

A *block design* (v, b, r, k) is an arrangement of v *objects* into b *blocks* so that

(i) each object appears in exactly r blocks;

(ii) each block contains exactly k distinct objects.

The block design is *balanced*, if in addition, each pair of distinct objects appears in exactly λ blocks. It is *incomplete* if $k < v$, that is every object does not appear in every block.

One often refers to a balanced incomplete block design (BIBD) as a (v, b, r, k, λ)-design, i.e. a (v, b, r, k, λ)-design is a BIBD with v objects (or varieties), b blocks each of size k with *replication number* r and *index* $\lambda \neq 0$.

As an example, consider a (4, 6, 3, 2,1)-design on objects $\{s_1, s_2, s_3, s_4\}$ and blocks

$$B_1 = \{s_1, s_2\},\ B_2 = \{s_1, s_3\},$$

$$B_3 = \{s_1, s_4\},\ B_4 = \{s_2, s_3\}$$

$$B_5 = \{s_2, s_4\},\ B_6 = \{s_3, s_4\}.$$

This is a BIBD with 6 blocks each of size 2 based on 4 objects with replication number 3 and index 1.

Instead of a list of the blocks a BIBD can also be described by the *incidence matrix*, M of the design. This is a v × b matrix. The rows of the matrix correspond to the objects $s_1, s_2, \ldots, s_v$ and the columns correspond to the blocks $B_1, B_2, \ldots, B_b$. The (i,j) entry a_{ij} is determined as follows:

$$a_{ij} = \begin{cases} 1 & \text{if } s_i \in B_j, \\ 0 & \text{otherwise.} \end{cases}$$

For example the above BIBD has incidence matrix as follows.

	B_1	B_2	B_3	B_4	B_5	B_6
s_1	1	1	1	0	0	0
s_2	1	0	0	1	1	0
s_3	0	1	0	1	0	1
s_4	0	0	1	0	1	1

Several results about block designs can be easily proven in terms of their incidence matrices. The incidence matrix may also be used to represent the block design in a computer.

In this paper block designs are represented by graphs. Graphs are a very useful tool for describing and analysing situations consisting of a set of elements in which various pairs of elements are related by some property. The advantage of using graphs to describe a block design instead of listing the sets element by element is that the structure of the design can be seen more clearly. Perhaps the nearest comparisons are the use of Venn diagrams in set theory or employing vectors in mechanics. Surprisingly the authors have not seen such a useful application of graphs in any standard text of graphs or combinatorics.

Note that only those theorems are proved, which can be established elegantly by graph theoretic methods, otherwise theorems are merely quoted and references ~~of~~ to the proofs are provided.

For convenience, those definitions and results of graph theory, which will be needed, are presented. Further explanations of these terms and the proofs of stated theorems can be found in any standard text, e.g. [7].

Basic results

A *graph* G is a pair (V(G), E(G)) consisting of a finite nonempty set V of elements called *vertices* and a finite set E of *edges* consisting of pairs of distinct points. If e = (u, v) is an edge of C, then e is said to join the vertices u and v, and these vertices are then said to be *adjacent*. We also say that e is *incident* to u and v. In this paper there will be at most one edge connecting any two given vertices.

Let us represent the block design in the example given above by a graph.

Let the four objects and the six blocks be vertices. An object will be adjacent with a block if the object appears in the block. For instance, s_1 and s_2 are adjacent to B_1 ; s_4 is adjacent to B_3, B_5 and B_6.

Thus the block design has the following graph representation:

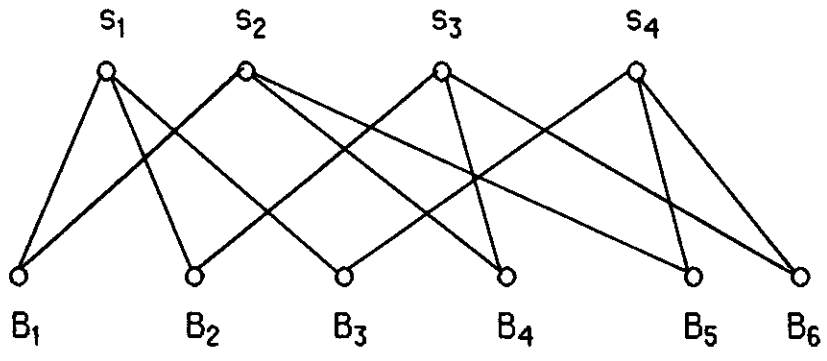


Fig. 1

The *degree* $d(v)$ of a vertex v is the number of vertices to which v is adjacent, formally

$$d(v) = |\{u \in V(G) : (u, v) \in E(G)\}|.$$

The following result is very useful:

In any graph, the sum of the degrees of all vertices is equal to twice the number of edges, formally:

$$\sum_{v \in V} d(v) = 2|E|.$$

Some call this result the handshaking lemma since it implies that if several people shake hands, the total number of hands shaken must be twice the number of people who shake hands.

In the example we can see that $d(s_i) = 3$ and $d(B_j) = 2$ for all $i = 1, \ldots, 4$ and $j = 1, \ldots, 6$, and by the handshaking lemma we have

$$2|E| = \sum d(s_i) + \sum d(B_j) = 24,$$

i.e. $$|E| = 12.$$

A graph is said to be regular if the degree of every vertex is the same.

A *subgraph* of a graph G = (V(G), E(G)) is a graph H = (V(E), E(H)) such that V(B) is a subset of V(G) and E(H) is a subset of E(G).

An important subgraph is a sequence of edges of the form $(v_0, v_1), (v_1, v_2), \ldots, (v_{k-1}, v_k)$ and is called an edge-sequence of graph G from v_0 to v_k. A path is an *edge-sequence* in which the vertices are distinct. The length of a path is the number of edges in the path. For instance, the *length* of the path from s_1 to s_2, in the example is 2.

We say, that the *distance* from s_i to s_j is P if it is the length of a shortest path between s_i and s_j.

A graph in which each pair of vertices is adjacent is called a complete graph. A *complete* graph on n vertices is denoted by K_n. K_n is a *regular* graph of degree n - 1.

A *bipartite* graph $G = G(V_1, V_2)$ is one whose vertex set V can be partitioned into two subsets V_1 and V_2 so that each edge has one end in V_1 and one end in V_2. Consequently no pair of vertices in V_1 is adjacent; likewise for V_2. If each vertex of V_1 is adjacent to each vertex of V_2 then it is called a complete bipartite graph, denoted $K_{m,n}$ where $|V_1| = m$ and $|V_2| = n$.

In the case of bipartite graphs we have an important special property of the handshaking lemma: If $G = G(V_1, V_2)$ is bipartite then no edge of G can be incident to two vertices in V_1 or to two vertices in V_2. In other words every edge in G is incident to exactly one vertex in V_1 and one vertex in V_2. So, we have

$$\sum d(V_1) = \sum d(V_2) = |E|.$$

The graph which represents the BIBD in the example is a bipartite graph of bipartition (V_1, V_2) where $V_1 = \{s_1, s_2, s_3, s_4\}$ and

$V_2 = \{B_1, B_2, B_3, B_4, B_5, B_6\}$. Every vertex of V_1 is of degree 3 and every vertex of V_2 is of degree 2. In fact, any block design can be represented by a bipartite graph. In particular, a BIBD of parameters (v, b, r, k, λ) is a bipartite graph $G(V, B)$ where V corresponds to the objects and B corresponds to the blocks. Vertex $v_i \in V$ is adjacent to a vertex $B_j \in B$ if and only if object v_i appears in block B_j. Each vertex $v_i \in V$ is of degree r and each vertex $B_j \in B$ is of degree k.

A block design is called *symmetric* if $v = b$ and $k = r$. The corresponding graph $G(V, B)$ is a regular graph. It is known that any two distinct blocks of a symmetric BIBD have exactly λ points in common. (For a proof see Street and Wallis (12) p.164.)

We say that a block design is *complete* if each block contains all objects. In this case we have a complete bipartite graph, $K_{v,b}$. If $v = b$ then $K_{v,b}$ represents a latin square based on v elements which is a particular block design.

In an incomplete block design, $r < b$ and $k < v$ and the corresponding graph $G(V, B)$ is a subgraph of $K_{v,b}$.

The block design is balanced if for any pair of vertices of V there are exactly λ vertices of B which are adjacent to both vertices of the pair. (Thus any two vertices of V are joined by exactly λ paths of length 2.) It is called a t-design if there are exactly λ vertices of B which are adjacent to all the members of a given t-subset of V.

The *adjacency matrix* $A(G)$ of a graph G on vertex set $X(G) = \{x_1, x_2, \ldots, x_n\}$ is a symmetric $n \times n$ matrix $A(G) = (a_{ij})$ such that

$$a_{ij} = \begin{cases} 1 & \text{if } x_i \text{ is adjacent to } x_j, \\ 0 & \text{otherwise.} \end{cases}$$

The (i,j)th entry of A^2 is the number of paths of length 2 from x_i to x_j in G (i.e. the number of vertices adjacent to x_i and x_j) and the (i,i)th (i. e. the diagonal) entry is the degree of the vertex x_i in G.

We have the following relationship between the adjacency matrix A(G) of the bipartite graph corresponding to the (v, b, r, k, λ)-design and its incidence matrix M:

$$A(G) = \begin{bmatrix} 0 & M \\ M^T & 0 \end{bmatrix}.$$

The *edge-adjacency matrix* U(G) of a graph G on edge set

$$e(G) = \{e_1, e_2, \ldots, e_m\}$$

is an m x m matrix $U(G) = (e_{ij})$ such that

$$e_{ij} = \begin{cases} 1 \text{ if } e_i \text{ and } e_j \text{ have a vertex in common.} \\ 0 \text{ otherwise.} \end{cases}$$

The *line* graph L(G) of a graph G is the graph with vertex set E(G) in which two vertices are joined if and only if they are adjacent edges in G. The edge-adjacency matrix U(G) of G is the (vertex) adjacency matrix of L(G).

Now we are ready to prove a few basic theorems.

Theorem 1. For a (v, b, r, k)-design vr = bk.

Proof. Let the block design be represented by the bipartite graph G = G(V, B). We count the number of edges of G in two ways. The sum of the degrees of vertices in V, $\Sigma\, d(v_i) = vr$, and the sum of the degrees of vertices in B, $\Sigma\, d(B_j) = bk$. By the counting principle we have $|E| = vr = bk$.

□

Theorem 2. Let the number of blocks in a t-design containing a given t-set be λ. If λ is the number of blocks containing a given i-set, then

$$\lambda_i \binom{k-i}{t-i} = \lambda \binom{v-i}{t-i}, \qquad i = 0, 1, \ldots, t,$$

where $\lambda_t = \lambda$ and λ_0 is the number of blocks in the design.

Proof. Let G(V,B) be the graphical representation of the t-design. Let I be the fixed i-subset of V. We count in two ways the number of $K_{1,t}$ with single point in B and the t-set in V containing I, in other words we are counting the number of stars of size t+1 with center in B and containing the set I in two ways as shown below.

First there are λ_i blocks containing I. The block size is k, hence the number of t-sets in V containing I in each block is $\binom{k-i}{t-i}$. Therefore the number of the required $K_{1,t}$ is $\lambda_i \binom{k-i}{t-i}$ on the other hand, the number of t-sets containing I is $\binom{v-i}{t-i}$ and each t-set occurs in λ_t blocks. Therefore the number of $K_{1,t}$'s is $\lambda \binom{v-i}{t-i}$. Hence the required result.

□

Corrollary. In a (v, b, r, k, λ)-design $\lambda(v-1) = r(k-1)$.

Remark: Notice that a path of length 2 is a $K_{1,2}$ where $\lambda_t = \lambda$ and λ_0 is the number of blocks in the design.

Theorem 3. If M is the incidence matrix of a (v, b, r, k, λ)-design then

$$MM^T = (r - \lambda)I_V + \lambda J_V,$$

where I_V is the v x v identity matrix and J_V is a v x v matrix with every entry 1.

Proof. The adjacency matrix of the bipartite graph G(V, B) corresponding to the (v, b, r, k, λ)-design is

$$A(G) = \left[\begin{array}{c|c} 0 & M \\ \hline M^T & 0 \end{array}\right].$$

Since A is symmetric, $A = A^T$ and we can write

$$AA^T = A^2 = \left[\begin{array}{c|c} 0 & M \\ \hline M^T & 0 \end{array}\right]^2 = \left[\begin{array}{c|c} MM^T & 0 \\ \hline 0 & M^TM \end{array}\right]$$

where MM^T is of size $v \times v$ and M^TM is of size $b \times b$.

Since each vertex $v \in V$ is of degree r and v_i is connected to every other vertex of V by λ distinct paths of length 2, we have that each diagonal entry of MM^T is r and all the other entries are λ. This gives us

$$MM^T = rI_V + \lambda J_V - \lambda I_V = (r - \lambda)I_V + \lambda J_V$$

as required.

□

On the other hand, M^TM has no analogous relationship between its entries unless $b = v$. For the number of paths of length 2 between pairs of vertices of B is not constant. However the diagonal elements are all equal to k.

In the case $b = v$, $MM^T = M^TM$. In this case all vertices are of degree r and the number of vertices adjacent simultaneously to any two vertices in V or in B is λ, i.e. in A^2 all diagonal entries are r and all other entries in MM^T and in M^TM are λ. The line graph of this graph is a strongly regular graph. It is a regular graph with the additional property that any two adjacent (non-adjacent) vertices are joined simultaneously to exactly λ_1 (λ_2) vertices. There are interesting connections between such graphs and certain block designs. Some of these can be found in [2], [3] and [4].

Constructions of block designs

In this section we shall construct new designs from old. To do that we need a few more concepts of graphs.

Two graphs G and H are *isomorphic* if there is a one-one correspondence (bijection) between the vertices of G and those of H, with the property that two vertices are adjacent in G if and only if the corresponding two vertices are adjacent in H.

Let G and H be block designs with parameters (v, b, r, k) and (v', b', r', k') respectively and let G(V, B) and H(V', B') be their respective bipartite graphs where $V = \{v_1, ..., v_v\}$, $V' = \{v_1', ..., v_v'\}$, $B = \{b_1, ..., b_b\}$ and $B' = \{b_1', ..., b_b'\}$. The block designs G and H are *isomorphic* if there exist two bijections Φ and Ψ:

$$\Phi: V \to V'; \quad \Psi: B \to B'$$

with the property that two vertices $v_i \in V$ and $b_j \in B$ are adjacent in G if and only if $\Phi(v_i)$ and $\Psi(b_j)$ are adjacent in H.

Let G be a graph on n vertices. The *complement* $\overline{G}$ of G is a graph which has the same vertex set as G has and in which two vertices are adjacent if and only if they are not adjacent in G. $\overline{G}$ can be constructed by deleting from K_n all the edges of G, i.e. $\overline{G} = K_n - E(G)$. In other words the edge set of $\overline{G}$ is the complement of the edge set of G in the edge set of K_n.

Let G(X,Y) be a bipartite graph such that $|X| = m$ and $|Y| = n$. Then we say that the complement of G in the complete bipartite graph $K_{m,n}$, denoted $\overline{G}(K_{m,n})$, is a bipartite graph with the same bipartition as G such that $\overline{G} = K_{m,n} - E(G)$, i.e. it is found by deleting from $K_{m,n}$ all the edges of G.

If e is an edge of G, then G - e is a graph obtained from G by deleting the edge e. We can say that G - e is the complement of e in G. More

generally if H is any set of edges in G then G - H is the graph obtained by deleting the edges in H or we say that G - H is the complement of H in G,and we denote it H(G). If G is bipartite, H(G) is also bipartite. If u is a vertex of G, then G - u is a subgraph of G obtained from G by deleting the vertex u together with all the edges incident with u. More generally, if X is any set of vertices in G then G - X is the graph obtained by deleting the vertices in X and all the edges incident with them. Again, if G is bipartite then G - X is also bipartite.
Now we are ready for a few basic constructions.

1. *The dual design*

Let G(V, B) be the bipartite graph of a (v, b, r, k, λ)-design. Then by interchanging the two partition sets V and B we obtain a new design G'(B, V) called the *dual* design.

It is obvious that G' is also an incomplete block design with b objects, v blocks, block size r, and replication number k. But it is not necessarily pairwise balanced. It is balanced only if v = b. (see for example Street and Wallis (13) p. 162).

We can see that the two graphs G'(B, V) and G(V, B) are isomorphic but the corresponding designs are not isomorphic. The two graphs are isomorphic if and only if v = b.

2. *The complementary design*

Let G(V, B) represent a (v, b, r, k, λ)-design. The *complementary* design is the complement of G(V, B) in $K_{v,b}$; i.e. edge $e \in \overline{G}$ if and only if $e \in K_{v,b}$ and e does not belong to G(V, B).

Theorem 4. The complementary design of a (v, b, r, k, λ)-design is a BIBD with parameters (v, b, b-r, v-k, b-2r+λ), provided $b-2r+\lambda \geq 0$.

Proof. (i) In $G(V, B)$ any vertex $v_i \in V$ is adjacent to r vertices of B; therefore in $\bar{G}$, v_i is adjacent to $b - r$ vertices of B. Thus the replication number is $b - r$.

(ii) In G any vertex $b_j \in B$ is adjacent to k vertices of V and so, in $\bar{G}$ any b_j is adjacent to $v - k$ vertices of V. Hence the block size is $v - k$.

(iii) $\bar{G}$ is incomplete since $v - k < v$.

(iv) In G each pair of vertices, say v_1 and v_2, in V is adjacent to λ vertices of B. Now v_1 is adjacent to r vertices of B so there are $r - \lambda$ adjacencies between v_1 and vertices of B, which are not adjacent to v_2. Similarly there are $r - \lambda$ adjacencies between v_2 and vertices of B, which are not adjacent to v_1. So the number of vertices in B which are adjacent to neither v_1 nor v_2 is $b - 2(r - \lambda) - \lambda = b - 2r + \lambda$. Hence there are $b - 2r + \lambda$ vertices in B' of $\bar{G}$ which are adjacent to both v_1 and v_2. Hence the index is $b - 2r + \lambda$.

□

3. *Derived design*

Consider a symmetric (v, v, k, k, λ)-design. If $B_1, B_2, \ldots, B_v$ are the blocks, then for any i,

$$B_1 \cap B_i, B_2 \cap B_i, \ldots, B_{i-1} \cap B_i, B_{i+1} \cap B_i, \ldots, B_v \cap B_i$$

form a BIBD called the *derived* design with respect to B_i.

Consider a bipartite graph $G(V, B)$ where $V = \{v_1, \ldots, v_v\}$, $B = \{B_1, \ldots, B_v\}$ and the degree of each vertex is k. The derived design is obtained by deleting a vertex B_i from vertex set B and all vertices in V not adjacent to B_i (and of course all edges incident to all of these vertices.)

Theorem 5. The derived design of a (v, v, k, k, λ)-design is a BIBD with parameters $(k, v-1, k-1, \lambda, \lambda-1)$ provided $\lambda \neq 1$.

Proof. Denote the bipartite graph of the derived design with respect to a block B_i by $G'(V', B')$.

(i) The size of V' is k since only k vertices in V adjacent to B_i remain; all others are deleted.

(ii) The size of B' is $v - 1$ as vertex B_i has been deleted.

(iii) In $G(V, B)$ there are λ vertices of V adjacent to both vertices B_i and, say B_j of B. Recall that any two blocks of a symmetric BIBD have exactly λ points in common. By construction, B_j' is adjacent to the λ vertices of V' which, in $G(V, B)$, are adjacent to the B_i and the B_j. Hence each vertex of B' has degree λ. Thus the block size is λ.

(iv) In G a vertex v_i is adjacent to k vertices of B; in G' one of these vertices, namely B_i, is deleted from G. Hence $v_i' \in V'$ has degree $k-1$, i.e. the replication number is $k-1$.

(v) Finally, any pair of vertices, v_i, v_j in G are adjacent to λ vertices of B. Suppose v_i, v_j are adjacent to B_i in G and so they become, say v_i', v_j' in G'. Then the deletion of B_i reduces the number of vertices of G' adjacent to both v_i', v_j' by one. Hence, v_i' and v_j' are adjacent simultaneously with $\lambda - 1$ vertices of B'; i.e. the index of the derived design is $\lambda - 1$.

(vi) Since $k < v$ in G, $k - 1 < v - 1$ in G', hence G' represents an incomplete block design.

□

4. *Residual design*

Let $B_1, B_2, \ldots, B_v$ be the blocks of a (v, v, k, k, λ) symmetric design. Then for any i, the blocks given by :

$$B_1 - B_i, B_2 - B_i, \ldots, B_{i-1} - B_i, B_{i+1} - B_i, \ldots, B_v - B_i$$

form a BIBD with objects $V - B_i$, called the *residual* design with respect to B_i.

Consider the bipartite graph G(V, B) corresponding to the above symmetric design. Then the bipartite graph of the corresponding residual design with respect to block B_i may be obtained by deleting from G(V,B) vertex B_i and those vertices which are adjacent to B_i.

Theorem 6. The residual design of a (v, v, k, k, λ)-design is a $(v-k, v-1, k, k-\lambda, \lambda)$-design.

We have mentioned that a complete bipartite graph may represent a complete BIBD. An important special case of this complete block design is the latin square in which the elements in each of the blocks are ordered. There are v blocks each containing all the v elements. The i^{th} element occupies the j^{th} position $(1 < j < v)$ exactly once. Thus if the elements in one block are standardised to read in order 1, 2, 3, ..., v then the other blocks are obtained from this by permutations which leave no element fixed. Furthermore if π_1 and π_2 are any two of these permutations then $\pi_1(i) \neq \pi_2(i)$ for any i.

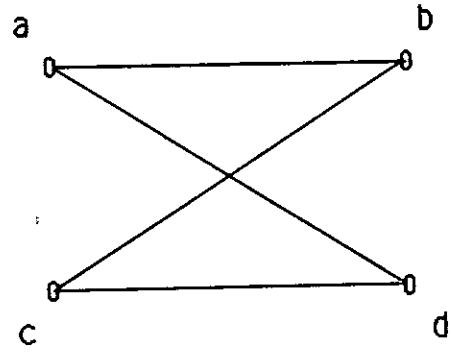
5. *Construction of partially balanced incomplete block designs (PBIBD)*

In this section we will construct *partially balanced incomplete block* designs, PBIBDs, using complete n-partite graphs. In a PBIBD, each block has the same number of elements, and each element is in the same number of blocks; but certain pairs of elements occur with one *frequency* and others occur with another frequency, or there may even be several

prescribed frequencies for certain pairs. Accordingly all $\binom{v}{2}$ unordered pairs of elements are divided into *association classes* such that any pair belongs to exactly one class. For a formal definition of a PBIBD, see Raghavarao [9].

An *n-partite graph* is one whose vertex set can be partitioned into n subsets so that no edge has both ends in any one of the partitions; i.e. in a complete n-partite graph each vertex is joined to every other vertex that is not in the same subset of the partition.

Assume that v is an mn-set of vertices and $V = V_1 \cup V_2 \cup \ldots \cup V_n$ is a partition of V into n disjoint subsets each of m vertices. Let E denote the set of edges of a simple, complete n-partite graph $G(V_1, \ldots, V_n; E)$. Let S_n denote the symmetric group of permutations* of the set V. Let $S = \{\alpha \in S_n : G'\alpha$ is a subgraph of G for each subgraph G' of G$\}$. S also acts naturally on the class of the sets of subsets of V. Let B be a subset of E and $X = \{B\sigma : \sigma \in S\}$. Consider X as a set of blocks and E as the set of vertices; then as we will see (E, X) is a PBIBD with 5 association classes denoted by PBIBD(5). In particular, when G is a complete bipartite graph, (E,X) is a PBIBD(2). Let us construct the PBIBD ($v = 4, b = 2, r = 1, k = 2, \lambda_1 = 1, \lambda_2 = 0$) from the complete bipartite graph as shown.



*In this section we are using a few elementary concepts in group theory, which can be found in any text on the subject.

Here E = {(a, b), (a, d), (c, b), (c, d)} and S consists of those permutations in S_4 which do not map any edge of E into edge (a, c) or (b, d). For example permutation (a b c d) does not belong to S. We start with B = {(a, b), (c, d)} so then X = {{(a, b), (c, d)}, {(a, d), (b, c)}} which is the required PBIBD, where the two association classes are

{(a, b), (c, d)}, {(a, d), (b, c)}.

Since E and X are orbits under the action of S, (E, X) admits S as a group of automorphisms. Let T denote the set of 2-sets of E. The action of S on T decomposes T into five orbits T_1, T_2, T_3, T_4 and T_5, where the members of T_1 are isomorphic to {(a, b), (a, c)} where b and c are vertices of the same class of the partition subset. The members of T_2 are isomorphic to {(a, b), (a, c)} where b and c are from different partition subsets. The members of T_3 consist of pairs of the type {(a, b), (c, d)} where a, c are from one class of the parition and b, d are from another class of the partition. The members of T_4 are {(a, b), (c, d)} where b, c are from the same class of the partition subset and a, d are from different classes of the partition. The members of T_5 are {(a, b), (c, d)} where a, b, c and d are from different classes of the partition. We notice that when n = 2 we have only two orbits T_1 and T_3 and when n = 3 we have four orbits T_1, T_2, T_3 and T_4. Let t_i be a member of T_i and let λ_i denote the number of blocks in X containing t_i. If t is any other member of T_i, then t is also contained in exactly λ_i members of X because S acts as an automorphism group of (E, X) and S is transitive on T_i. In other words (E, X) is a PBIBD (v, b, r, k, λ_i; i = 1, 2, 3, 4, 5), $v = m^2n(n-1)/2$, b = |X| and k = |B|. If all λ_i coincide we get a BIBD. Let $A(B) = \{\alpha \in S \mid B\alpha = B\}$. B is an element of orbit X so that |X| = [S: A(B)]. We can check that $|S| = (m!)^n(n!)$ and hence we have $b = (m!)^n(n!)/g$ where g = |A(B)| and $(m!)^n n!$ divides (mn)! as S is a subgroup of S_{mn}.

Let $u_i = |T_i \cap B|$, $n_i = |T_i|$, $t \in T_i$, $c \in X$, $t \leq c$. If we count the number of ordered pairs (t, c) in two ways we obtain on the one hand $n_i\lambda_i$ and on the other hand bu_i, hence $\lambda_i = bu_i/n_i$.

There are $\binom{n}{2}$ ways to choose a pair V_i, V_j of the partition subsets. For some fixed $a \in V_i$, there are $\binom{m}{2}$ pairs of edges $\{(a, b), (a, c)\}$ where $b, c \in V_j$. Now as a varies we get $m\binom{m}{2}$ such pairs of edges. Similarly there are $m\binom{m}{2}$ pairs $\{(b, a), (c, a)\}$ for $a \in V_j$ and $b, c \in V_i$. As the number of pairs $\{V_i, V_j\}$ is $\binom{n}{2}$, we have $n_1 = 2m\binom{m}{2}\binom{n}{2} = m^2(m-1)n(n-1)/2$. By similar counting arguments we obtain

$$n_2 = n(n-1)(n-2)m^3/3,$$

$$n_3 = n(n-1)m^2(m-1)^2/4,$$

$$n_4 = n(n-1)(n-2)m^3(m-1)/2$$

and $$n_5 = n(n-1)(n-2)(n-3)m^4/8.$$

If all the λ_i coincide we get the following relations:

$$u_1 = (m-1)u_2/m(n-2)$$

$$= 2u_3/(m-1)$$

$$= u_4/m(n-2)$$

$$= 4(m-1)u_5/(n-2)(n-3)m^2.$$

Example

When n = 2, we have only two orbits T_1 and T_3 and $n_1 = m^2(m-1)$ and $n_3 = m^2(m-1)^2/2$. Let B be a cycle of length 2L, then $u_1 = 2L$ and $u_3 = L(2L-3)$. The λ's coincide if

$$m^2(m-1)/2L = m^2(m-1)^2/2L(2L-3)$$

i.e.

$$2L - 3 = m - 1$$

or

$$2L = m + 2.$$

Table 2 gives the parameters of the first four values of L. Counting the number of distinct cycles of length 2L gives

$$b = m^2(m-1)^2 \ldots (m-L+1)^2 / 2L.$$

Table 2.

L	v	b	r	k	λ
2	4	1	1	4	1
3	16	96	36	6	12
4	36	16200	1800	8	360
5	64	125440	19600	10	2800

Applications of colouring

A graph G is said to be k-*colourable* if, to each of its vertices, we can assign one of the k colours in such a way that no two adjacent vertices have the same colour. In such a case we also say that G has a *proper* k-colouring. It is well known that G is 2-colourable if and only if it is bipartite. The *chromatic number*, $\chi(G)$, of G is the minimum k for which G is k-colourable.

G is said to be *k-edge-colourable* if its edges can be coloured with k colours in such a way that no two adjacent edges have the same colour. In such a case we also say that G has a proper k-edge-colouring. The *edge-chromatic number* or the *chromatic index*, $\chi'(G)$, of G is the minimum k for which G is k-edge colourable. A classical theorem of Konig says that if G

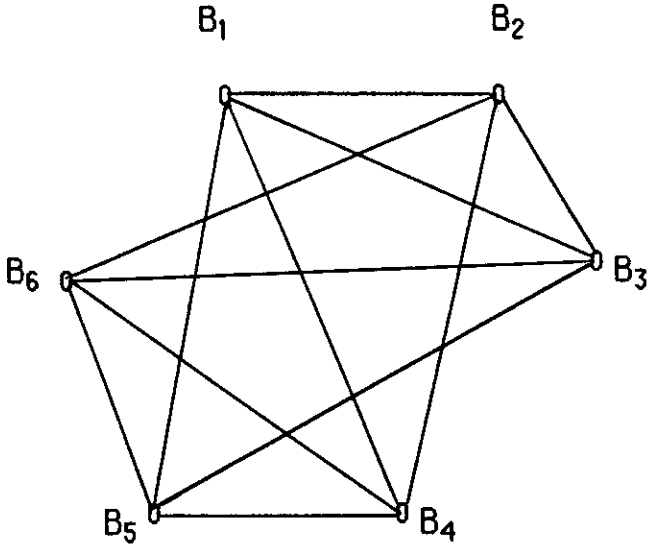
is bipartite, then $\chi'(G) = p$ where p is the maximum vertex-degree of G (see for example Wilson[16]).

First we apply vertex colouring for constructing resolvable designs. A BIBD whose blocks can be partitioned into sets in such a way that every set contains every object exactly once is called *resolvable design*. The set of blocks is called a *resolution class*. The set of resolution classes is a resolution. A design may be resolvable in several ways, each manner of resolving is a resolution. Kirkman's schoolgirls problem is to find a (15, 35, 7, 3, 1) resolvable design: the 35 blocks with block size 3 can be partitioned into 7 resolution classes such that each resolution class contains every object exactly once. All affine planes are resolvable designs: the set of all blocks in one parallel class forms a resolution, for every point belongs to one and only one line in a parallel class. In addition any two lines which are not in the same parallel class have exactly one common point. We can see that Kirkman's design is not affine resolvable. Our example, in the Introduction, is also a resolvable design. A resolution is the following.

$$(B_1, B_6), (B_3, B_4), (B_2, B_5).$$

Now we show how to find such a set of resolutions by applying vertex colouring. We construct a graph G', called a block graph, whose vertices are the b blocks of the design. Two vertices are joined by an edge if the two blocks have an object in common. If the chromatic number of G' is $\chi(G') = r$, then the r colours used define the r resolutions.

The block graph of our example is shown below.



This is a regular graph of degree 4. The vertices B_1 and B_6 are not adjacent, neither are B_3 and B_4, or B_2 and B_5. Hence the non-adjacent pairs of vertices can be coloured with three colours.

If the block graph of a BIBD(v, b, r, k, l) is r-chromatic then it is resolvable with r resolution classes, and each containing v/k blocks.

Now we present some more applications with edge colourings.

We have mentioned that an n x n latin square can be regarded as a labelled complete bipartite graph $K_{n,n}$. By Konig's edge colouring theorem the chromatic index of $K_{n,n}$ is n. The matrix interpretation of the coloured graph is that the colour of the edge u_i, v_j is the (i, j) entry of the latin square. Similarly, consider the bipartite graph G(V, B) which corresponds to the BIBD(v, b, r, k, λ). G has chromatic index r. A matrix representation, of this coloured graph, shall be such that the colour of the edge (s_i, B_j) is the (i, j)th entry of a v x b matrix , and all other entries are

0. In fact we replace the entries 1 by the corresponding colour in the incidence matrix M of the BIBD. The coloured (incidence) matrix corresponding to our BIBD(4, 6, 3, 2, 1) is

$$M_C = \begin{bmatrix} x & y & z & 0 & 0 & 0 \\ y & 0 & 0 & z & x & 0 \\ 0 & z & 0 & x & 0 & y \\ 0 & 0 & x & 0 & y & z \end{bmatrix}$$

In general the coloured matrix, M_C of a (v, b, r, k, λ) design is a modified (v x b) Latin rectangle. Each row has r different labels (colours) and the other v-r entries are all 0. Each column has k different labels out of the r labels and all other entries are 0.

It turns out that coloured matrices are very useful in producing new block designs. Due to lack of space we cannot go into particulars in this paper. We refer the reader to the papers of Hammer, Sarvate and Seberry [7], Rodger, Sarvate and Seberry [10] and Sarvate and Seberry [11].

There are several other graph representations of block designs for constructing new block designs. For instance, Alltop [1] has constructed block designs by representing the v objects by the edges of a complete graph K_v and the blocks by the sets of edges of subgraphs. Generalizing Alltop's method, we construct block designs by means of a complete directed graph K_v^*. Another graphical representation of a block design is where the v objects are the vertices of K_v and the blocks consist of the set

of complete subgraphs K_k such that each edge of K_v occurs exactly λ times. We will not present applications of these graph representations in this introductory paper.

Acknowledgement:

The authors are thankful to Dr. D. R. Breach, Dr. Elizabeth Billington and Professor Anne Penfold Street.

References

1. ALLTOP, W. O., On the construction of block designs, 1966, J. Combinatorial Theory 1, 501-502.

2. CAMERON, P. J., Strongly regular graphs, 1978, Selected Topics in Graph Theory, edited by BEINEKE, L. W. and WILSON, R. J.,Academic Press 337-360.

3. CAMERON, P.J. and VAN LINT, J.H., Graphs, Codes and Designs, 1980, Londan Math. Soc. Lecture Note Series, 43, Cambridge University Press.

4. DURBIN, J., Incomplete blocks in ranking experiments, 1951, Brit. J. Psychology, 4, 85-90.

5. ERDOS, P., Problems and Results on block designs and set systems, 1982 Congressus Numerantium, 35, 3-16.

6. FISHER, R. A., The arrangement of Field Experiments, 1926, J. Minist. Agric., 33, 503-513.

7. HAMMER, J., SARVATE, D, G. and SEBERRY, J., A note on orthogonal designs, 1987, Ars Combinatoria, submitted.

8. KIRKMAN, T.P., Query, 1850, Lady's and Gentleman's Diary, 48.

9. RAGHAVRAO, D., Construction and Combinatorial Problems in Design of Experiments, 1971, Wiley, New York.

10. RODGER, C.A. SARVATE, D. G. and SEBERRY, J., Colourable designs, new group divisible designs and pairwise balanced designs, 1987, J. Statistical Plann. and Inf.

11. SARVATE, D. G. and SEBERRY, J., Encryption methods based on combinatorial designs, 1986,Ars Combinatoria, 19 A, 237-246.

12. STEINER, J., Combinatorische Aufgabe, J. Reine Angew. Math., 1853, 45,181-182.

13. STREET A. P. AND WALLIS, W. D., Combinatorial Theory: An Introduction, 1984, Winnipeg, Canada.

14. TERRY, G., Le Probleme de 36 officieurs, C. R. Assoc. Fr. Avance. Sci. Nat., 1, 1900, 122-123; 2, 1901, 170-203.

15. WELLHAUSEN, E. J., The accuracy of incomplete block designs on varietal trials in West Virginia, 1943, J. Amer. Soc. of Agronomics, 35, 66-76.

16. WILSON, R. J., Introduction to Graph Theory, Third edition, 1985, Longman.

17. WOOLHOUSE, W.S.B., Prize question 1733, 1844, Lady's and Gentleman's Diary.

18. YATES, F., Incomplete randomized blocks, 1936, Ann. Eugen., 7, 121-140.

19. YOUDEN, W. J., Use of incomplete block replications in estimating Tobacco-Mosaic virus,1937, Contr. Boyce Thompson Inst., 9, 41-48.

CHAPTER 2

DIRECTED AND CYCLIC DESIGNS

A directed balanced incomplete block design, denoted by DBIBD(v, b, r, k, λ^*), is a BIBD(v, k, 2λ) in which every block is arranged so that each ordered pair occurs λ times. The "*" on λ indicates that the occurrences of ordered pairs are counted. A block $< a_1, a_2, \ldots, a_k >$ is said to have k(k-1)/2 ordered pairs viz. (a_i, a_j) i = 1, 2, ... , k-1, j = i+1, ... , k.

A directed group divisible design, DGD[k, λ^*, m; v], is a group divisible design, GD[k, 2λ, m; v], in which each ordered pair of elements from different groups occurs in exactly λ^* blocks where each block is said to have k(k-1)/2 ordered pairs as in a DBIBD. Similarly we can define a directed partially balanced incomplete block design.

A cyclic BIBD, denoted by CBIBD[v, k, λ^*] is a BIBD(v, k, $(k-1)\lambda$) in which every block is arranged so that each ordered pair occurs λ times. A block $[a_1, a_2, \ldots, a_k]$ is said to have only k ordered pairs, viz. (a_i, a_{i+1}), i = 1, 2, ..., k-1 and (a_k, a_1).

A cyclic group divisible design, CGD[k, λ^*, m; v], is a group divisible design, GD[k, $(k-1)\lambda^*$, m; v], in which each ordered pair of elements from different groups occurs in exactly λ^* blocks. As in a CBIBD each block is said to have only k ordered pairs.

The word "cyclic" may cause some confusion. We do not mean a design developed cyclically from a starter block. As Dr. Breach has suggested "circular" might have been a better word but cyclic is well entrenched in the literature. Cyclic BIBDs with block size 3 and λ =1 are also called Mendelsohn triple systems (see e.g. Rodger(1986)). A paper by Bermond, Haung and Sotteau (1978) uses the term "balanced circuit designs" for what is termed a cyclic BIBD. They have also proved Theorem 2.1.3 but not any other result mentioned below.

Directed designs have applications in the development of computer networks and data flow machine architecture (Skillicorn (1981)) and in experiments, where the order of the treatments in time is significant (Street (1981)).

The definition of a group divisible design can also be given as follows:

A group divisible design (GD[k,λ,m;v]) is a PBIBD(2) with parameters $v = mn$, b, r, k, $\lambda_1 = 0$ and $\lambda_2 = \lambda$ for which the points (set X) may be divided into m groups of n distinct points such that the points that belong to the same group are first associates and two points that belong to different groups are second associates.

Consider a PBIBD(2), say P, with parameters $v = mn$, b, r, k, λ_1 and λ_2 for which the points (set X) may be divided into m groups of n distinct points such that the points that belong to the same group are first associates and two points that belong to different groups are second associates. If $\lambda_1 = r$, then P is called a singular GDD. On the other hand if $r-\lambda_1 > 0$ and $rk - v\lambda_2 > 0$, then P is called a regular GDD.

2.1 Some results on directed and cyclic designs

The main results proved in the attached published papers

(a) "All directed GDDs with block size 3, $\lambda_1 = 0$, exist", Utilitas Mathematica, 26, 1984, 311-317

and (b) "Some results on directed and cyclic designs", Ars Combinatoria, 19A, 1985, 179-190

are the following:

Theorem 2.1.1: *The necessary conditions are sufficient for the existence of directed group divisible designs with block size 3 and block size 4 .*

Proof. Theorem 13 of (a) and Theorem 3.4 of (b).

□

Theorem 2.1.2: *The necessary conditions are sufficient for the existence of cyclic group divisible designs with block size 3 .*

Proof. Theorem 4.10 of (b).

□

Theorem 2.1.3: *A* CBIBD(v, 4, (4t+2)*) *exists for* $v \equiv 0, 1 \pmod 4$ *and a* CBIBD(v, 4, (4t)*) *exists for all* $v \geq 4$.

Proof. Theorem 2.9 of (b).

□

Theorem 2.1.4: (i) *If a directed partially balanced incomplete block design* DPBIBD(v, b, r, k=3, $\lambda_1^* = 0$, λ_2^*, n_1, n_2) *exists, then* DPBIBD(Nv, N^3b, N^2r, k=3, $\lambda_1^* = 0$, $N\lambda_2^*$, Nn_1, Nn_2) *exists* .

(ii) *If directed group divisible designs* DGD(k, λ^*, m; v) *and* DGD(k, λ^*, v; kv) *exist, then* DGD(k, λ^*, m; kv) *exists* .

Proof. Lemmas 14 and 15 of (a).

□

Note that, according to the definition of GDD in Hanani (1975), we do not have to mention $\lambda_1 = 0$ in (a). For notation used in the attached papers please refer Hanani (1965), e. g. GD(K, λ, M) is defined (on page 264) as the set of integers v for which a GD[K, λ, M; v] exists.

In these papers, we pursue similar lines to those of Street and Seberry (1980) and Street and Wilson (1980). Designs are specified by giving one or more initial blocks and instructions on how they should be developed. Thus 'mod p' means "to each element of the initial block, add in

turn each of the non-zero elements of GF(p), using addition in GF(p); 'mod (p, q)' means "to each ordered pair in the initial block, add in turn each non-zero element of GF(p) × GF(q)"; 'mod (p, -)' means "to each ordered pair in the initial block, add in turn each non-zero element of GF(p) × {0}".

All directed GDDs with block size three, $\lambda_1 = 0$, exist

Dinesh. G. Sarvate

1. Introduction.

A *directed design* (see D. B. Skillicorn, [8]) is a collection of subsets of cardinality k from {1, 2, . . . , v} with the property that each ordered t-subset appears in a k-subset (of block) exactly λ times. Such a directed design is described by a sextuple of the form t-(v, b, r, k, λ^*) where b is the number of blocks required and r is the number of times that any element occurs. The star on λ indicates that it counts the occurrences of ordered t-sets. These designs can be used in the development of computer networks and data flow machine architecture [7]. They also have application to agricultural or medical experiments where the order of treatment in time might be significant.

These designs were studied by a number of authors including J. E. Dawson, J. R. Seberry and D. B. Skillicorn [1], J. R. Seberry and D. B. Skillicorn [6], D. Street and J. Seberry [10], D. Street and W. Wilson [11], D. B. Skillicorn and R. G. Stanton [9], S. H. Y. Hung and N. S. Mendelsohn [5], C. J. Colbourn and M. J. Colbourn [2] and M. J. Colbourn and C. J. Colbourn [3].

We define a group divisible design as in [11] and [4]. Let X be a v-set such that $X = \cup G_i$, $G_i \cap G_j = \phi$, $i \neq j$, $|G| = m$ for all i. The G_i's are called groups. *A group divisible design*, GD(k, λ, m; v), is a collection of k-subsets of the v-set X

(called *blocks*) such that each block intersects each group in at most one element and a pair of elements of X from different groups occurs in exactly λ blocks. In a similar way we can define a GD[K,λ,M;v], where the size of each block is an element of K and the size of each group is an element of M. GD(K,λ,M) denotes the set of all v such that a GD[K,λ,M;v] exists.

A directed design with $t = 2$ is a directed balanced incomplete block design (DBIBD). As in Hanani [4], B(k,λ) is the set of all v such that a BIBD(v,b,r,k,λ) exists, DB(k,λ*) is the set of all v such that a directed BIBD(v,b,r,k,λ*) exists. A directed group divisible design, DGD[K,λ*,M;v] is a GD[K,2λ ,M;v] in which each ordered pair of elements from different groups occurs in exactly λ^* blocks. DGD(K,λ*,M) denotes the set of all v such that a DGD[K,λ*,M;v] exists. Given a block (a,b,c) we say the three ordered pairs (a,b), (a,c) and (b,c) occur in it.

In Section 2 we prove that the necessary conditions for the existence of GD designs are sufficient for the existence of DGD with $k = 3$. In Section 3 we give some general results.

2. *DGD with* $k = 3$.

The existence of a GD[k,λ,m;v] implies the existence of DGD[k,λ*,m;v]. The DGD is obtained by writing each block of GD twice - once in the given order and once in the reverse order - and hence, using Hanani [4], we have the following results:

LEMMA 1. *If* $v \in GD(3,\lambda,m)$ *holds and if* r *is a positive integer, then* $rv \in DGD(3,\lambda^*,rm)$ *holds.*

LEMMA 2. *If* $n \equiv 0$ *or* $1 \pmod 3$, *then* $2n \in DGD(3,1^*,2)$ *holds.*

We notice that for $n \equiv 2 \pmod 3$, the necessary conditions are not satisifed.

LEMMA 3. *If* $n \equiv 1 \pmod 2$, *then* $3n \in DGD(3,1^*,3)$ *holds.*

LEMMA 4. *For every* $n \geq 3$, $6n \in DGD(3,1^*,6)$ *holds.*

LEMMA 5. *For every* $n \geq 3$, $3n \in DGD(3,2^*,3)$ *holds.*

LEMMA 6. *For every* $n \geq 3$, $2n \in DGD(3,3^*,2)$ *holds.*

In [10] the following result is proved:

LEMMA 7. *If* $n \in DB(K,\lambda^*)$ *and* $mK \subset GD(k,\lambda,m)$, *then* $mn \in DGD(k,\lambda\lambda^*,m)$.

We also have

LEMMA 8. (Lemma 2.20 [4]). *If* λ' *divides* λ, *then* $DGD(K,\lambda'^*,M)$ *is a subset of* $DGD(K,\lambda^*,M)$.

LEMMA 9. *If* $v \in DGD(3,1^*,x)$ *and* $x \in DGD(3,1^*,3)$, *then* $v \in DGD(3,1^*,3)$.

Proof. $v \in DGD(3,1^*,x)$, so every ordered pair (a,b), where a and b belong to different groups, occurs once. Writing together the blocks of $DGD(3,1^*,3;|G_i|)$ where G_i is a group and treatments are the elements of G_i, for $i = 1,2,\ldots,\frac{v}{x}$, we get the required result.

We now give two examples for further reference, the blocks are written as columns.

Example 1. $4 \in DB(3,1^*)$

1	2	3	4
2	4	1	3
3	1	4	2

Example 2. $6 \in DB(3,1^*)$

0	2	3	2	4	5	0	1	4	5
4	1	1	3	3	1	2	3	5	0
1	0	2	4	0	4	5	5	2	3

Using Examples 1 and 2 with Lemmas 7 and 3 we get

LEMMA 10. $\{12,18\} \subseteq DGD(3,1^*,3)$.

Now we prove (Lemma 2.16, Hanani [4]):

LEMMA 11. *Let* $n \in B(K,\lambda)$ *and* $mK \subset DGD(k,\lambda^*,m)$, *then* $mn \in DGD(k,\lambda\lambda^*,m)$.

Proof. Consider the groups of the required DGD(k,λ*,m) as points of B[K,λ,n] and form a DGD(k,λ*,m) on every block of B[K,λ,n].

LEMMA 12. *For every* $n \geq 3$, $3n \in DGD(3,1^*,3)$ *holds.*

Proof. We know that, for every integer $n \geq 3$, $n \in B(K_3,1)$ where $K_3 = \{3,4,5,6,8\}$ (see [4]). By Lemma 11 it suffices to show that $3n \in DGD(3,1^*,3)$ for every $n \in K$. For $n = 3,5$ this follows from Lemma 3, whereas for $n = 4,6$ this follows from Lemma 10. For $n = 8$, we give DGD(3,1*,3;24) (with the notations of [4]).

Let the set of vertices be $X = Z(3,2)X\left(Z(7,3) \cup \infty\right)$.

Blocks: $< (\phi,\phi), (0,\alpha'), (0,-\alpha') >$ mod(3,7), $\alpha' = 1,2,3$

$< (0,\alpha+4), (0,\alpha+1), (\phi,\phi) >$ mod(3,7), $\alpha = 0,1$

$< (\phi,3), (\phi,\infty), (\phi,0) >$ mod(3,7),

$< (\phi,\infty), (1,0), (0,\phi) >$ mod(3,7),

$< (1,3), (0,\phi), (\phi,\infty) >$ mod(3,7).

THEOREM 13. *Let* m, λ, *and* v *be positive integers. Necessary and sufficient conditions for the existence of a directed group divisible design* $DGD[3,\lambda^*,m;v]$ *are*

$$v \equiv 0 \pmod{m}, \quad v \geq 3m,$$

and

$$\lambda v(v-m) \equiv 0 \pmod{3}.$$

Proof. The necessity follows from Theorem 6.2 [4] and the fact that a directed GD(3,λ*,m) is a GD(3,2λ,m). In order to prove sufficiency, as in [4], we consider only those values of λ and of m which are factors of 6. In all these cases the existence of the relevant directed group divisible designs is proved in the Lemmas listed in Table 1. We notice that for m = 1, a directed GD is a directed BIBD whose existence has been proved in [6].

TABLE 1

m	λ*	Proof
2	1	Lemma 2
2	2	Lemmas 2 and 8[†]
2	3	Lemma 6
2	6	Lemmas 6 and 8
3	1	Lemma 12
3	2	Lemmas 12 and 8
3	3	Lemmas 12 and 8
3	6	Lemmas 12 and 8
6	1	Lemma 4 and using Lemma 8 for $\lambda^* = 2,3,6$.

[†]We observe that for $\lambda^* = 2^*$, $m = 2$, necessary conditions are satisfied only for $n \equiv 0$ or $1 \pmod 3$. It is, in fact, sufficient to prove for those values of λ and m which are factors of 3.

3. General Results.

We can define directed partially balanced incomplete block design in a similar way.

LEMMA 14. *If a directed partially balanced incomplete block design* $DPBIBD(v,b,r,k=3,\lambda_1^*=0,\lambda_2^*,n_1,n_2)$ *exists, then* $DPBIBD(Nv,N^2b,N^2r,k=3,\lambda_1^*=0,N\lambda_2^*,Nn_1,Nn_2)$ *exists.*

Proof. Replace the treatments $u_1,\ldots,u_v$ by $u_1^1,\ldots,u_1^N,\ldots,u_v^1,\ldots,u_v^N$ and blocks $\left(u_\ell,u_m,u_n\right)$ by $\left(u_\ell^i,u_m^j,u_n^k\right)$, $i,j,k = 1,2,\ldots,N$. It is easy to check that we get the required DPBIBD.

LEMMA 15. *Let DBIBD (v,b,r,k,λ^*) exist and r be even. Then the corresponding singular group divisible design obtained by replacing each treatment by a group of m treatments is directed.*

Proof. The corresponding SGD is directed up to the second associates and the first associates are also directed once we write $u_1,u_2,\ldots,u_m$ first associates in one order $r/2$ times and in reverse order for another $r/2$ times in the blocks in which they occur.

LEMMA 16. *If $DGD(k,\lambda^*,m;v) = X$ and $DGD(k,\lambda^*,v;kv) = Y$ exist, then $DGD(k,\lambda^*,m;kv)$ exist.*

Proof. Let the kv vertices be $u_1^1,\ldots,u_v^1,u_1^2,\ldots,u_v^2,\ldots,u_1^k,\ldots,u_v^k$. Let X^i denote the DGD with $u_1^i,\ldots,u_v^i$ vertices, $i = 1,2,\ldots,k$. Then

$$X^1:X^2:\ldots:X^k:Y$$

gives the required DGD.

Acknowledgement. I would like to express my thanks to Dr. Jennifer R. Seberry for suggesting the problem and for her valuable guidance.

REFERENCES

[1] J. E. Dawson, J. R. Seberry and D. B. Skillicorn, *The directed packing numbers* $DD(t,v,v)$, $t \geq 4$. Combinatorica (to appear).

[2] C. J. Colbourn and M. J. Colbourn, *Every twofold triple system can be directed,* J. Combinatorial Theory, Ser. A. *34* (1983), 375-378.

[3] M. J. Colbourn and C. J. Coloburn, *Recursive constructions for cyclic block designs.* To appear.

[4] H. Hanani, *Balanced incomplete block designs and related designs,* Discrete Math., *11* (1975), 255-369.

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

[6] J. R. Seberry and D. B. Skillicorn, *All directed BIBDs with* $k = 3$ *exist,* J. Combinatorial Theory, Ser. A, *29, No. 2* (1980), 244-248.

[7] D. B. Skillicorn, Directed Packings and Coverings with Computer Applications, Ph.D. Thesis, University of Manitoba, (1981).

[8] D. B. Skillicorn, *Complete directed designs,* Congressus Numerantium, *38* (1983), 247-252.

[9] D. B. Skillicorn and R. G. Stanton, *The directed packing numbers* $DD(t,v,v)$, Proceedings of Eleventh Manitoba Conference on Numerical Math. and Computing, Winnipeg, Manitoba, 1981, Congressus Numerantium, *34* (1982), 425-428.

[10] D. Street and J. Seberry, *All DBIBDs with block size four exist,* Utilitas Mathematica, *18* (1980), 27-34.

[11] D. Street and W. Wilson, *On directed balanced incomplete block designs with block size five,* Utilitas Mathematica, *18* (1980), 161-174.

Department of Applied Mathematics
University of Sydney
N.S.W. 2006 AUSTRALIA

Received November 2, 1983; Revised March 21, 1984.

Some results on directed and cyclic designs

Dinesh G. Sarvate

1. Introduction.

Directed and cyclic designs are studied by a number of authors including Dawson, Seberry, Skillicorn [1], Colbourn and Colbourn [3,4], Colbourn and Harms [5], Hung and Mendelsohn [10], Sarvate [12] Seberry and Skillicorn [13], Skillicorn [15], Skillicorn and Stanton [16], Street abd Wilson [18], and Rodger [11].

A directed balanced incomplete block design, denoted by DBIBD(v, b, r, k, λ^*) is a BIBD(v, k, 2λ) in which every block is arranged so that each ordered pair occurs λ times. A block $<a_1, a_2, \ldots, a_k>$ is said to have k(k-1)/2 orderd pairs, viz. (a_i, a_j) i = 1, 2, ..., k-1, j = i+1, ..., k, e. g., the blocks of DBIBD[4, 3, 1^*] are

$<1, 2, 3>, <2, 1, 4>, <4, 3, 1>, <3, 4, 2>$.

We define a group divisible design as in Hanani [7]: Let X be a v-set such that $X = \cup G_i$, where the union is over i = 1, 2, ..., n; $G_i \cap G_j = \phi$, $i \neq j$; and $|G_i| = m$ for all i. The G_i's are called the groups. A group divisible design, GD[k, λ, m; v] is a collection of k-subsets (called the blocks) of the v-set X such that each block intersects each group in at most one element and a pair of elements from different groups occurs in exactly λ blocks. In a similar way we can define a GD[k, λ, m; v], where the size of each block is an element of K and the size of each group is an element of M.

A directed group divisible design, DGD[k,λ*,m;v], is a group divisible design, GD[k,2λ,m;v], in which each ordered pair of elements from different groups occurs in exactly λ* blocks where each block is said to have k(k-1)/2 ordered pairs as in a DBIBD.

A cyclic BIBD, denoted by CBIBD[v,k,λ*] is a BIBD(v,k,(k-1)λ) in which every block is arranged so that each ordered pair occurs λ times. A block $[a_1,a_2,\ldots,a_k]$ is said to have only k ordered pairs viz. (a_i,a_{i+1}) $i = 1,2,\ldots,k-1$ and (a_{k-1},a_1), e.g. the blocks of CBIBD[5,4,1*] are

[1,2,3,4], [1,3,5,2], [1,4,2,5], [1,5,4,3] and [2,4,5,3].

We use the notation [a,...,z] to denote a cyclic block of a CBIBD.

A cyclic group divisible design CGD[k,λ*,m;v] is a GD[k,(k-1)λ*,m;v] in which each ordered pair of elements from different groups occurs in exactly λ* blocks. As in CBIBD each block is said to have only k ordered pairs. We use the notation CGD[k,λ*,m] to denote CGD[k,λ*,m;v] wher. there is no doubt about the value of v. The set of v for which a CGD[k,λ*,m] exist is denoted by CGD(k,λ*,m). For any other definition and notation the reader is referred to Hanani [7] and Street & Seberry [17].

Directed designs can be used in the development of computer networks and data flow machine architecture [14] and cyclic designs can be used in virus research and animal husbandry experiments like neighbour designs [8]. Neighbour designs are not the same as cyclic designs. In cyclic designs we consider ordered pairs and the same treatment cannot occur more than once in the same block, whereas in neighbour designs ordered pairs are not considered and the same treatment can occur in the same block more than once. We use the notation <a,...,z> to denote a block of a directed design.

2. CYCLIC BIBD WITH k = 4.

One can easily prove

Theorem 2.1. *Suppose there exists a* CBIBD[k,j,λ*] *and a* BIBD(v,k,λ'), *then there exists a* CBIBD[v,j,(λλ')*].

Proof. We replace each block of the BIBD(v,k,λ') by the corresponding CBIBD[k,j,λ*] to get the required CBIBD[v,j,(λλ')*].

e.g. CBIBD(4,3,1*) is given by the blocks [1,2,3], [1,3,4],

[1,4,2], [2,4,3] and BIBD(5,4,3) is given by the blocks {1,2,3,4}, {1,2,3,5}, {1,2,4,5}, {1,3,4,5}, {2,3,4,5}. We replace each of these blocks by the corresponding CBIBD(4,3,1*) and get CBIBD[5,4,3*] as follows:

[1,2,3], [1,2,3], [1,2,4], [1,3,4], [2,3,4];
[1,3,4], [1,3,5], [1,4,5], [1,4,5], [2,4,5];
[1,4,2], [1,5,2], [1,5,2], [1,5,3], [2,5,3];
[2,4,3], [2,5,3], [2,5,4], [3,5,4], [3,5,4].

Corollary 2.2. *Suppose there exists a* PBD[K,λ,v] *where* $K = \{k_1,k_2,\cdots,k_n\}$ *and a* CBIBD[k,j,μ*] *for each* $k \in K$, *then there exists a* CBIBD[v,j,(λμ)*].

Corollary 2.3. CBIBD[11,4,2*] *and* CBIBD[15,4,4*] *exist.*

Proof. We use BIBD(11,5,2) and BIBD(15,5,4) together with the CBIBD[5,4,1*] given in the introduction.

Using theorem 2.1 and de Launey and Seberry [6] we have

Theorem 2.4. (i) *If* $u \equiv 0$ *or* 1(mod 4), $u \geq 4$ *and there exists a* CBIBD[k,j,λ*] *for* $k \in K_4^1 = \{4,5,8,9,12\}$, *then there exists a* CBIBD[u,j,λ*]. (ii) *If* $u \equiv 1$(mod 3) *and there exists a* CBIBD[k,j,λ*] *for all* $k \in H_3^3 = \{4,7,10,19\}$, *then there exists a* CBIBD[u,j,λ*]. (iii) *If* $u \geq 4$ *and if there exists a* CBIBD[k,j,λ*] *for all* $k \in K_4^2 = \{4,\cdots,12,14,15,18,19,22,23\}$, *then there is a* CBIBD[u,j,λ*].

Professor C. Colbourn pointed out that the following theorem can be proved immediately using the decomposition of complete directed graphs into cycles. See [19].

Theorem 2.5. BIBD(v,k,λ) => CBIBD(v,k,λ*) *except for* k=4 *and* 6.

Remark (1). For the case k=p, a prime, we can get CBIBD(v,p,λ*) from (p-1) copies of BIBD(v,p,λ) as shown below:

Let a particular block of BIBD(v,p,λ) be {1,2,...,p}. We arrange its (p-1) copies, say $B_1,\ldots,B_{p-1}$ as follows:

The first treatment of each B_i is 1 and the next treatment is obtained by adding i in the previous treatment for $i = 1,\ldots,\frac{(p-1)}{2}$. The remaining blocks are obtained by taking the reverse of these blocks. (The addition is under mod p.) For example, if p=5, the arranged blocks are

[1,2,3,4,5], [1,3,5,2,4], [1,4,3,5,3], [1,5,4,3,2] .

Remark (2). BIBD(v,4,λ) ⇒ CBIBD(v,4,(2λ)*). If we take an arbitrary block, say {1,2,3,4}, of a BIBD(v,4,λ), its six copies are arranged as [1,2,3,4], [1,2,4,3], [1,3,2,4], [1,3,4,2], [1,4,2,3] and [1,4,3,2].

Remark (3). BIBD(v,6,λ) ⇒ CBIBD[v,6,(2λ)*]; the CBIBD is obtained by taking ten copies of the BIBD, each block, say {1,···,6}, of the BIBD is arranged as:

[1,2,3,4,5,6], [1,4,3,6,2,5], [1,3,2,4,5,6],
[1,4,6,2,5,3], [1,2,4,6,3,5]

and their reverses.

Examples.

(1) CBIBD[9,4,1*]:

[0,1,4,3]	[1,2,5,4]	[2,0,3,5]
[0,5,1,8]	[1,3,2,6]	[2,4,0,7]
[6,7,1,0]	[7,8,2,1]	[8,6,0,2]
[6,2,7,5]	[7,0,8,3]	[8,1,6,4]
[3,4,7,6]	[4,5,8,7]	[5,3,6,8]
[3,8,4,2]	[4,6,5,0]	[5,7,3,1].

(2) CBIBD[6,4,2*]:

[1,2,3,4]	[6,3,2,1]	[1,3,2,5]
[1,2,4,5]	[2,1,4,6]	[2,6,1,5]
[1,5,4,3]	[1,3,6,4]	[3,1,6,5]
[6,1,4,5]	[2,3,5,4]	[2,4,3,6]
[2,6,3,5]	[4,2,5,6]	[3,4,6,5].

(3) CBIBD[7,4,2*]: Develop the complementary difference sets mod 7:

[0,1,3,2]	[0,3,2,6]	[2,0,4,6].

(4) CBIBD[8,4,2*]:

[1,2,3,4]	[1,7,6,2]	[1,3,7,5]
[1,4,5,6]	[1,5,2,8]	[1,6,8,3]
[1,8,4,7]	[2,7,5,4]	[2,5,3,6]
[2,8,6,4]	[2,3,8,7]	[3,7,4,6]
[3,5,8,4]	[5,8,7,6]	

and the same blocks in the reverse order.

Remark (4). If the complementary difference sets of a BIBD(v,k,(k-1)λ) can be arranged so that the differences between the adjacent numbers are λ* times each nonzero integer (mod v) then we get a cyclic BIBD with λ*.

Theorem 2.6. *A* CBIBD[v,4,2*] *exists for* v ≡ 0,1(mod 4).

Proof. By theorem 2.4(i) it is merely necessary to show the existence of

a CBIBD for $v \in K_4^1$ which is done as follows:

v = 4 : Remark (2) with λ=1. v = 5 : Introduction.

v = 8 : Example 4. v = 9 : Two copies of example 1.

v =12 : Developing the initial blocks [0,1,7,3], [3,7,1,0], [0,2,8,7], [7,8,2,0], [∞,0,3,1], [1,3,0,∞] mod 11.

Theorem 2.7. *A* CBIBD[v,4,4*] *exists for all* $v \geq 4$.

Proof. By theorem 2.4(iii) we have to show the existence of CBIBD[v,4,4*] for $v \in K_4^2$. For $v \equiv 0,1 \pmod 4$ it is proved using theorem 2.6 and for remaining values of v the result follows by developing the initial blocks in table 2.1.

Table 2.1

Treatments	Construction
6	Two copies of example (2).
7	Example (3). Take two copies.
10	[∞,2,4,0], [∞,0,3,1], [0,1,2,5], [5,0,2,1], [2,0,6,3] mod 9 and each initial block in reverse order also.
11	[0,1,4,2], [0,2,8,4], [0,5,4,8], [0,8,5,10], [0,10,5,9] mod 11 giving CBIBD(11,4,2*), take two copies.
14	[∞,0,1,3], [∞,0,5,2], [0,2,8,4], [0,3,7,2], [0,6,1,2], [0,1,8,5], [0,4,7,1] mod 13 and each block in reverse order also.
15	Corollary 2.3.
18	[∞,4,3,0], [∞,7,0,5], [0,8,5,1], [0,6,13,8], [0,5,8,6], [0,8,6,13], [0,6,14,13], [0,13,14,2], [0,10,16,2] mod 17 and each block in reverse order also.
19	[0,1,3,9], [0,3,9,8], [0,9,8,5], [0,8,5,15], [5,0,7,15], [0,15,7,23], [0,6,2,7], [0,18,6,2], [0,16,18,6] mod 19 and each block in reverse order also.
22	Theorem 2.4(ii).
23	[0,1,5,2], [0,10,2,5], [4,0,2,10], [4,10,0,20], [4,20,8,0], [20,0,17,8], [0,8,17,16], [17,0,11,16], [11,16,0,9], [0,11,9,22], [0,18,22,9] mod 23 and each block in reverse order also.

Using Hanani's Lemma 2.3 [7] we have

Lemma 2.8. *If* $\lambda' | \lambda$ *then* $CB(K,\lambda') \subseteq CB(K,\lambda)$.

Using Lemma 2.8 together with Theorems 2.6 and 2.7 we have

Theorem 2.9. *A* CBIBD[v,4(4t+2)*] *exists for* $v \equiv 0,1 \pmod 4$ *and a* CBIBD[v,4,(4t)*] *exists for all* $v \geq 4$.

3. DIRECTED GROUP DIVISIBLE DESIGNS WITH $k = 4$ AND $\lambda_1 = 0$.

The existence of a $GD[k,\lambda,m;v]$ implies the existence of $DGD[k,\lambda^*,m;v]$; the DGD is obtained by writing each block of the DGD twice - once in the given order and once in the reverse order. Hence using Hanani's results we have:

Lemma 3.1. (a) *If* λ' *divides* λ, *then* $DGD(k,\lambda',m) \subseteq DGD(k,\lambda,m)$.

(b) *If* $v \in GD(4,\lambda,m)$, *then for* $r \notin \{2,6\}$, $rv \in DGD(4,\lambda^*,rm)$.

(c) *If* $n \equiv 1 \pmod 3$, *then* $v = 2n \in DGD(4,1^*,2)$.

(d) *If* $n \equiv 0$ or $1 \pmod 4$, *then* $v = 3n \in DGD(4,1^*,3)$.

(e) *If* $n \geq 4$, *then* $v = 6n \in DGD(4,1^*,6)$.

(f) *For all* $n \geq 4$, $n \in B(K_4,1^*)$ *holds, where* $K_4 = \{4,\cdots,12,14,18,19,23\}$.

Proof. Proof of (b) is a part of the proof of Theorem 6.3 of [2].

(c) can be proved by observing that for $n \equiv 1 \pmod 3$, $n \neq 4$, $2n \in GD(4,1,2)$ (refer [2]) and for $n = 4$, the $DGD[4,1^*;2;8]$ is given below:

<1,3,2,4> <5,6,8,7> <2,7,1,8> <6,4,3,5>
<3,8,6,1> <7,5,4,2> <4,1,7,6> <8,2,5,3>.

For (e), if $n > 4$, then Lemma 6.15 of Hanani gives $6n \in DGD(4,1^*,6)$ and for $n = 4$, $DGD[4,1^*,6;24]$ is given below:

<1,20,12,13>	<4,14,22,8>	<13,21,12,1>	<19,15,10,4>
<1,8,23,17>	<4,12,16,23>	<16,9,22,1>	<20,18,8,4>
<1,9,14,24>	<4,11,21,15>	<24,15,11,1>	<17,22,11,4>
<20,1,7,15>	<4,7,17,24>	<17,7,1,21>	<16,12,4,19>
<23,1,11,18>	<23,4,10,13>	<18,10,1,22>	<14,7,4,20>
<1,10,19,16>	<21,4,9,18>	<19,8,14,1>	<24,13,9,4>
<2,7,18,19>	<5,14,19,11>	<22,14,12,2>	<20,16,11,5>
<2,11,20,17>	<5,22,18,10>	<17,10,23,2>	<18,9,21,5>
<2,12,14,21>	<5,23,9,15>	<24,16,7,2>	<13,23,7,5>
<19,2,9,13>	<19,5,12,17>	<13,8,2,22>	<17,12,5,20>
<2,10,15,24>	<22,5,7,16>	<18,11,2,23>	<15,8,5,21>
<21,2,8,16>	<5,8,13,24>	<15,20,9,2>	<24,14,10,5>
<3,8,18,20>	<6,7,23,14>	<19,18,7,3>	<15,7,22,6>
<3,21,7,13>	<6,8,15,19>	<16,21,10,3>	<23,16,8,6>
<3,12,22,15>	<6,9,16,20>	<15,23,12,3>	<9,17,19,6>
<20,3,10,14>	<6,10,21,17>	<13,11,3,19>	<13,10,20,6>
<3,11,16,24>	<6,11,22,13>	<24,17,8,3>	<21,11,14,6>
<22,3,9,17>	<6,12,18,24>	<14,9,3,23>	<24,18,12,6>.

From Street and Seberry [17] we have

Lemma 3.2. (a) *If* $n \in DB(K,\lambda^*)$ *and* $mK \subset GD(k,\lambda',m)$, *then* $mn \in DGD(k,\lambda'\lambda^*,m)$. (b) *If* $v \equiv 1 \pmod 3$, *then* $v \in DB(4,1^*)$.

Lemma 3.3. *For all* $n \geq 4$, $3n \in DGD(4,1^*,3)$.

Proof. In view of lemma 3.1(f), it is sufficient to prove that for all $n \in K_4$, $3n \in DGD(4,1^*,3)$. Lemma 3.1(d) proves this for $n \equiv 0,1 \pmod 4$. For the remaining values of n the solution is given in table 3.1.

Table 3.1

n	v=3n	DGD(4,1*,3)
6	18	Initial blocks to be developed mod(3,5). <(1,1), (0,∞), (1,4), (0,0)>, <(0,0), (2,2), (0,∞), (2,3)>, <(1,4), (1,1), (2,3), (2,2)>.
7	21	Lemma 3.2; 12 ∈ GD(4,1,3).
10	30	Lemma 3.2; 12 ∈ GD(4,1,3).
11	33	11 ∈ DB(5,1*) (Table 1 of Street and Seberry [17] and 15 ∈ GD(4,1,3)).
14	42	Initial blocks to be developed mod(3,13). <(1,2), (1,11), (2,4), (2,9)>, <(1,3), (1,10), (2,6), (2,7)>, <(2,5), (2,8), (1,1), (1,12)>, <(1,11), (2,3), (1,2), (2,10)>, <(2,7), (2,6), (1,9), (1,4)>, <(1,12), (0,∞), (0,0), (1,1)>, <(0,0), (2,8), (0,∞), (2,5)>.
15	45	Table 1 of Street and Seberry [17].
18	54	Initial blocks to be developed mod(3,17). <(2,12), (1,3), (1,14), (2,5)>, <(1,9), (2,7), (2,10), (1,8)>, <(2,6), (1,15), (1,2), (2,11)>, <(1,14), (1,3), (2,8), (2,9)>, <(2,4), (1,10), (2,13), (1,7)>, <(1,5), (2,2), (2,15), (1,12)>, <(2,16), (1,11), (2,1), (1,6)>, <(1,1), (0,0), (0,∞), (1,16)>, <(2,13), (0,∞), (0,0), (2,4)>.
19	57	Lemma 3.2; 12 ∈ GD(4,1,3).
23	69	Initial blocks to be developed mod(3,23). <(1,22), (1,1), (2,5), (2,18)>, <(1,18), (1,5), (2,2), (2,21)>, <(1,21), (2,10), (2,13), (1,2)>, <(2,4), (2,19), (1,13), (1,10)>, <(2,3), (1,19), (2,20), (1,4)>, <(1,20), (2,15), (1,3), (2,8)>, <(1,8), (1,15), (2,6), (2,17)>, <(1,17), (2,7), (1,6), (2,16)>, <(2,11), (2,12), (1,16), (1,7)>, <(2,9), (2,14), (1,12), (1,11)>, <(2,1), (1,14), (2,22), (1,9)>.

Initial blocks of the directed designs are written as <a,b,···,k>.

Remark (4). If $m \equiv 0 \pmod 2$, the necessary conditions for the existence of $GD[4,\lambda,m]$ are the same as for the existence of $GD[4,2\lambda,m]$ and hence $DGD[4,\lambda^*,m]$ exists if and only if $GD[4,\lambda,m]$ exists, except for two non-existing transversal designs $T[4,1;2]$ and $T[4,1;6]$.

Theorem 3.4. *Let* m, λ *and* v *be positive integers. The necessary and sufficient conditions for the existence of a directed group divisible design* DGD[4,λ*,m;v] *are*

$v \equiv 0 \pmod m$, $\lambda^*(v-m) \equiv 0 \pmod 3$, $\lambda^* v(v-m) \equiv 0 \pmod 6$ and $v \geq 4m$.

Proof. Theorem 6.1 of [7] gives the necessary conditions. By Theorem 6.3 of [2], lemma 3.1(b) and the above remark (4) we need to prove the sufficiency only for $m = 3$. This is done in lemma 3.3 and lemma 3.1(a).

4. CYCLIC GROUP DIVISIBLE DESIGNS WITH $k = 3$.

The existence of a GD[3,λ,m;v] implies the existence of CGD[3,λ*,m;v]. The CGD is obtained by writing each block of GD twice - once in the given order and once in the reverse order - and hence using Hanani [7], we have the following results:

Lemma 4.1. *If* $v \in$ GD(3,λ,m) *holds and if* r *is a positive integer, then* rv ∈ CGD(3,λ*,rm) *holds.*

Lemma 4.2. *If* $n \equiv 0$ *or* $1 \pmod 3$, *then* 2n ∈ CGD(3,1*,2) *holds.*

We notice that for $n \equiv 2 \pmod 3$, the necessary conditions are not satisfied.

Lemma 4.3. *For every* $n \geq 3$, 6n ∈ CGD(3,1*,6) *holds.*

Lemma 4.4. *For every* $n \geq 3$, 2n ∈ CGD(3,3*,2) *holds.*

Lemma 4.5. *If* n ∈ CB(K,λ*), mK ⊂ GD(k,λ,m), *then* mn ∈ CGD(k,λλ*,m).

Proof. Similar to the proof of Street and Seberry [17] except that, while constructing GD[k,λ,m] from the blocks of CB(K,λ*), we write the elements from the groups G_i's in the same order as the G_i's have occurred in the block of CB(K,λ*).

Lemma 4.6. *If* λ' *divides* λ, *then* CGD(K,λ'*,M) *is a subset of* CGD(K,λ*,M).

Proof. Let $\lambda = p.\lambda'$ and $v \in$ CGD(K,λ'*,M) then there exists a CGD[K,λ'*,M;v], hence $v \in$ CGD(K,λ*,M).

Lemma 4.7. *If* $v \in$ CGD(3,λ*,x) *and* $x \in$ CGD(3,λ*,3), *then* $v \in$ CGD(3,λ*,3).

Proof. For each group of the CGD[3,λ*,x;v] construct the corresponding CGD[3,λ*,3;v]. We write the blocks of all the CGD[3,λ*,3;x] to get the CGD[3,λ*,3;v].

Lemma 4.8. *If* n ∈ B(K,λ') *and* $mK \subseteq$ CGD(k,λ*,m), *then* mn ∈ CGD(k,λ'λ*,m).

Proof. There are n groups for the required $CGD[k,\lambda'\lambda^*,m]$. Considering these n groups as treatments we construct a $B[K,\lambda';n]$. Replace each block by the corresponding $CGD[k,\lambda^*,m]$, (which exist by the hypothesis), to get the required $CGD[k,\lambda'\lambda^*,m]$.

Lemma 4.9. *For every* $n \geq 3$, $3n \in CGD(3,1^*,3)$.

Proof. We know that for every integer $n \geq 3$, $n \in B(K_3,1)$ where $K_3 = \{3,4,5,6,8\}$. (See [7].) By Lemma 4.8, it suffices to show that $3n \in CGD(3,1^*,3)$ for every $n \in K_3$. For $n \equiv 1 \pmod 2$, $3n \in GC(3,1,3)$ (see [7]) and hence for $n = 3,5$, $3n \in CGD(3,1^*,3)$. For $n=4$, we use Lemma 4.5 and the fact that $4 \in CB(3,1)$ and $9 \in GD(3,1,3)$. For $n=8$ the required CGD is given below (with the notation of [7]). Let the set of vertices be $X = Z(3,2) \times (Z(7,3) \cup \infty)$; the following blocks developed mod (3,7) give the blocks of the design.

$[(\phi,\phi), (0,\alpha'), (0,-\alpha')] \bmod (3,7)$, $\alpha = 1,2,3$;

$[(0,\alpha+4), (0,\alpha+1), (\phi,\phi)] \bmod (3,7)$, $\alpha = 0,1$;

$[(\phi,0), (\phi,\infty), (\phi,3)] \bmod (3,7)$;

$[(\phi,\infty), (1,0), (0,\phi)] \bmod (3,7)$;

$[(1,3), (\phi,\infty), (0,\phi)] \bmod (3,7)$.

For $n = 6$, $CGD(3,1^*,3;18)$ is given below.

[0,6,9] [1,7,5] [2,8,6] [3,9,7] [4,5,8]
[5,11,14] [6,12,10] [7,13,11] [8,14,12] [9,10,13]
[10,1,4] [11,2,0] [12,3,1] [13,4,2] [14,0,3]
[0,7,8] [1,8,9] [2,9,5] [3,5,6] [4,6,7]
[5,12,13] [6,13,14] [7,14,10] [8,10,11] [9,11,12]
[10,2,3] [11,3,4] [12,4,0] [13,0,1] [14,1,2]
[8,7,0] [9,8,1] [5,9,2] [6,5,3] [7,6,4]
[13,12,5] [14,13,6] [10,14,7] [11,10,8] [12,11,9]
[15,11,5] [15,12,6] [15,13,7] [15,14,8] [15,10,9]
[15,5,14] [15,6,10] [15,7,11] [15,8,12] [15,9,13]
[15,4,1] [15,0,2] [15,1,3] [15,2,4] [15,3,0]
[16,1,10] [16,2,11] [16,3,12] [16,4,13] [16,0,14]
[16,10,4] [16,11,0] [16,12,1] [16,13,2] [16,14,3]
[16,9,6] [16,5,7] [16,6,8] [16,7,9] [16,8,5]
[17,6,0] [17,7,1] [17,8,2] [17,9,3] [17,5,4]
[17,0,9] [17,1,5] [17,2,6] [17,3,7] [17,4,8]
[17,14,11] [17,10,12] [17,11,13] [17,12,14] [17,13,10] .

Theorem 4.10. *Let* m, λ *and* v *be positive integers. The necessary and sufficient conditions for the existence of a cyclic group divisible design* CGD[3,λ^*,m;v] ($v \neq 6$ *and* $m \neq 1$) *are*

$$v \equiv 0 \pmod{m}, \quad v \geq 3m \quad \textit{and} \quad \lambda v(v-m) \equiv 0 \pmod{3}.$$

Proof. The necessity follows from the Theorem 6.2 of Hanani [7] and the fact that a CGD[3,λ^*,m;v] is a GD[3,2λ,m;v]. In order to prove the sufficiency, as in [7] we consider only those values of λ and of m which are factors of 6. In all these cases the existence of the relevant CGD is proved in the Lemmas listed in table 4.1. For $m = 1$ CGD is a cyclic triple system and hence the exception of $v = 6$ [10].

Table 4.1

m	λ^*	Proof
2	1,2,3,6	Lemmas 4.2, 4.4 and 4.6
3	1,2,3,6	Lemmas 4.6 and 4.9
6	1	Lemma 4.3

Summary.

We have proved:

(i) CBIBD(v,b,r,4,(4t+2)*) exist for $v \equiv 0, 1 \bmod 4$;

(ii) CBIBD(v,b,r,4,(4t)*) exist for all $v \geq 4$;

(iii) DGDDs with block size 4 exist;

(iv) CGDDs with block size 3 exist except $v = 6$ and group size 1.

Our proofs of the results mentioned above depend on the various elementary results similar to those of Hanani and recall that our definition of GDD is the one given by Hanani. To prove the results for cyclic BIBDs we proved the following intermediate results:

(i) existence of CBIBD[k,j,λ^*] and BIBD(v,k,λ') ⇒ existence of CBIBD[v,j,($\lambda'\lambda$)*];

(ii) existence of PBD[K,λ,v] and CBIBD[k,μ^*,v] for each k => existence of CBIBD[v,j,($\lambda\mu$)*];

(iii) CBIBD[k,4,2*] exists for $k \in \{4,5,8,9,12\}$ and hence CBIBD[u,4,2*] exists for $u \equiv 0$ or $1 \bmod 4$;

(iv) CBIBD[k,4,4*] exist for $k \in \{4,\ldots,12,14,15,18,19,22,23\}$ and hence CBIBD[v,4,4*] exist for $v \geq 4$.

Similarly to prove the existence of directed GDDs we proved:

(i) For $n \equiv 1 \bmod 3$, $2n \in DGD(4,1^*,2)$;

(ii) For $n \equiv 0$ or $1 \bmod 4$, $3n \in DGD(4,1^*,3)$;

(iii) For $n \in \{4,\ldots,12,14,18,19,23\}$ $3n \in DGD(4,1^*,3)$ and hence for all $v \geq 4$, $3v \in DGD(4,1^*,3)$.

For CGDDs with block size 3, we proved the similar results, in particular, we proved that $3n \in CGD(3,1^*,3)$ for every $n \in \{3,4,5,6,8\}$ and hence $3n \in CGD(3,1^*,3)$ for all $n \geq 3$.

Acknowledgement: I would like to express my thanks to Dr. J.R. Seberry for suggesting the problems and for her valuable guidance.

REFERENCES

1. J.E. Dawson, J.R. Seberry and D.B. Skillicorn, The directed packing numbers DD(t,v,v), $t \geq 4$, *Combinatorica*. To appear.
2. A.E. Brouwer, A. Schrijven and H. Hanani, Group divisible designs with block size four, *Discrete Math.*, 20, no. 1, (1977), 1-10.
3. C.J. Colbourn and M.J. Colbourn, Every two-fold triple system can be directed, *J. Combinatorial Theory*, Ser. A. 34, (1983), 375-378.
4. M.J. Colbourn and C.J. Colbourn, Recursive constructions for cyclic block designs, *J. Stat. Plan. and Inf.*, 10(1984), 97-103.
5. C.J. Colbourn and J.J. Harms, Directing triple systems, *Ars Combinatoria*, 15, (1983), 261-266.
6. W. de Launey and J.R. Seberry, Generalized Bhaskar Rao designs of block size four, *Congressus Numerantium*, 41, (1984), 229-294.
7. H. Hanani, Balanced incomplete block designs and related designs, *Discrete Math.*, 11, (1975), 255-369.
8. F.K. Hwang and S. Lin . Neighbour designs, *J. Combinatorial Theory*, Ser. A. 23, (1977), 302-313.
9. S.H.Y. Hung and N.S. Mendelsohn, Directed triple systems, *J. Combinatorial Theory*, Ser. A. 14, (1973), 310-318.
10. N.S. Mendelsohn, A natural generalization of Stainer triple systems, *Computers in Number Theory* (A.O.L. Atkin and B.J. Birch, eds.), Academic Press, New York, (1971), 323-329.

11. C.A. Rodger, Triple systems with a fixed number of repeated triples. Preprint.

12. D.G. Sarvate, All directed GD's with $k = 3$ and $\lambda^* = 0$, exist, *Utilitas Mathematica*. To appear.

13. J.R. Seberry and D.B. Skillicorn, All directed BIBDs with $k = 3$ exist, *J. Combinatorial Theory*, Ser. A. 29 (1980), 244-248.

14. D.B. Skillicorn, Directed Packings and Coverings with Computer Applications, *Ph.D. Thesis*, University of Manitoba, (1981).

15. D.B. Skillicorn, Complete directed designs, *Congressus Numerantium*, 38, (1983), 247-252.

16. D.B. Skillicorn and R.G. Stanton, The directed packing numbers DD(t,v,v), Proceedings of the Eleventh Manitoba Conference on Numerical Mathematics and Computing, Winnipeg, Manitoba, 1981, *Congressus Numerantium*, 34, (1982), 247-252.

17. D. Street and J.R. Seberry, All DBIBDs with block size four exist, *Utilitas Mathematica*, 18, (1980), 27-34.

18. D. Street and W. Wilson, On directed balanced incomplete block designs with block size five, *Utilitas Mathematica*, 18, (1980), 161-174.

19. T.W. Tillson, A Hamiltonian decompostion of K^*_{2m}, $2m \geq 8$, *J. Combinatorial Theory*, Ser. B. 29, (1980), 68-74.

2.2 An observation

Replacing each block of a BIBD(v, 3, 2) = X by six directed blocks, which are permutations of the original block, produces a DBIBD(v, 3, 6*). We say that X underlies the DBIBD(v, 3, 6*). A decomposition of DBIBD(v, 3, 6*) into six DBIBD(v, 3, 1*) is denoted by DDBIBD(v, 3, 1*) and if such a decomposition of a DBIBD(v, 3, 6*) exists, then we say that the DBIBD(v, 3, 6*) underlies DDBIBD(v, 3, 1*). Harms and Colbourn (1983) have conjectured that DBIBD(v, 3, 6*), obtained from a BIBD(v, 3, 2), underlies a DDBIBD(v, 3, 1*).

Hanani's theory can be used to prove that, for the parameters satisfying the necessary conditions for the existence of BIBD(v, 3, 2), there exists a BIBD(v, 3, 2) = X such that the DBIBD(v, 3, 6*) obtained from X underlies a DDBIBD(v, 3, 1*). We use the notation of Hanani (1975).

Lemma 2.2.1: *If* $n \in B(K, 1)$ *and if for each* $k \in K$ *there exists a* BIBD(k, 3, 2) *which underlies a* DDBIBD(k, 3, 1*), *then there exists a* BIBD(n, 3, 2) *which underlies a* DDBIBD(n, 3, 1*).

Proof. Form the BIBD(k, 3, 2) which underlies a DDBIBD(v, 3, 1*) on each block of B[K, 1; n]. Writing all these BIBD(k, 3, 2)'s together will give us a BIBD(n, 3, 2) which underlies a DDBIBD(n, 3, 1*).

□

Theorem 2.2.2: *Necessary conditions are sufficient for the existence of a* BIBD(v, 3, 2) *which underlies a* DDBIBD(v, 3, 1*).

Proof. Using Lemma 2.2.1 and the fact that for $v \equiv 0, 1 \pmod 3$, with $v \in B[\{3, 4, 6\}, 1]$ we need to prove that for k = 3, 4, 6 there exists a BIBD(k, 3, 2) which underlies a DDBIBD(k, 3, 1*). For k = 4, 6 this is proved in Harms and Colbourn (1983). For k = 3, we take the BIBD(3, 3, 2) as
{1 2 3, 1 2 3}

and the corresponding DDBIBD(3, 3, 1*) is:

1 2 3, 3 2 1

1 3 2, 2 3 1

2 1 3, 3 1 2

2 3 1, 1 3 2

3 1 2, 2 1 3

3 2 1, 1 2 3.

Each row is a DBIBD(3, 3, 1*).

□

CHAPTER 3

EQUI-NEIGHBOURED DESIGNS

Kiefer and Wynn(1981) have defined an equi-neighboured BIBD (an EBIBD[k, λ^*; v]) to be a BIBD[k, λ; v,] in which the points in each block are arranged along a line and each pair of distinct points is adjacent $\lambda^* = 2\lambda/k$ times.

The following main theorems are proved in the attached published paper "A note on equi-neighboured block designs", Utilitas Mathematica, 28, 1985, 91-98.

Theorem 3.1: *An equi-neighboured* BIBD[3, 3; v] *can be embedded into an equi-neighboured* BIBD[3,3; 2v+1] *and an equi-neighboured* BIBD[3, 3; 2v+3].

Proof. Theorem 3.1 of the attached paper. □

Theorem 3.2: *If there exists an* EBIBD[3, λ; v], *then it can be embedded into an* EBIBD[3, λ; 2v+1].

Proof. Theorem 3.2 of the attached paper. □

Theorem 3.3: *Every group divisible design with* $\lambda = 3t$ *is an underlying design for an* EGDD[3, λ, m; v], *where t is an integer and* $t \geq 1$.

Proof. Theorem 4.1 of the attached paper. □

We have given many embedding theorems in this thesis. Hence here we will carry out a detailed count of occurences of the following pairs for a BIBD(2v+3, 3, 3) which is obtained by Lemma 2.4 of the attached paper. We use the BIBD(v, 3, 3) on points {1, 2, ... , v} and three copies of the complete graph over the new points {v+1, ..., 2v+3} :

(i) pair (a, b) where a and b both are points of BIBD(v, 3, 3) (i. e. old-old pair);

(ii) pair (a, b) where a is old point and b is a point in {v+1, ..., 2v+3} (i. e. old-new pair);

(iii) pair (a, b) where a and b both are from {v+1, ..., 2v+3} (i.e. new-new pair).

Please refer to Figure 1 and the proof of Lemma 2.4 of the attached paper, for the notation, A_V, B_1, C_1, and C_2 used below.

(i) old-old pair : The old-old pair can occur in the blocks obtained from A_V only, i.e. only in the blocks of BIBD(v, 3, 3). Hence every old-old pair occurs only 3 times as required.

(ii) old-new pair : Each block obtained from the submatrix

$$M = \begin{matrix} B_1 \\ C_1 \end{matrix}$$

gives two old-new pairs. Consider a fixed old point a. There are 3(v+3)/2 consecutive columns with 1's in the a^{th} row of M. These columns have two 1's in C_1 corresponding to the three distinct one-factors of K_{V+1} in C_1(see the arrangement of F_i's in the proof of Lemma 2.4). Hence the point a has occured with every new point only 3 times. Note that this also proves that the blocks corresponding to M are distinct.

(iii) new-new pair: We have used up all the one factors of the three copies of the complete graph K_{V+1} and hence each new-new pair occurs 3 times as required.

If we start with a simple BIBD(v, 3, 3), then the blocks corresponding to the matrix A_V are distinct. The blocks obtained from C_2 are distinct, as they arise from 3 one-factors and each block contains an edge from each one-factor. Hence the BIBD(2v+3, 3, 3) will be simple.

□

A note on equi-neighboured block designs

Dinesh G. Sarvate

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. Keifer and Wynn [6] have defined an equi-neighboured BIBD (an EBIBD) as a BIBD in which the points in each block are arranged along a line and each pair of points is adjacent the same number of times. These are useful in any experimental situation where correlation of the errors of adjacent plots is suspected [4,6].

Kiefer and Wynn [6] and Cheng [2] have shown that the necessary conditions are sufficient for the existence of EBIBDs with $k = 3$. Dawson [4] proved that the necessary conditions are sufficient for the existence of EBIBDs of block size 4. Hanani [5] has proved that the necessary conditions are sufficient for the existence of BIBDs of block size 3 but the designs have repeated blocks. Stanton and Goulden [8] proved the existence of BIBDs with $k = 3$ and $\lambda = 1$ without repeated blocks, using factorization of complete graphs. Street [9], on the similar lines, proved the existence of BIBDs with $k = 3$ and $\lambda = 2$ and $\lambda = 3$. She used the embedding of a BIBD with v points into BIBDs of $2v+1$ and $2v+7$ points for $\lambda = 3$. We use her embedding of $2v+1$ points together with our embedding theorem for $2v+3$ points to prove the existence of BIBDs with $k = 3$ and $\lambda = 3$. We use the graph factorization of Stanton and Goulden [8] and by properly ordering the blocks we get embedding theorems for equi-neighboured BIBDs. Such embedding theorems for directed designs are given by Seberry and Skillicorn [7] and we extend their theorem for $2v+1$ points to equi-neighboured designs.

We generalize the definition of equi-neighboured BIBD in a natural way to define equi-neighboured group divisible designs. Then, using the same construction method as Kiefer and Wynn [6], prove that given a group divisible design which satisfies the necessary condition, it can be ordered to get the equi-neighboured GDD. Using the similar terminology used in Colbourn and Colbourn [3], we can write our results as:

Every group divisible design with $\lambda = 3t$ underlies a equi-neighboured GDD.

We define a *group divisible design* as in Hanani [5]. Let X be a v-set such that $X = \bigcup_{i=1}^{n} G_i$, $G_i \cap G_j = \phi$, $i \neq j$, $|G_i| = m$ for all i. The G_i's are called the groups. A group divisible design, $GD[k,\lambda,m;v]$, is a collection of k-subsets of the v-set X such that each block intersects each group in at most one element and a pair of elements of X from different groups occurs in exactly λ blocks. In a similar way, we can define a $GD[K,\lambda,M;v]$, where the size of each block is an element of K and the size of each group is an element of the set M. $GD(K,\lambda,M)$ denotes the set of all v such that a $GD[K,\lambda,M;v]$ exist.

An *equi-neighboured BIBD* $EBIBD[K,\lambda,\lambda^* v]$ is a $BIBD[K,\lambda;v]$ in which each block is given a linear ordering and each pair of distinct points is adjacent λ^* times. If $K = \{k\}$, then $\lambda^* = 2\lambda/k$ and we call it an $EBIBD[k,\lambda;v]$.

In a similar way, we define an *equi-neighboured group divisible design* $EGDD[K,\lambda,\lambda^*,M;v]$ system and when $K = \{k\}$ and $M = \{m\}$ we call it an $EGDD[k,\lambda,m;v]$.

A *complete graph* K_n on n vertices consists of n vertices and the $\binom{n}{2}$ joining edges [refer 8]. A *one-factor* of K_{2n} consists of n vertex-disjoint edges. A *one-factorization* of K_{2n} consists of $2n-1$ one-factors such that the edges in the one-factors are all distinct. For examples the reader is referred to [8].

2. Recursive Constructions

A block design can also be written as a vxb incidence matrix with $(i,j)^{th}$ entry equal to 1 if the element i belongs to j^{th} block and 0 otherwise. For the sake of completeness and the point of view of the application to the construction of equi-neighboured design, we reproduce the required theorems from Stanton and Goulden [8] and the proof of the embedding theorem of Street [9].

All the edges of K_{2n} fall into n disjoint classes $P_1, P_2, \cdots, P_n$ where the edge (i,j) is in P_k if and only if $i-j = k \pmod{2n}$. Stanton and Goulden [8] called this splitting the difference partition of K_{2n}. Consider the triangles (1+i,2+i,4+i) for i = 1,2,···,2n. This gives a set T of 2n triangles.

Theorem 2.1 [8]: *The set T of 2n triangles contains exactly those edges from* P_1, P_2, P_3.

Theorem 2.2 [8]: *The graph* K_{2n} *may be factored into a set of triangles covering* P_1, P_2, P_3 *and a set of (2n-7) one-factors covering the other* P_i's.

Using Lemma 2 and Theorem 3.1 of [2] we get:

Theorem 2.3: *The graph* K_{2n} *may be factored into a set of 6 one-factors covering* P_1, P_2, P_3 *and a set of (2n-7) one-factors covering the other* P_i's.

This observation immediately leads us to the embedding of a BIBD[3,3;v] into a BIBD[3,3;2v+3].

Lemma 2.4: *If there exists a BIBD[3,3;v], then it can be embedded into a BIBD [3,3;2v+3].*

Proof: Let A_v denote the incidence matrix of the BIBD[3,3; v]. For V = 2v+3, the structure of the incidence matrix is given in figure 1.

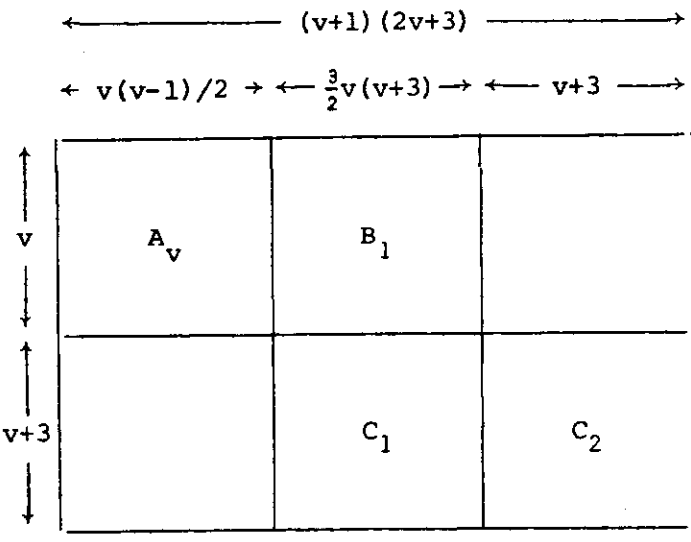


Fig. 1: Incidence matrix A_V of BIBD[3,3;2v+3].

Here $B_1 = I_v \times J_{1,(3(v+3)/2)}$ where I_v denotes the identity matrix of order v and $J_{m,n}$ in general denotes the m×n matrix of all entries 1. Let P11,P12,P(23)1,P(23)2,P(23)3,P(23)4 denote the one-factors arising from P_1, P_2, P_3. The remaining one-factors are denoted by F1,F2, ...,F(v-4). The first $4\times(3(v+3)/2)$ columns of C_1 correspond to

P11,P(23)1,P(23)2,P12,P(23)2,P(23)3,P11,P(23)3,P(23)4,P12,P(23)4,P(23)1

and the (v+3) columns of C_2 are filled by the set T of triangles. The remaining columns of C_1 correspond to the 3 sets of the one-factors Fi's. The one-factors are arranged so that there are no repeated blocks. This can

be done as follows: The remaining columns of C_1 are filled by:

F1,F2,F3;F2,F3,F4;F3,F4,F5;$\cdots$;F(v-6),F(v-5),F(v-4);F(v-5),F(v-4),F1;
F(v-4),F1,F2;.

Notice that each one-factor has occurred at $3s^{th}$ position only once for some $s = 1,2,\cdots,(v-4)$.

Lemma 2.5 [9]: *If there exists a BIBD[3,3; v], then it can be embedded into a BIBD[3,3,2v+1].*

Proof: Consider the incidence matrix A_v of the BIBD[3,3;v]. Let $V = 2v+1$. The structure of A_V is shown in figure 2.

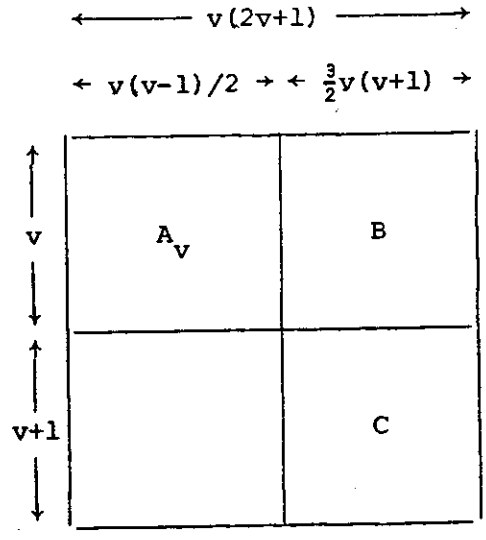


Fig. 2: The incidence matrix A_V of BIBD[3,3;2v+1].

Here $B = I_v \times J_{1,3(v+1)/2}$, and if the one-factors of K_{v+1} are F1,F2,$\cdots$,F(v+1), the columns of C correspond to:

F1,F2,F3;F2,F3,F4;$\cdots$;Fv,F(v+1),F1;F(v+1),F1,F2;.

Again the construction is such that each one-factor has occurred once at the $3s^{th}$ place for some $s = 1,2,\cdots,(v+1)$.

Theorem 2.6: *The necessary conditions are sufficient for the existence of simple (no repeated blocks) BIBD[3,3;v]. (v > 3).*

Proof: The necessary condition for BIBD[3,3;v] is $v \equiv 1 \bmod 2$. We use induction to prove the sufficiency. To start the induction we need BIBD's for $V = 5,7,9$ which is done in [9] and the references therein. Now lemmas 2.4 and 2.5 complete the proof.

3. Construction of Equi-neighboured Designs

Theorem 3.1: *Equi-neighboured BIBD[3,3;v] can be embedded into an equi-neighboured BIBD[3,3;2v+1] and an equi-neighboured BIBD[3,3;2v+3].*

Proof: The case of embedding in BIBD[3,3;2v+1] is obvious from the proof of the lemma 2.5. We arrange the one-factors occurring at the $3s^{th}$ place such that the point $1,\cdots,v$ placed in the middle. In other words, if (a,b) is an edge of one-factor occurring with the point i of the EBIBD[3,3;v], then the ordered block will be [a,i,b]. The proof for the case 2v+3 is similar except that the blocks corresponding to C_2 are arranged as [1+i,4+i,2+i].

We now extend the result of Seberry and Skillicorn [7] for the equi-neighboured designs.

Theorem 3.2: *If there exists an EBIBD[3,λ;v], then it can be embedded into an EBIBD[3,λ;2v+1].*

Proof: Recall that in EBIBD notation, λ means we arrange the blocks such that each pair occurs 2λ/3 times. We take the blocks of EBIBD[3,λ;v] together with the blocks given by Seberry and Skillicorn λ/3 times, arranged as [j,v+i,v+i+j], i = 1,•••,v+1; j = 1,•••,v. Where the elements in the third position are reduced, when greater than 2v+1, by subtracting v+1, so as to remain in the set {v+1,•••,2v+1}. For fixed j, as i varies, the resulting set of blocks cover once all pairs of the form (j,x) and twice all pairs of the form (x,x+j); x and x+j in {v+1,•••,2v+1}. Now we take the one-factorization of K_{v+1} as given by Stanton and Goulden [8] and form the blocks for i = 1,•••,v such that the pairs from the i^{th} one-factor come with the point i where i occurs in the middle of the block. For example, one extends the EBIBD[3,3;3] on three elements ([1,2,3],[2,1,3],[2,3,1]) by adding first the blocks of the form [j,v+i,v+i+j] viz.

[1,4,5], [1,5,6], [1,6,7], [1,7,4];
[2,4,6], [2,5,7], [2,6,4], [2,7,5];
[3,4,7], [3,5,4], [3,6,5], [3,7,6];

and then adjoining the blocks arising from one-factors of K_4 viz.

F1: (4,7), (5,6);
F2: (5,7), (6,4);
F3: (6,7), (4,5);

so that the blocks are:

[4,1,7], [5,1,6];

[5,2,7], [6,2,4];

[6,3,7], [4,3,5]; .

4. Equi-neighboured Group Divisible Designs

As mentioned in the introduction, we extend the proof of Keifer and Wynn [6] for EGDD. Using the terminology of Colbourn and Colbourn [3] we write our result as:

Theorem 4.1: *Every group divisible design with* $\lambda = 3t$ *is an underlying design for a* $EBDD[3,\lambda,m;v]$, *where* t *is an integer* ≥ 1.

Proof: Consider a group divisible design with $v = mn$ points, where n is the number of groups and m is the group size. As we know, there are $b = tv(v-m)/2$ blocks, each point occurs $r = 3t(v-m)/2$ times and each pair of points from the different groups occurs in $3t$ blocks. The points from the same group do not occur together.

There are $v(v-m)/2$ pairs to be considered. If we can order the blocks such that all these pairs occur at the end of the blocks t times, then automatically we will get $2t$ times each of these pairs occurring together in a block. Notice that there are only $t\big(v(v-m)\big)/2$ blocks.

Now write each block as a triple (t_1, t_2, t_3) of subsets of size 2 contained in it. In what follows the two blocks with identical elements are considered different.

Let S_{ti} be the set of all blocks containing a fixed subset t_i of size 2. For any p different subsets $t_1,t_2,\cdots,t_p$ of size 2, $1 \le p \le \big(v(v-m)\big)/2$, the number of distinct blocks in $\cup S_{ti}$ is greater than or equal to t.p.

Using Agrawal's theorem of system of distinct representatives [1], we can select a collection H_i of blocks in each S_{ti}, with $H_i \cap H_j = \phi$ for $i \neq j$. Notice that $\cup H_i$, $i = 1,\cdots,v(v-m)/2$, is the set of all the blocks of the GDD. Each block of H_i is ordered so that the pair of points in t_i occurs at the end, which completes the proof.

Defining equi-neighboured partially balanced designs in the similar way to equi-neighboured GDD, we obtain:

Lemma 4.2: *If an EPBIBD(v,b,r,k=3,λ_1=0,λ_2,n1,n2) exists, then EPBIBD(Nv,N^3b,N^2r,k=3,0,Nλ_2,Nn1,Nn2) eixsts.*

Proof: Replace the points ul,u2,$\cdots$,uv by $u_1^1,\cdots,u_1^N,\cdots,u_v^1,\cdots,u_v^N$ and blocks [uℓ,um,un] by $\{u_\ell^i,u_m^j,u_n^k\}$, i,j,k = 1,2,$\cdots$,N. It is easy to see that we get the required EPBIBD.

Lemma 4.3: *If EGDD[k,λ,m;v] = X and EGDD[k,λ,v;kv] = Y exists, then a EGDD[k,λ,m;kv] exists.*

Proof: Let kv points be $u_1^1,\cdots,u_v^1,u_1^2,\cdots,u_v^2,\cdots,u_1^k,\cdots,u_v^k$. Let X_i denote the EGDD with $u_1^i,u_2^i,\cdots,u_v^i$ points. Then

$$X_1,X_2,X_3,\cdots,X_k;Y$$

gives the required EGDD.

Acknowledgements

My sincere thanks to my supervisor, Dr. J.R. Seberry, for her constant help and encouragement.

References

[1] Hiralal Agrawal, *Some generalizations of distinct representatives with Applications to statistical designs*, Ann. Math. Statist., 37, 525-526 (1966).

[2] Ching-Shui Cheng, *Construction of optimal balanced incomplete block designs for correlated observations*, Ann. Statist., 11, 240-246 (1983).

[3] C.J. Colbourn and M.J. Colbourn, *Every two fold triple system can be directed*, J. Combinat. Theory, A 34, 375-378 (1983).

[4] J.E. Dawson, *Equi-neighboured designs of block size four*, Ars Combinatoria, to appear.

[5] Haim Hanani, *Balanced incomplete block designs and related designs*, Discrete Math., 11, 255-369 (1975).

[6] J. Kiefer and H.P. Wynn, *Optimum balanced incomplete block designs and Latin square designs for correlated observations*, Ann. Statist., 9, 737-757 (1981).

[7] J.R. Seberry and D.B. Skillicorn, *All directed designs with k=3 exist*, J. Combinat. Theory, A 29, 244-248 (1980).

[8] R.G. Stanton and I.P. Goulden, *Graph factorization, general triple systems and cyclic triple systems*, Aequationes Mathematicae, 22, 1-22 (1981).

[9] A.P. Street, *Some designs with block size three*, Combinatorial Mathematics VII, Lecture Notes in Mathematics, 829 (Springer-Verlag, Berlin), 224-237 (1980).

CHAPTER 4

SIMPLE DESIGNS

A BIBD without repeated blocks is called a simple BIBD. The motivation to study simple BIBDs came from reading A. P. Street (1980) and the applications of simple designs to prove the existence of other designs. For example, if simple designs are used in existence algorithms, more elegant and efficient proofs can be obtained because of inherent constraints imposed by the initial simple design. Two published papers are attached:

(a) "Block designs without repeated blocks", Ars Combinatoria, 21, 1986, 71-87

and (b) "All simple BIBDs with block size 3 exist", Ars Combinatoria, 21A, 1986, 257-270.

Recall that the necessary conditions for the existence of a BIBD(v, k, λ) are

(i) $\lambda(v-1) = r(k-1)$,

(ii) $vr = bk$,

(iii) $b \geq v$.

For a simple BIBD(v, k, λ), we have an additional condition

(iv) $\lambda \leq \binom{v-2}{k-2}$.

In particular, the necessary conditions for the existence of a simple BIBD(v, 3, λ) are

(i) $\lambda \leq (v-2)$,

(ii) (a) if the greatest common divisor of λ and 6 (G.C.D(λ, 6)) is equal to 1, then $v \equiv 1, 3 \pmod 6$;

(b) if GCD(λ, 6) = 2, then $v \equiv 0, 1 \pmod 3$;

(c) if GCD(λ, 6) = 3, then $v \equiv 1 \pmod 2$;

(d) if GCD(λ, 6) = 6, then no condition on v.

For the notation used in the attached papers, please refer to Hanani(1975).

The main result is:

Theorem 4.1: *The necessary conditions are sufficient for the existence of simple BIBDs with block size 3.*

Proof. Theorem 2.5 of (b). □

The proof of the above theorem depends on the following lemma and some theorems given in (a) and (b).

Lemma 4.2: *For all t such that* $t \leq \binom{v-2}{k-2} / \lambda$, *except possibly for one value of t, the existence of a simple* BIBD(v, k, λ) *implies the existence of a simple* BIBD(v, k, λt) *and the exceptional value of t satisfies*

(i) *t is odd,*

and (ii) $t\lambda < \binom{v-2}{k-2} < (t+1)\lambda$.

Proof. Lemma 2.11 of (b). □

In the proof of Theorem 3.7 of (b), the third sentence of the second paragraph (which starts with "Observe that") can be rewritten for clarity as follows.

Consider three distinct even numbers, say a, b and c, where $2 < a, b, c < n-1$. If n-1 is even then apply Lemmas 3.3, 3.4 and 3.5 on P_1, $(P_2 \cup P_3), \ldots, P_{a+1}, (P_{a+2} \cup P_{a+3}), \ldots, P_{b+1}, (P_{b+2} \cup P_{b+3}), \ldots, P_{c+1}, (P_{c+2} \cup P_{c+3}), \ldots, (P_{n-2} \cup P_{n-1})$. We get 2n-8 one-factors. If n-1 is odd, then apply Lemmas 3.3, 3.4 and 3.5 on P_1, $(P_2 \cup P_3), \ldots, P_{a+1}, (P_{a+2} \cup P_{a+3}), \ldots, P_{b+1}, (P_{b+2} \cup P_{b+3}), \ldots, P_{c+1}, (P_{c+2} \cup P_{c+3}), \ldots, (P_{n-3} \cup P_{n-2})$. We get 2n-10 one-factors.

The definition of s-distance apart arrangement of one-factor given after the proof of Theorem 3.8 can be restated as follows.

An arrangement of one-factors, (not necessarily distinct), is called "s-distance apart", if there are at least "s" other one-factors between the occurences of the same one-factor.

In the proof of Theorem 3.9 of (b), the required sets of P_i's are not given for t = 9. They are listed here:

t = 9: Required sets of P_i's = Sets of P_i's as in the case of t = 8 and $\{P_1, P_6, P_7\}$.

Obtain same P_i's from the 1st to the 8th copy of K_{2n} as in the case of t = 8 and from the 9th copy obtain $\{P_1, P_6, P_7\}$.

□

Please note that Lemmas 4.1 and 4.2 of the attached paper (a) are true for simple BIBDs. The word "simple" is missing in the statements of these two theorems.

We use "induction" in the proof of Theorem 4.3. How the induction works in the theorem is shown below. Similar arguments can be given at other places in the thesis, where we use induction.

The necessary conditions require that $v \equiv 0, 1 \pmod 3$. We have shown that simple BIBDs exist for smaller values of v. Now for a larger v, let v = 3t. Then v can be written as 2(3(s-1))+4 or as 2(3s+1)+1 depending on whether t = 2s or 2s+1. Similarly when v = 3t+1, it can be written as 2(3s)+1 or 2(3s)+4. Hence either Lemma 4.1 or Lemma 4.2 gives simple BIBD(v, 3, 2).

□

Block designs without repeated blocks

Dinesh G. Sarvate

1. Introduction

A t-design $S_\lambda(t, k, v)$ is a collection of k-subsets called blocks of a v-set E such that every t-subset of E is contained in exactly λ blocks. An $S_\lambda(t, k, v)$ is called simple if it has no repeated blocks. A Block design can be written as a v x b incidence matrix, where b is the number of blocks in the design, with $(i, j)^{th}$ entry 1 if the element i belongs to the j^{th} block and 0 otherwise.

Hanani [1] has proved that the necessary conditions are sufficient for the existence of $S_\lambda(2, 3, v)$ and $S_\lambda(2, 4, v)$, but the designs have repeated blocks. Van Buggenhaut [10,11] has proved that for the existence of simple $S_\lambda(2, 3, v)$, $\lambda=2$ and $\lambda=3$, the necessary conditions are sufficient.

The present work is motivated by the papers of R.G. Stanton and I.P. Goulden [8] and A.P. Street [9]. Stanton and Goulden[8] provide an elegant proof for the existence of $S_1(2, 3, v)$ based on factorization of complete graphs and Street[9] extends the result for $\lambda = 2$ and 3 by giving recursive constructions for simple and irreducible $S_2(2, 3, v)$ and

$S_3(2,3,v)$ for all possible values of v (irreducible means not consisting of unions of smaller designs). Recently Sarvate[5] has applied this construction to obtain equi-neighboured designs. We give straightforward recursive constructions for simple $S_\lambda(2,3,v)$ for λ = 2,4,5 and 6 depending on the graph factorization of Stanton and Goulden [8]. Our proof for the case λ =2 is slightly different from Street [9] and similar to the proof for the case λ = 3 in Sarvate[5]. The results of this paper are used in Sarvate[6] to prove that all simple BIBDs with block size 3 exist.

In what follows I_n denotes the identity matrix of order n and $J_{m,n}$ denotes the m x n matrix of all entries 1. We use both the symbols $S_\lambda(2,k,v)$ and BIBD(v,k,λ) to denote the balanced incomplete block design with the parameters v,k,λ .

2. Some observations:

Recently Lu [4] has shown that the maximum number (v-2) of pairwise disjoint $S_1(2,3,v)$ can be attained for v > 7 and v ≡1,3 (mod 6), except possibly for v = 141, 283, 501, 789, 1501 and 2365. However for simple systems and small values of λ, the method given by Stanton and Goulden[8] and Street[9] is preferable. As a consequence of Lu's result we get:

Theorem 2.1: The necessary conditions are sufficient for the existence of simple $S_\lambda(2,3,v)$ for v>7, $\lambda \leq v-2$, v ≡1,3 (mod 6) and except possibly for v = 141, 283, 501, 789, 1501, 2365.

The study of simple block designs can be useful to prove the existence of other combinatorial structures , e.g. in de Launey ,Sarvate and Seberry [3] it was easy to prove that a generalised Bhaskar Rao design (GBRD) over Z_4, for v=15, exists, by using a simple $S_4(2,3,15)$. We

observe that the nonexistence result for a simple $S_2(2,k,v)$ leads to a nonexistence result for GBRD over Z_2 for $k \geq 3$.

The existence results of de Launey and Seberry [2], section 4.1, give the following results for block size 4.

Theorem 2.2 : (i) Let $v \equiv 1 \pmod 6$ be a prime power. Then there exists a simple $S_2(2,4,v)$.

(ii) Simple $S_2(2,4,v)$ exist for $v < 500$, $v \equiv 1 \pmod 6$ except possibly for v in {145,205,265,319,355,415,493}.

A very powerful theorem of Stanton and Collens [7, page 136] together with results of Street[9] and Van Buggenhaut [10,11] gives us:

Theorem 2.3 : (i) Simple $S_\lambda(2,3,v)$ exist for $v \equiv 0,1 \pmod 3$ and $\lambda = 2^n \leq v-2$. In other words, the necessary conditions are sufficient for the existence of simple $S_{2^n}(2,3,v)$.

(ii) Simple $S_\lambda(2,3,v)$ exist for $v \equiv 1 \pmod 2$ and $\lambda = 2^n.3 \leq v-2$.

(iii) The existence of simple $S_\lambda(2,3,v)$ implies the existence of simple $S_{2^n.\lambda}(2,3,v)$ for $2^n.\lambda \leq v-2$.

3. Graph factorization:

A complete graph K_n on n vertices consists of all $\binom{n}{2}$ edges. A one-factor of K_{2n} contains n vertex-disjoint edges. A one-factorization of K_{2n} contains 2n-1 one-factors , which are all disjoint. For examples and details please refer to Stanton and Goulden [8].

All the edges of K_{2n} fall into n disjoint classes $P_1, P_2, \ldots, P_n$; where the edge (i,j) is in P_k if and only if $i-j \equiv k \pmod{2n}$. Stanton and Goulden [8] called this splitting the difference partition of K_{2n}. Consider

the triangles (1+i,2+i,4+i) for i= 1,2, ... ,2n. This gives a set of 2n triangles.

Theorem 3.1[8] : The set of 2n triangles contains exactly those edges from P_1, P_2, P_3.

We observe the following:

Theorem 3.2 : Consider the set T of triangles (1+i,1+x+i,1+x+y+i) for i= 1,2, ... ,2n. The set T contains exactly those edges from P_x, P_y, P_{x+y}, where $x+y < n$.

Remark: This is an important observation as we get various sets of triangles to be used in next sections, e.g. P_1, P_2, P_3 and P_1, P_4, P_5 cover 4n triangles { (1+i,2+i,4+i) } and { (1+i,2+i,6+i) }, i =1,2, ... ,2n.

4. The case $\lambda = 2$.

For the recursive constructions, it is sufficient to be able to construct an $S_2(2,3,V)$ from a given $S_2(2,3,v)$ for (i) V = 2v+1 and (ii) V = 2v+4 and to construct $S_2(2,3,v)$ for initial values of v.

The cases V = 2v+1 (v even) and V = 2v+4 (v odd) have been dealt with in Street [9]. We give the proofs for V = 2v+1 (v odd) and V = 2v+4 (v even).

Lemma 4.1: If there exists a BIBD(v,3,2) then it can be embedded into a BIBD(2v+1,3,2).

Proof: The case v even is proved in Street[9]. Let v be odd. Let A_V denote the incidence matrix of the BIBD(V,3,2). For V=2v+1, the structure of the incidence matrix is given in figure 1.

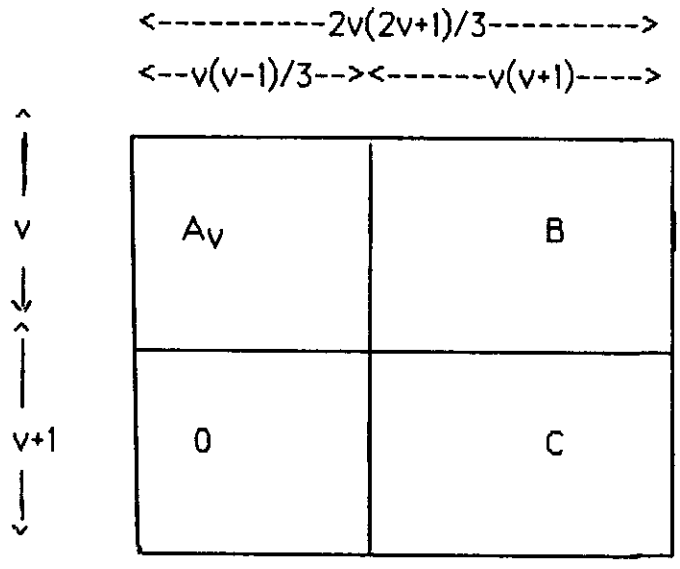


Fig. 1 Incidence matrix A_V of BIBD(2v+1,3,2).

Here $B = I_V \times J_{1,V+1}$ and the columns of C correspond to the one factors of K_{V+1}. In other words if $F_1, F_2, \ldots, F_V$ are the one-factors of K_{V+1} then the columns of C correspond to

$$F_1\ F_2; F_2\ F_3; F_3\ F_4; \ldots ; F_{V-1}\ F_V; F_V\ F_1.$$

Lemma 4.2 : If there exists a BIBD(v,3,2),then it can be embedded into a BIBD(2v+4,3,2).

Proof: The case v odd is done in Street[9]. We consider the case when v is even. The structure of the incidence matrix A_{2V+4} is shown in figure 2.

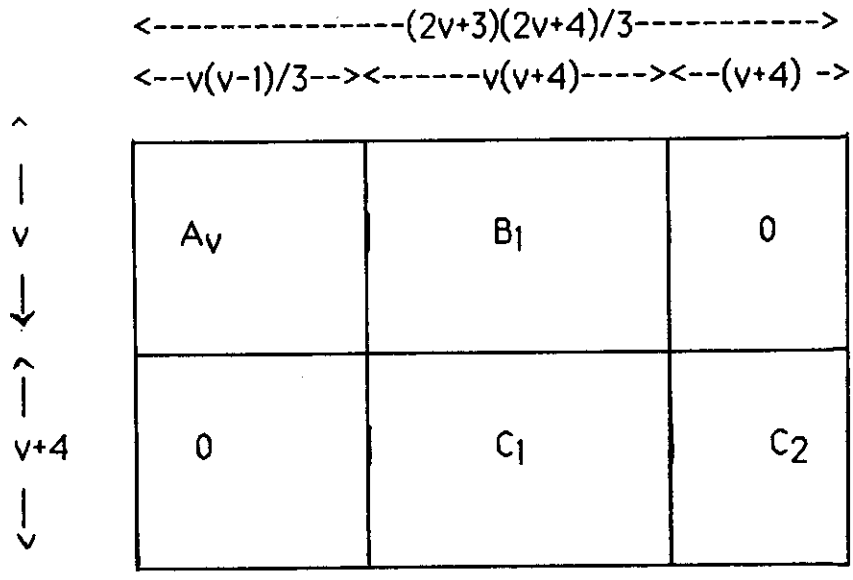


Fig. 2. Incidence matrix A_V of BIBD(2v+4,3,2).

Here $B_1 = I_V \times J_{1,(v+4)}$. The columns of C_2 correspond to the set of (v+4) triangles given by Theorem 3.1 above. The columns of C_1 correspond to the one-factors of $2K_{v+4}$ (i.e. two copies of K_{v+4}), but since the columns of C_2 account for 6 one-factors coming from P_1, P_2 and P_3 these must be excluded once each in considering the columns of C_1. One trivial arrangement of the one-factors is given: Let the one-factors corresponding to the set of (v+4) triangles be $F_1, F_2, \ldots, F_6$ and the remaining one-factors be $F_7, \ldots, F_{v+3}$. Then the columns of C_1 correspond to

$$F_7, \ldots, F_{v+3} ; F_1, \ldots, F_{v+3}.$$

Theorem 4.3 : The necessary conditions are sufficient for the existence of simple BIBD(v,3,2) for $v > 3$.

Proof: We use induction. To start with, we need designs for small values of $v > 3$, viz. for $v=6,7,9,10,12$ which are easy to construct; we have given these designs in Appendix A for the sake of completeness.

5. General results.

The following is proved in Street[9], Van Buggenhaut[11] and Sarvate [5].

Theorem 5.1: The necessary conditions are sufficient for the existence of simple $S_3(2,3,v)$.

We note that the necessary conditions for the existence of $S_2^n(2,3,v)$ are same as for the existence of $S_2(2,3,v)$ and hence as mentioned in Theorem 2.3(i) the necessary conditions are sufficient for the existence of $S_\lambda(2,3,v)$ for $\lambda = 2^n \leq v-2$.

Now we intend to give some direct embedding results:

Lemma 5.2 : If there exists a simple BIBD$(v,3,\lambda)$, $\lambda \leq v-2$, then, for v odd , it can be embedded into a simple BIBD$(2v+1,3,\lambda)$.

Proof: The structure of the incidence matrix A_V, $V = 2v+1$, is given in figure 3.

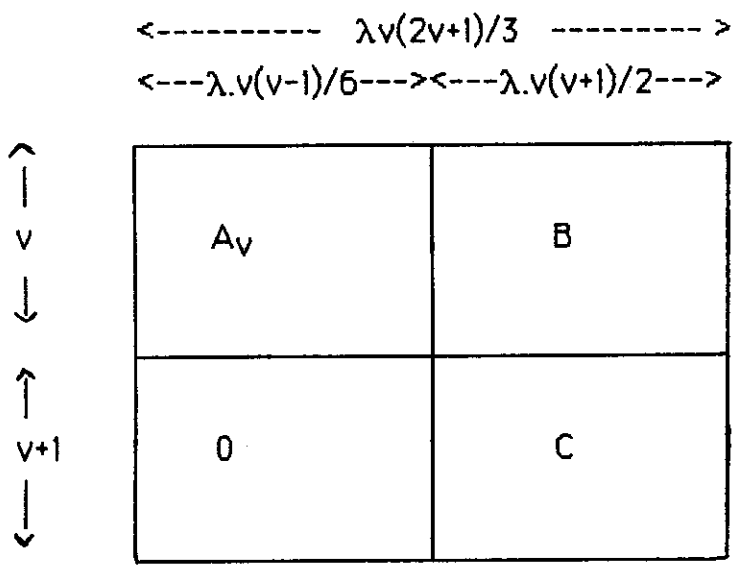


Fig. 3. Incidence matrix A_V of BIBD(2v+1,3,λ).

Here $B = I_V \times J_{1,\lambda(v+1)/2}$. Now as in K_{v+1} we can have at most v(v+1)/2 distinct edges and each column of C will correspond to some edge, $\lambda(v+1) \leq v(v+1)$ and hence $\lambda \leq v$ is a necessary condition. Let the one-factors of K_{v+1} be $F_1, F_2, \ldots, F_v$. Then the columns of C correspond to λ copies of $F_1, F_2, \ldots, F_v$.

Lemma 5.3: If there exists a BIBD(v,3,4), v even, $v \geq 8$, then it can be embedded into a BIBD(2v+4,3,4).

Proof : The structure of the incidence matrix A_{2v+4} of BIBD(2v+4,3,4) is given in figure 4.

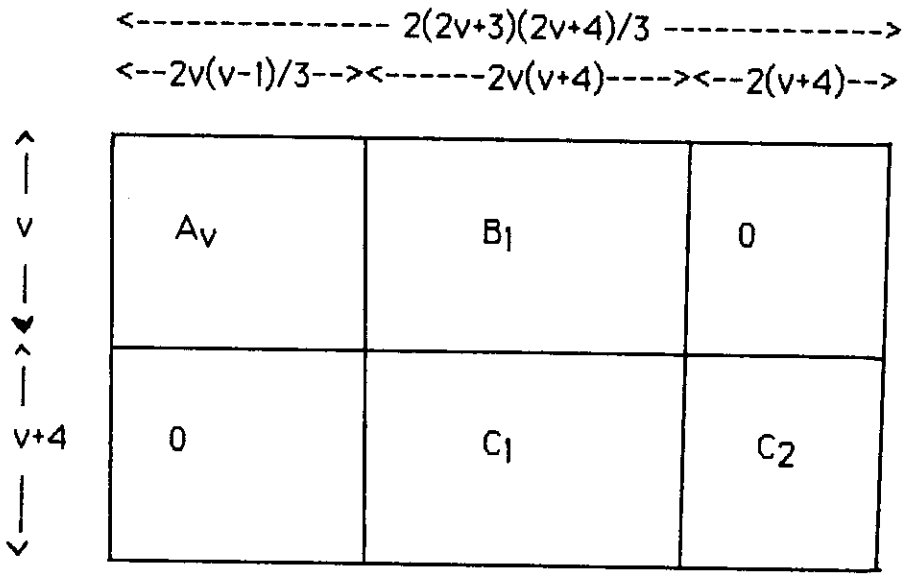


Fig. 4. Incidence matrix A_V of BIBD(2v+4,3,4).

Here $B_1 = I_V \times J_{1,2(v+4)}$. We need to get 2 disjoint sets of (v+4) triangles to fill up the columns of C_2. The remark after Theorem 3.2 guarantees us the existence of such sets for those values of v for which $6 \leq (v+4)/2$ i.e. for $v \geq 8$. Let F_i's denote the one-factors of $K_{(v+4)}$. An arrangement for the columns of C_1 corresponds to :

$F_7, \ldots, F_{v+3} ; F_1, \ldots, F_{v+3} ; F_3, F_4, F_5, F_6, F_{11}, \ldots, F_{v+3} ; F_1, \ldots, F_{v+3}$.

In other words, arrange the one-factors of the required P_i's in the following order:

$P_4, P_5, \ldots, P_{(v+4)/2} ; P_1, \ldots, P_{(v+4)/2} ; P_2, P_3, P_6, \ldots, P_{(v+4)/2} ; P_1, \ldots, P_{(v+4)/2}$.

6. The case λ=5.

As a corollary to Lemma 5.2 we have:

Lemma 6.1: If there exists a BIBD(v,3,5), then it can be embedded into a BIBD(2v+1,3,5).

Lemma 6.2: If there exists a BIBD(v,3,5) then it can be embedded into a BIBD(2v+7,3,5) for $v \geq 23$.

Proof: The structure of the incidence matrix of BIBD(2v+7,3,5) is given in figure 5.

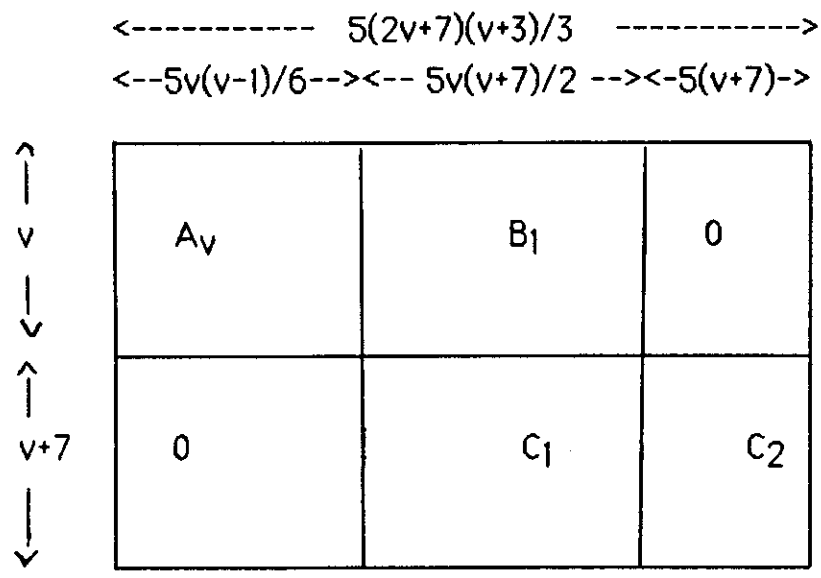


Fig. 5. Incidence matrix A_V of BIBD(2v+7,3,5).

Here $B_1 = I_V \times J_{1,5(v+7)/2}$. We take five copies of $K_{(v+7)}$. If $v \geq 23$ i.e. $v+7 \geq 30$, then we can use $P_1, P_2, \ldots, P_{15}$ to get 5 disjoint sets of v+7 distinct triangles viz. the triangles $\{1+i,2+i,14+i\}$, $\{1+i,3+i,9+i\}$, $\{1+i,4+i,11+i\}$, $\{1+i,5+i,16+i\}$ and $\{1+i,6+i,15+i\}$, $i = 1, \ldots, v+7$, from P_1, P_{12}, P_{13} ; P_2, P_6, P_8; P_3, P_7, P_{10} ; P_4, P_{11}, P_{15} and P_5, P_9, P_{14}. We use these triangles to form the columns of C_2. The columns of C_1

correspond to one copy of the one-factors from P_{16}, ... ,$P_{(v+7)/2}$ followed by the four copies of the one-factors of K_{v+7}.

We observe that the blocks corresponding to the columns of C_2 do not intersect in more than one treatment. If we allow them to have at most one pair of treatments in common then we get the following result.

Lemma 6.3: If there exists a BIBD(v,3,5) then it can be embedded into a BIBD(2v+7,3,5) for v≥ 9.

Proof: We take the triangles obtained from P_1,P_2,P_3; P_1,P_3,P_4; P_1,P_4,P_5; P_2,P_3,P_5 and P_2,P_4,P_6 viz. {1+i,2+i,4+i}, {1+i,2+i,5+i}, {1+i,2+i,6+i}, {1+i,3+i,5+i} and {1+i,3+i,7+i}, i = 1, ... ,v+7, as the columns of C_2.

The columns of C_1 correspond to the two copies of the one factors from P_1, P_2, P_3 and P_4, three copies of the one-factors from P_5, and four copies of the one-factors from P_6 and five copies of the one-factors from the remaining P_i's. If $F_{1,x}$, $F_{2,x}$ are the one-factors obtained from P_x for x odd and x < v+7 then, " $F_{1,7}$,$F_{2,7}$,F_{15}, ... ,F_{v+6} ; F_1, ... ,F_{v+6} ; $F_{1,5}$,$F_{2,5}$,F_{11}, ... ,F_{v+6} ; F_1, ... ,F_{v+6} ; F_{11}, ... ,F_{v+6} ", is an arrangement for the blocks of C_1.

Lemma 6.4: If there exists a BIBD(v,3,5), v ≡ 3 (mod 6),then it can be embedded into a BIBD(2v+3,3,5).

Proof: The structure of the incidence matrix A_V, for $V = 2v+3$,of the BIBD(2v+3,3,5) is given in Figure 6.

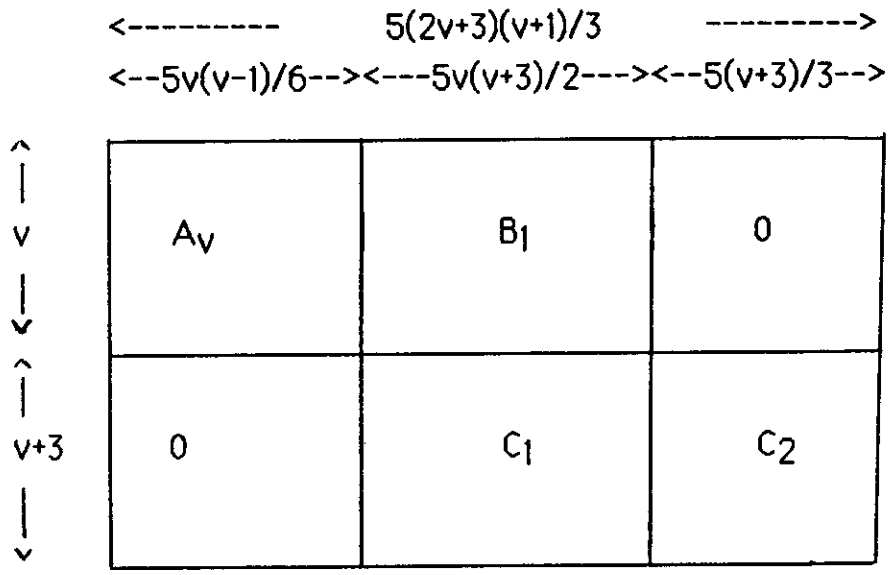


Fig. 6. Incidence matrix A_V of BIBD(2v+3,3,5).

We observe that we need ten one-factors to form 5(v+3)/3 triangles as 6 one-factors give (v+3) triangles. Let v+3 be equal to 6s. Form the 2s blocks of P_{2s} viz. {a,a+2s,a+4s}, a =1,2, ... ,2s :

1	2	3	.....	2s
2s+1	.....		.....	4s
4s+1	.....		.....	6s

Take any s blocks, B_1, B_2, ... ,B_s. Now construct 6s blocks of the form {a,a+s,a+2s}; a=1,2, ... , 6s. Select 3s blocks from these 6s blocks such that they do not have any pair common with any of the B_i's ; these blocks together with 6s' blocks from $\{P_1, P_2, P_3\}$ correspond to the columns of C_2. The remaining 5v factors of the 5 copies of K_{v+3} count for the columns of C_1 (5v=5(v+2)-10).

For example, if we take {a,a+2s,a+4s}, for a = 1,2 , ... , s, as our s blocks B_1 , ... , B_s then we consider the following as our next 3s blocks:

{a,a+s,a+2s} a= s+1, ... , 2s
{a,a+s,a+2s} a=3s+1, ... , 4s
{a,a+s,a+2s} a=5s+1, ... , 6s.

The columns of C_1 can be obtained by writing the one-factors of P_i's except P_1,P_2,P_3,P_{2s} followed by the four copies of the one-factors of K_{v+3}.

Theorem 6.5: The necessary conditions are sufficient for the existence of simple BIBD(v,3,5), v ≥ 7.

Proof: We use induction and lemmas 6.1, 6.2 and 6.3. To start the induction we have given simple BIBD(v,3,5) for small values of v ,viz. v = 7,9,13 and 21 in appendix B.

7. The case λ=6.

For λ = 6 there is no condition on v except v ≥ 8. For v odd Theorem 2.3 (ii) gives the existence of simple BIBD(v,3,6). For v even we have following lemmas:

Lemma 7.1: If there exists a BIBD(v,3,6) then it can be embedded into a BIBD(2v+2,3,6). v ≥ 8.

Proof : The structure of the incidence matrix A_{2v+2} of BIBD(2v+2,3,6) is given in figure 7.

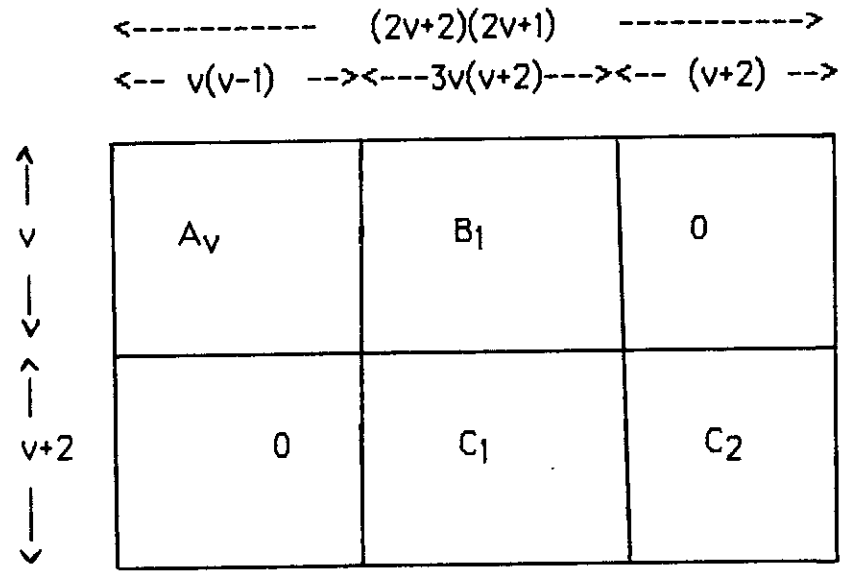


Fig. 7. Incidence matrix A_V of BIBD(2v+2,3,6).

Here $B_1 = I_V \times J_{1,3(v+2)}$ and columns of C_2 correspond to the v+2 triangles obtained from P_1, P_2, P_3 and the columns of C_1 correspond to the one-factors of P_4, ... ,$P_{(v+2)/2}$ followed by five copies of the one-factors of P_1, ... , $P_{(v+2)/2}$.

Lemma 7.2 : If there exists a BIBD(v,3,6) and $v \neq 10$ then it can be embedded into a BIBD(2v+4,3,6) .

Proof: The structure of the incidence matrix A_V of the BIBD(2v+4,3,6) is given in figure 8.

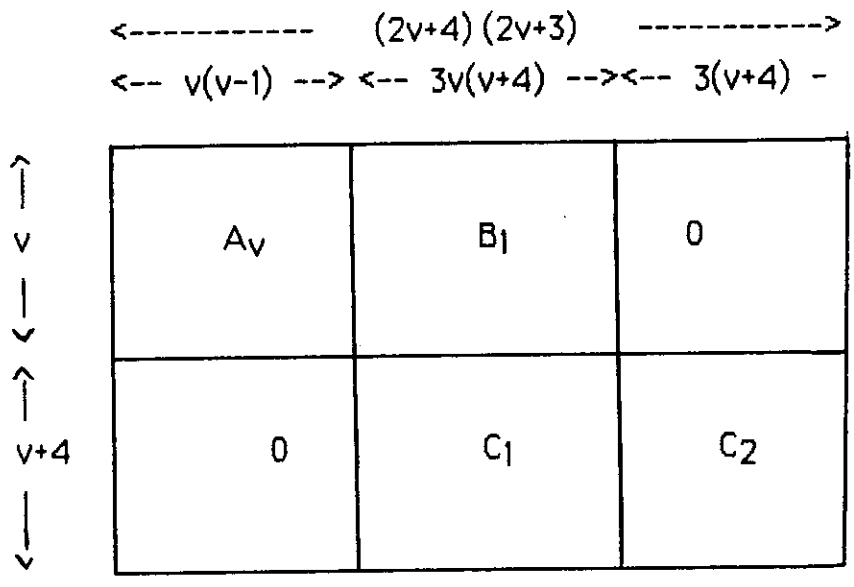


Fig. 8. Incidence matrix A_V of BIBD(2v+4,3,6).

Here $B_1 = I_V \times J_{1,3(v+4)}$. The columns of C_2 correspond to the triangles obtained from P_1,P_2,P_3; P_1,P_3,P_4; P_2,P_4,P_6; when $v \geq 12$ and P_1,P_2,P_3; P_1,P_3,P_4; P_2,P_3,P_5; when $v = 8$. The columns of C_1 correspond to the one-factors obtained from P_i's as follows:

(i) $v = 8$:

P_6 ; P_1,P_2,P_4,P_5,P_6 ; P_1,P_3,P_4,P_5,P_6 ; $P_1, \ldots ,P_6$; $P_2, \ldots ,P_6$; P_1,P_2,P_4,P_5,P_6.

(ii) $v \geq 12$:

$P_5,P_7, \ldots ,P_{(v+4)/2}$; $P_1, \ldots ,P_{(v+4)/2}$; $P_1, \ldots ,P_{(v+4)/2}$; $P_1, \ldots ,P_{(v+4)/2}$; $P_2, \ldots ,P_{(v+4)/2}$; $P_1,P_5,P_6,P_7, \ldots ,P_{(v+4)/2}$.

Notice that for v = 8, P_2 gives two one-factors [8, Lemma 3] and P_6 provides one one-factor but for v=10 , P_2 does not split into two one-factors. This is a reason why the triangles given in the case for v = 8 can not be used for v = 10. The construction for v ≥ 12 does not work for v = 10 because P_7 is 'special' for v = 10 and we need P_6 to get three one-factors from the pair P_6,P_7.[8, Lemma 4].

Theorem 7.3 : The necessary conditions are sufficient for the existence of simple BIBD(v,3,6).

Proof : We use induction. To start the induction we need simple BIBD(v,3,6) for v= 8,10,12,14,16,20,24 which are given in the Appendix C.

Acknowledgement :

My sincere thanks to Dr. Jennifer Seberry for helpful guidance and encouragement. I am greatful to the referee for many useful suggestions.

References:

[1]. Hanani H., *Balanced incomplete block designs and related designs*, Discrete Math. ,11, 1975, 255-369.

[2]. de Launey W. and Seberry J., *Generalised Bhaskar Rao designs of block size four*, Congressus Numerantium, Vol 41, 1984, 229-294.

[3]. de Launey W. , Sarvate D.G. and Seberry J., *Generalised Bhaskar Rao designs with block size 3 over Z_4* ,Ars Combinatoria 19A(to appear).

[4]. Lu Jia-Xi, *On large sets of disjoint Steiner triple systems vi*, Journal of Combinatorial Theory, Series A ,37,189-192 (1984).

[5]. Sarvate D.G., *A note on equi-neighboured block designs*, Utilitas Mathematica, (to appear).

[6]. Sarvate D.G., *All simple BIBDs with block size 3 exist*, Preprint.

[7]. Stanton R.G. and Collens R.J., *A computer system for research on the family classification of BIBDs* , Colloquio Internazionale Sulle Teorie Combinatorie(Roma 1973) Tomo I, Attidei Convegni Lincei, No. 17, Accad. Naz. Lincei., 1976, 133-169.

[8]. Stanton R.G. and Goulden I.P., *Graph factorization, general triple systems and cyclic triple systems*, Aequationes Mathematicae 22, 1981, 1-28.

[9]. Street A. P., *Some designs with block size three* Combinatorial Mathematics vii, Lecture Notes in Mathematics, 829, (Springer - Verlag , Berlin - Heidelberg - New York), 1980, 224-237.

[10]. Van Buggenhaut J., *On the existence of 2-designs $S_2(2,3,v)$ without repeated blocks*, Discrete Math., 8,1974, 105-109.

[11]. Van Buggenhaut J., *Existence and construction of 2-designs $S_3(2,3,v)$ without repeated blocks*, J. Geom., 4, 1974, 1-10.

Appendix A

Following is the list of **simple BIBD(v,3,2)** required for the proof of Theorem 4.3. For v = 7 and 10 the designs are given in Street [8]. The blocks are written in columns.

v=6.

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

v=9.

1	1	1	1	1	1	1	1	2	2	2	2
2	2	3	3	4	4	5	5	3	3	4	5
6	9	7	8	7	8	6	9	4	9	5	8
2	2	3	3	3	3	4	4	4	5	6	6
6	7	4	5	5	6	5	7	8	7	7	8
7	8	6	7	9	8	6	9	9	8	9	9.

v=12.

1	1	1	1	1	1	1	1	1	1
2	2	3	3	4	4	5	5	6	6
7	8	8	9	9	10	10	11	11	12
1	2	2	2	2	2	2	2	2	2
7	3	3	4	4	5	5	6	6	7
12	11	12	11	12	9	10	9	10	8
3	3	3	3	3	3	3	4	4	4
4	4	5	7	7	8	11	5	6	7
5	6	6	9	10	10	12	7	8	11
4	4	5	5	5	5	6	6	6	7
8	9	6	8	8	9	7	8	9	8
12	10	7	11	12	12	11	10	12	9
7		8		9		10			
10		9		10		11			
12		11		11		12.			

Appendix B.

Simple BIBD(v,3,5) for 7,9,13 and 21.

v=7.

Consider the set of all 3-sets of {1, ... ,v}, it forms a simple BIBD(v,3,v-2).

v=9.

Consider the set of all 3-sets of {1, ... ,9}; it forms a simple BIBD(9,3,7); take out simple BIBD(9,3,2) which is given in Appendix A; we get simple BIBD(9,3,5).

v=13.

Remove simple BIBD(13,3,6), which exists by Theorem 2.3(ii), from the set of all 3-sets of {1, ..., 13}.

v=21.

Let $F_i = \{(x, y) : y - x \equiv i(\text{mod } 12), 1 \le x, y \le 12\}$ for $i = 1, \ldots, 6$. Notice that Fi's are disjoint and F_6 contains only six pairs, viz. {(1, 7), (2, 8), (3, 9), (4, 10), (5, 11), (6, 12)} and other F_i's contain twelve pairs. Let G_1 = { (1, 2), (2, 3), (3, 4), (8, 9), (9, 10), (10, 11), (11, 12), (12, 1), (1, 7), (2, 8), (3, 9), (4, 10)}, G_4 = {(9, 3), (10, 4), (11, 5), (12, 6), (5, 9), (6, 10), (7, 11), (8, 12), (9, 1), (10, 2), (11, 3), (12, 4)}. Let $F_{1,3}$ = {(1, 4), (2, 5), (3, 6), (7, 10), (8, 11), (9, 12)} and $F_{2,3}$ = {(4, 7), (5, 8), (6, 9), (10, 1), (11, 2), (12, 3)}. Let $G_{1,3}$ = {(5, 11), (6, 12), (7, 1), (7, 10), (8, 11), (9, 12)} and $G_{2,3}$ = {(8, 2), (5, 8), (6, 9), (10, 1), (11, 2), (12, 3)}. The following blocks form simple BIBD(21,3,5):

The blocks of a simple BIBD(9,3,5) over {13, 14, ... , 21};

{13, x, y}: (x, y) in G_1, F_2, $F_{1,3}$; {14, x, y}: (x, y) in $F_{2,3}$, G_4, F_5;
{15, x, y}: (x, y) in F_1, F_2, $G_{1,3}$; {16, x, y}: (x, y) in $G_{2,3}$, F_4, F_5;
{17, x, y}: (x, y) in F_1, F_2, F_6 ; {18, x, y}: (x, y) in F_3, F_5, F_6;
{19, x, y}: (x, y) in F_1, F_2, $F_{1,3}$; {20, x, y}: (x, y) in $F_{2,3}$, F_4, F_5;
{21, x, y}: (x, y) in F_4, F_5, F_6 ;
{i, 1+i, 3+i}, i = 1, 2, ... , 12;
{1, 4, 5}, {2, 5, 6}, {3, 6, 7}, {4, 7, 8};
{1, 5, 9}, {2, 6, 10}, {3, 7, 11}, {4, 8, 12}.

Appendix C:

Simple BIBD(v,3,6) for v= 8,10,12,14,16,20 and 24.

v=8

As in Appendix B for v = 7.

v=10.

Remove simple BIBD(10,3,2) from the set of all 3-sets of {1,...,10}.

v=12

Remove simple BIBD(12,3,4), (which exists by Theorem 2.3(i)), from the set of all 3-sets of {1, ... , 12}.

v=14.

1	1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	3	3	3	3
3	4	5	6	7	8	9	10	11	12

1	1	1	1	1	1	1	1	1	1
3	4	4	4	4	4	5	5	5	5
13	14	5	6	7	8	9	10	11	12

1	1	1	1	1	1	1	1	1	1
6	6	6	6	7	7	7	8	8	8
7	8	13	14	9	10	11	12	13	14

1	1	1	1	1	1	1	1	1	2
9	9	9	10	10	11	11	12	13	3
10	11	12	13	14	12	14	13	14	4

2	2	2	2	2	2	2	2	2	2
3	3	3	3	4	4	4	4	5	5
5	6	7	8	9	10	11	12	6	7

2	2	2	2	2	2	2	2	2	2
5	5	6	6	6	7	7	7	8	8
13	14	8	9	10	11	12	13	9	10

2	2	2	2	2	2	2	2	2	2
8	9	9	9	10	10	10	11	11	12
14	11	13	14	11	12	14	12	13	13

2	2	3	3	3	3	3	3	3	3
12	13	4	4	4	4	4	5	5	5
14	14	5	6	7	8	9	10	11	12

3	3	3	3	3	3	3	3	3	3
5	6	6	6	6	7	7	7	8	8
13	7	8	9	14	10	11	12	9	13

3	3	3	3	3	3	3	3	3	3
8	9	9	10	10	11	11	12	12	13
14	10	11	12	14	13	14	13	14	14

4	4	4	4	4	4	4	4	4	4
5	5	5	5	6	6	6	6	7	7
11	12	13	14	7	8	9	10	11	13

4	4	4	4	4	4	4	4	4	4
7	8	8	8	9	9	10	10	10	11
14	10	11	12	13	14	11	12	14	13

4	4	4	5	5	5	5	5	5	5
12	12	13	6	6	6	6	6	7	7
9	13	14	7	8	9	10	11	8	12

5	5	5	5	5	5	5	5	5	5
7	7	8	8	8	8	9	9	9	10
13	14	9	10	13	14	10	11	12	13

5	5	6	6	6	6	6	6	6	6
11	12	7	7	8	9	9	10	10	10
14	14	11	12	13	12	14	11	12	13

6	6	6	6	6	6	7	7	7	7
11	11	11	12	12	13	8	8	8	8
12	13	14	13	14	14	9	10	12	13

7	7	7	7	7	7	7	7	8	8
8	9	9	9	9	10	10	12	9	9
14	10	11	13	14	13	14	14	11	12

8	8	8	8	8	9	9	9	9	10	10	11
10	10	11	11	11	10	10	12	13	11	11	12
11	12	12	13	14	13	14	13	14	12	13	14.

v=16

Remove simple BIBD(16,3,8), which exists by Theorem 2.3(i), from the set of all 3-sets of {1, ..., 16}.

v=20

Apply Lemma 7.2.

v=24

Simple BIBD(24,3,16) exists by Theorem 2.3(i); remove it from the set of all 3-sets of {1, ..., 24}.

All simple BIBDs with block size 3 exist

Dinesh G. Sarvate

1. Introduction

A balanced incomplete block design BIBD(v,k,λ) is an arrangement of v points into sets of size k (k-sets) such that each pair of points occurs λ times. We call a BIBD *simple* if it has no repeated blocks.

It is well known that the necessary conditions are sufficient for the existence of BIBDs with block size 3; for a list of references the reader is referred to Doyen and Rosa [2]. A number of authors, including Lindner and Rosa [5], Lu [7], Rosa [8], Schreiber [12] and Teirlinck [16], have discussed the existence of large sets (partition of the complete design into copies of block designs with specified λ). Their results immediately give simple designs(designs without repeated blocks). A number of authors, including Lindner and Rosa [6], Rosa [9] and the references therein, have studied BIBDs having a prescribed number of triples in common. The present note gives an elementary

proof to show that the necessary conditions are sufficient for the existence of simple BIBDs with block size 3. The known results about the existence of simple BIBDs include the existence of (i) simple BIBD$(v,3,\lambda)$ for $\lambda = 2$ and $\lambda = 3$ (Street [15], Van Buggenhaut [17, 18]), for $\lambda = 6$ (Sarvate [11]), (ii) simple cyclic 3-designs for $v \equiv 2 \pmod 4$ (Kohler [4]) and (iii) simple BIBD(v,k,λ) implies existence of simple BIBD$(v,k,2^n\lambda)$ for $2^n\lambda$ less than or equal to $\binom{v-2}{k-2}$ (Stanton and Collens [13]). In the next section we will show that the known results for block size 3 are sufficient to prove that all simple BIBDs with block size 3 exist.

The study of simple block designs can be useful in proving the existence of other combinatorial structures, e.g. in de Launey, Sarvate and Seberry [1] the existence of a generalized Bhaskar Rao design over Z_4 for $v = 15$ was easily proved by using a simple BIBD$(15,3,4)$. Another application of simple designs is demonstrated in Sarvate [10] to prove the existence of equi-neighboured designs with block size 3.

This note was motivated by the papers of Stanton and Goulden [14] and Street [15]. Stanton and Goulden gave an interesting proof of the existence of BIBD$(v,3,1)$ by using embedding theorems based on a graph factorization. Street extended their result to obtain irreducible (not consisting of smaller designs) and simple BIBD$(v,3,\lambda)$ for $\lambda = 2$ and 3. We give some general embedding theorems on a similar line.

2. The result

We observe that, in general, we cannot apply Hanani-Wilson theory of pairwise balanced designs to obtain simple BIBDs but if we can construct appropriate small generating sets in certain cases, for example, when $k = 4$ and $\lambda = 2$, the theory can be very useful.

We first restate some results of Hanani for simple designs. For the notation, the reader is referred to Hanani [3].

Lemma 2.1: *If* $n \in GD(S,1,R)$, $mR \subseteq$ *simple* $B(k,\lambda)$ *and* $mS \subseteq$ *simple* $GD(k,\lambda,m)$, *then* $mn \in$ *simple* $B(k,\lambda)$.

Lemma 2.2: *If* $v \in$ *simple* $B(K,\lambda)$ *such that for any two blocks* B_1 *and* B_2 *of* $B(K,\lambda)$, $|B_1 \cap B_2| < k$, *and for each* k_i *in* K *there exists a simple* $BIBD(k_i,k,1)$, *then a simple* $BIBD(v,k,\lambda)$ *exists.*

Note that for $\lambda = 1$ and for any value of μ we have

Corollary 2.3: *If* $v \in B(K,1)$ *and, for each* k_i *in* K, *there exists a simple* $BIBD(k_i,k,\mu)$, *then a simple* $BIBD(v,k,\mu)$ *exists.*

For easy reference, we give two observations:

Lemma 2.4: (i) *If a simple* $BIBD(v,k,\lambda)$ *exists, then a simple* $BIBD\left(v,k,\binom{v-2}{k-2}-\lambda\right)$ *exists.* (Formed by taking complement of the block set).

(ii) *If a simple* $BIBD(w,k,\lambda)$ *exists, then a simple* $BIBD(w,w-k,b-2r+\lambda)$ *exists, where* b *is the number of blocks and* r *is the replication number of* $BIBD(w,k,\lambda)$. (Formed by taking complement of the blocks with respect to the point set).

As mentioned in the introduction, the known results on the existence of simple BIBDs with block size three are used here to prove:

Theorem 2.5: *The necessary conditions are sufficient for the existence of simple* BIBDs *with block size* 3.

The proof depends heavily on the following theorem of R.G. Stanton and R.J. Collens [13]:

Theorem 2.6: *If* D *is a design without repeated blocks and if* $\lambda \leq \binom{v-2}{k-2}/2$, *then it is possible to choose a permutation* P *of* $\{1,2,\cdots,v\}$ *such that* $D \cup PD$ *has no repeated blocks.*

As an obvious corollary, we have

Corollary 2.7: *If a simple* BIBD(v,k,λ) *exists and* $2^n\lambda \le \binom{v-2}{k-2}$, *then a simple* BIBD(v,k,$2^n\lambda$) *exists.*

To introduce the notation, we prove the above corollary. Let D_1 be a simple BIBD(v,k,λ), then

$$D_2 = D_1 \cup P_1 D_1$$

is a simple BIBD(v,k,2λ) for some permutation P_1. In general,

$$D_i = D_{(i-1)} \cup P_{(i-1)} D_{(i-1)}$$

is a simple BIBD(v,k,$2^{i-1}\lambda$), where $D_{(i-1)}$ is a simple BIBD(v,k,$2^{(i-2)}\lambda$) and $P_{(i-1)}$ is a permutation of $\{1,\cdots,v\}$ obtained by using Theorem 2.2. Notice that $P_{(i-1)}D_{(i-1)}$ is also a simple BIBD(v,k,$2^{(i-2)}\lambda$).

Immediately we can prove

Lemma 2.8: *If a simple* BIBD(v,k,λ) *exists, then a simple* BIBD(v,k,λt) *exists for* t *which satisfies the inequality*

$$t \le 2^m \le \binom{v-2}{k-2}/\lambda$$

for some integer m.

Proof. Let $2^{n-1} \le t < 2^n \le \binom{v-2}{k-2}/\lambda$. Then, by Corollary 2.7, there exists a simple BIBD(v,k,$2^n\lambda$) = $D_n = D_{n-1} + P_{n-1}D_{n-1}$. Let the binary representation of $2^n - t$ be $\sum_{i=0}^{n-1} a_i 2^i$. Now, in case $a_i = 1$, remove P_iD_i from D_n. We obtain a simple BIBD(v,k,tλ). □

Corollary 2.9: *For* λ *even, if a simple* BIBD(2λ+2,3,2) *exists, then a simple* BIBD(2λ+2,3,λ) *exists.*

Proof. Let m be such that

$$2^{m-1} \leq \lambda=2s < 2^m \leq 2\lambda .$$

Then, as a simple BIBD(2λ+2,3,2) exists, a simple BIBD(2λ+2,3,2s=λ) also exists. □

Lemma 2.10: *If* λ *divides* $\binom{v-2}{k-2}$ *and a simple* BIBD(v,k,λ) *exists, then for all* t *such that*

$$t \leq \binom{v-2}{k-2}/\lambda ,$$

a simple BIBD(v,k,λt) *exists.*

Proof. If $\binom{v-2}{k-2}/\lambda = 2^m$ for some m, then Lemma 2.8 proves the result. Now let n be such that

$$2^n < \binom{v-2}{k-2}/\lambda < 2^{n+1} .$$

We need to prove that, for t greater than 2^n and less than $\binom{v-2}{k-2}/\lambda$, a simple BIBD(v,k,λt) exists. Observe that

$$\left(\binom{v-2}{k-2}/\lambda\right) - t \leq 2^{n+1} - 2^n = 2^n .$$

Therefore, by Lemma 2.4, D = simple BIBD(v,k,$\binom{v-2}{k-2}$-tλ) exists, hence, taking out the blocks of D from the set of all k-sets of {1,···,v}, we get a simple BIBD(v,k,tλ). □

If a simple BIBD(v,k,λ) exists, then for all $t \leq \binom{v-2}{k-2}/\lambda$, a simple BIBD(v,k,λt) exists except for t such that (i) t is odd and (ii) $t\lambda < \binom{v-2}{k-2} < (t+1)\lambda$. In other words,

Lemma 2.11: *For all* t *such that* $t \leq \binom{v-2}{k-2}/\lambda$, *except possibly for one value of* t, *the existence of a simple* BIBD(v,k,λ) *implies the existence of a simple* BIBD(v,k,λt) *and the exceptional value of* t *satisfies (i) and (ii) given above.*

Proof. If $\binom{v-2}{k-2}/\lambda$ is an integer, Lemmas 2.8 and 2.10 prove the result. If $\binom{v-2}{k-2}/\lambda$ is not an integer, then for integers t and n such that

$$t\lambda \leq 2^n\lambda < \binom{v-2}{k-2} < 2^{n+1}\lambda$$

a simple BIBD(v,k,tλ) exists by Lemma 2.8. We have to prove that for t in $\{2^n+1, 2^n+2, \cdots, 2^n+s\}$, where $(2^n+s)\lambda < \binom{v-2}{k-2} < (2^n+s+1)\lambda$, a simple BIBD(v,k,λt) exists. Now if $t = 2^n+2q$, then, as $2^{n-1}+q < 2^n$ by Lemma 2.8, a simple BIBD(v,k,$(2^{n-1}+q)\lambda$) exists and hence, by Theorem 2.6, a BIBD(v,k,$2(2^{n-1}+q)\lambda=t\lambda$) exists. Observe that in the proof of Lemma 2.8 we have not removed at any stage the initial simple BIBD(v,k,λ) and hence the simple BIBD(v,k,λt) constructed in the Lemma has a simple subdesign BIBD(v,k,λ). By removing it from a simple BIBD(v,k,λt), we get a simple BIBD(v,k,2^n+2q-1), hence we have proved the result for all t in $\{2^n+1, \cdots, 2^n+s\}$ except for $t = 2^n+s$ when s is odd. □

Lemma 2.12: *If a simple* BIBD(v,3,λ) *exists for* $\lambda = 1,2,3,6$, *then for all integers* t *such that*

$$t\lambda \leq (v-2)$$

a simple BIBD(v,3,λt) *exists.*

Proof. In view of Lemmas 2.8, 2.10 and 2.11, it is sufficient to prove that, when t is odd and

$$t\lambda < (v-2) \leq (t+1)\lambda ,$$

a simple BIBD(v,k,tλ) exists.

When $\lambda = 1$, $v \equiv 1,3 \pmod 6$ and Lemma 2.10 implies that we have a simple BIBD(v,3, t) for all $t \leq (v-2)/\lambda$

When $\lambda = 2$ and v is even, $v-2$ is even and we apply Lemma 2.10. If v is odd, then $v \equiv 1,3 \pmod 6$ and so a simple BIBD(v,3,2t) exists.

When $\lambda = 3$, v satisfies $v \equiv 1,3,5 \pmod 6$. If $v \equiv 1,3 \pmod 6$, a simple BIBD(v,3,3t) exists and for $v \equiv 5 \pmod 6$, $v-2 \equiv 0 \pmod 3$ and hence we apply Lemma 2.10.

When $\lambda = 6$, $v \equiv 0,1,2,3,4,5 \pmod 6$. For $v \equiv 0,4 \pmod 6$, 2 divides $(v-2)$ and, as a simple BIBD(v,3,2) exists, a simple BIBD(v,3,6t) exists. When $v \equiv 1,3 \pmod 6$, a simple BIBD(v,3,1) implies the existence of a simple BIBD(v,3,6t). When $v \equiv 5 \pmod 6$, $v-2 \equiv 0 \pmod 3$ and hence, as a simple BIBD(v,3,3) exists, a simple BIBD(v,3,6t) exists. When $v \equiv 2 \pmod 6$, 6 divides $(v-2)$ and hence Lemma 2.10 implies that a simple BIBD(v,3,6t) exists for all t such that $6t \leq (v-2)$. □

Theorem 2.13: *The necessary conditions are sufficient for the existence of a simple* BIBD(v,3,λ).

Proof. The necessary conditions are:

(i) $\lambda \leq (v-2)$;

(ii) (a) if $(\lambda,6) = 1$, then $v \equiv 1,3 \pmod 6$,
(b) if $(\lambda,6) = 2$, then $v \equiv 0,1 \pmod 3$,
(c) if $(\lambda,6) = 3$, then $v \equiv 1 \pmod 2$,
(d) if $(\lambda,6) = 6$, then no condition on v.

Now Lemma 2.12 proves the Theorem. □

3. Graph factorization

In what follows, I_n denotes that the identity matrix of order n and $J_{m,n}$ denotes the $m \times n$ matrix with all entries 1.

A *complete graph* K_n on n vertices consists of all $\binom{n}{2}$ edges. A *one-factor* of K_{2n} contains n vertex-disjoint edges. A *one-factorization* of K_{2n} contains $2n-1$ one-factors, which are all disjoint. For examples and details, the reader is referred to Stanton and Goulden [14].

All the edges of K_{2n} fall into n disjoint classes $P_1, P_2, \cdots, P_n$, where the edge (i,j) is in P_k if and only if $(i-j) \equiv k \pmod{2n}$. Stanton and Goulden called this splitting *the difference partition of* K_{2n}. Consider the triangles $(1+i, 2+i, 4+i)$ for $i = 1, 2, \cdots, 2n$. This gives a set of $2n$ triangles.

Theorem 3.1 [14]: *The above set of* $2n$ *triangles contains exactly the edges from* P_1, P_2, P_3.

Theorem 3.2 [11]: *Consider the set* T *of triangles* $(1+i, 1+x+i, 1+x+y+i)$ *for* $i = 1, 2, \cdots, 2n$. *The set* T *contains exactly the edges from* P_x, P_y, P_{x+y}, *where* $x+y < n$.

Lemma 3.3 [14]: *The pairs in* P_{2x+1} $(2x+1 < n)$ *split into two one-factors.*

Lemma 3.4 [14]: *If* $2x+1 < 2n$, *then* $P_{2x} \cup P_{2x+1}$ *splits into four one-factors.*

Lemma 3.5 [14]: *If* n *is even, then* P_n *is a single one-factor. If* n *is odd, then* $P_{n-1} \cup P_n$ *can be split into three one-factors.*

Theorem 3.6 [14]: *The graph* K_{2n} *may be factored into a set of triangles covering* P_1, P_2, P_3, *and a set of* $2n-7$ *one-factors covering the other* P_i*'s.*

Suppose X is a subset of $\{P_1, \cdots, P_n\}$, by one-factors of $K_{2n}-X$ we mean the one-factors of K_{2n} except the one-factors obtained from P_i's in X. If X is a singleton $\{P_i\}$, then we write $K_{2n}-X$ as $K_{2n}-P_i$. We assume hereafter that the one-factors of K_{2n} are arranged

in some fixed order and when we say that "let X_i be the one-factors of i^{th} copy of K_{2n}", we mean that the one-factors are arranged according to the same fixed order. Similarly, the one-factors of $K_{2n}-P_i$ are arranged in the same fixed order except that one-factors obtained from the P_i are removed.

Theorem 3.7: *For* t *such that* $t \neq 4,6$ *and* $1 < t < (n-1)$, t *copies of the graph* K_{2n} *may be factored into* t *disjoint sets of* $2n$ *triangles covering* (P_1,P_{1+i},P_{2+i}), $i = 1,2,\cdots,t-1$, *and* (P_2,P_4,P_6) *and* $t(2n-7)$ *one-factors, and for all* t, $1 < t < n-1$, $(t+1)$ *copies of the graph* K_{2n} *may be factored into* t *disjoint sets of* m *triangles and* $t(2n-7) + (2n-1)$ *one-factors.*

Proof. For $t \neq 4,6$, obtain P_1,P_{2i},P_{2i+1} from the $(2i-1)^{th}$ and $(2i)^{th}$ copies of K_{2n} for $i = 1,\cdots,(t-1)/2$ and P_4,P_6,P_{t+1} from the t^{th} copy of K_{2n} when t is odd and $\{P_1,P_{2i},P_{2i+1}\}$ from the $(2i-1)^{th}$ and $(2i)$th copies of K_{2n} for $i = 1,\cdots,(t-2)/2$; $\{P_1,P_t,P_{t+1}\}$ from the $(t-1)^{th}$ copy of K_{2n} and $\{P_4,P_6,P_t\}$ from the t^{th} copy of K_{2n} when t is even. Notice that the P_i's form $\{P_1,P_{1+i},P_{2+i}\}$ and $\{P_2,P_4,P_6\}$, $i = 1,2,\cdots,t-1$. Theorem 3.5 gives the required set of triangles.

As in the proof of Theorem 3.2 of Stanton and Goulden [14], we get $2(2n-7)$ one-factors from the $(2i-1)^{th}$ and $(2i)^{th}$ copies of K_{2n}. When t is even, the $(t-1)^{th}$ copy of K_{2n} gives $(2n-7)$ one-factors. Observe that for distinct even numbers (therefore we have $t \neq 4,6$) a,b,c if we use Lemmas 3.3, 3.4 and 3.5 on $P_1,(P_2 \cup P_3),\cdots,P_{a+1},(P_{a+2} \cup P_{a+3})$, $\cdots,P_{b+1},(P_{b+2} \cup P_{b+3}),\cdots,P_{c+1},(P_{c+2} \cup P_{c+3}),\cdots,P_{n-2} \cup P_{n-1}$ {or $P_{n-3} \cup P_{n-2}$ when n is odd} we get $4\left(\left((n-2)/2\right)-3\right)+8 = 2n-8$, {$(2n-10)$, when n is odd} one-factors. Now, as in Theorem 3.2 of [14], we get $(2n-7)$ one-factors from $\{P_1,\cdots,P_n\} - \{P_a,P_b,P_c\}$, therefore, from the t^{th} copy of K_{2n}, we get $(2n-7)$ one-factors. For $t = 4,6$, we take the one-factors of $K_{2n} - \{P_4,P_6\}$ from the t^{th} copy and the one-factors of $K_{2n} - \{P_t\}$ from the $(t+1)^{th}$ copy. □

Definition: An arrangement of one-factors is called *s-distance apart*, if between any pair of the same one-factor there are at least s other one-factors.

For example, if $F_1,\cdots,F_{2n-1};F_1,\cdots,F_{2n-1}$ are the one-factors obtained from 2 copies of K_{2n}, then the arrangement is (2n-2)-distance apart.

Lemma 3.8: *Let* X_i *denote the* (2n-7) *one-factors of the* i^{th} *copy of* K_{2n} *obtained according to Theorem 3.7 for* $i = 1,\cdots,t-1$. *Let* Y_i *denote the* (2n-1) *one-factors of* $K_{2n} - P_i$ *and* X *denote all the* (2n-1) *one-factors of* K_{2n}, *then the arrangement*

$$Y_4Y_6Y_jXX_1XX_2\cdots XX_{t-1},$$

where $j = t$ *when* t *is even and* $j = t+1$ *when* t *is odd, is* (2n-8)*-distance apart.*

The above result can be checked easily. Suppose we have the following arrangement:

$$P_1P_2P_3P_4P_5P_6\cdots P_n;P_4\cdots P_n;P_1P_2P_3P_4\cdots .$$

The minimum distance will be the distance between the one-factors obtained from P_4,P_5. Let F_1,F_2,F_3,F_4 denote the one-factors from P_4,P_5:

$$P_1P_2P_3F_1F_2F_3F_4P_6\cdots P_n;F_1F_2F_3F_4P_6\cdots P_n .$$

Clearly, $P_6,\cdots,P_n$ contribute (2n-11) one-factors and F_j's contribute 3 one-factors between any pair (F_i,F_i), hence the total distance is (2n-8). □

One disadvantage of Theorem 3.10 is that we have used up to P_{t+1} and the number of P_i's is n. We improve upon the restriction "$t < n-1$" by giving the following theorem:

Theorem 3.9: *For* t, $t < 2n-10$, t *copies of the graph* K_{2n} *may be factored into* t *disjoint sets of* $2n$ *triangles covering* $\{P_1,P_{1+i},P_{2+i}\}$, $i = 1,\cdots,(t+1)/2$; $\{P_2,P_{3+i},P_{5+i}\}$, $i = 1,\cdots,(t-1)/2$; *for* t *odd and* $\{P_1,P_{1+i},P_{2+i}\}$, $i = 1,\cdots,t/2$; $\{P_2,P_{3+i},P_{5+i}\}$, $i = 1,\cdots,t/2$; *for* t *even, and* $t(2n-7)$ *one-factors.*

Proof. For small values of t, no general pattern can be given but we will see that, after $t = 8$, the general pattern will be clear. Obtain the required P_i's in the following manner:

$t = 1$: Required set of P_i's = $\{P_1,P_2,P_3\}$.

We obtain these P_i's from the first copy of K_{2n}.

$t = 2$: Required sets of P_i's = $\{P_1,P_2,P_3\},\{P_2,P_4,P_6\}$.

We obtain from the first copy of K_{2n} the first set $\{P_1,P_2,P_3\}$ and from the second copy of K_{2n} the second set of P_i's.

$t = 3$: Required sets of P_i's = $\{P_1,P_2,P_3\},\{P_2,P_4,P_6\};\{P_1,P_3,P_4\}$.

Obtain from the first copy of K_{2n}, P_1,P_2,P_3,P_4, from the second copy of K_{2n}, P_1,P_2,P_3, and from the third copy of K_{2n}, P_4,P_6.

$t = 4$: Required sets of P_i's = $\{P_1,P_2,P_3\},\{P_2,P_4,P_6\}$; $\{P_1,P_3,P_4\},\{P_2,P_5,P_7\}$.

Obtain from the first two copies of K_{2n} $\{P_1,P_2,P_3\}$; from the third copy of K_{2n} $\{P_2,P_4,P_5\}$ and from the fourth copy $\{P_2,P_4,P_7\}$.

$t = 5$: Required sets of P_i's = sets of P_i's for the case $t = 4$ and $\{P_1,P_4,P_5\}$.

Obtain P_i's as in the case $t = 4$ and from the fifth copy obtain $\{P_1,P_4,P_5\}$.

$t = 6$: Required sets of P_i's = sets of P_i's in the case $t = 5$ and $\{P_2,P_6,P_8\}$.

Obtain P_i's as in the case $t = 5$ and from the sixth copy obtain $\{P_2,P_6,P_8\}$.

$t = 7$: Required sets of P_i's = sets of P_i's as in the case of $t = 6$ and $\{P_1,P_5,P_6\}$.

Obtain P_i's as follows:

From the 1^{st} copy: $P_1P_2P_3P_6$
" " 2^{nd} " : $P_1P_2P_3$
" " 3^{rd} " : $P_1P_4P_5$
" " 4^{th} " : $P_1P_4P_5$
" " 5^{th} " : $P_2P_4P_5$
" " 6^{th} " : $P_2P_6P_8$
" " 7^{th} " : P_6P_7 .

Notice that P_{2i+1} is always taken out with P_{2i} so that we can obtain the required one-factors from K_{2n}.

t = 8: Required sets of P_i's = sets of P_i's as in the case of t = 7 and $\{P_2,P_7,P_9\}$.

Obtain P_i's as in case of t = 7 except from 6^{th} copy of K_{2n}. Obtain from the 6^{th} copy P_2,P_6,P_7 and from 8^{th} copy of K_{2n}, obtain $\{P_2,P_8,P_9\}$. Now, for even t, the pattern is clear, when required set of P_i's is $\{P_2,P_{2s},P_{2s+2}\}$ obtain from 1^{st} to $(t-1)^{th}$ copies of K_{2n} same P_i's as in the case of (t-1) and from the t^{th} copy obtain $\{P_2,P_{2s},P_{2s+2}\}$. When the required set of P_i's is $\{P_2,P_{2s+1},P_{2s+3}\}$ obtain same P_i's from 1^{st} to $(t-1)^{th}$ copies of K_{2n} except $(t-2)^{th}$ copy and from $(t-2)^{th}$ copy instead of $\{P_1,P_{2s},P_{2s+2}\}$, obtain $\{P_1,P_{2s},P_{2s+1}\}$ and from the t^{th} copy obtain $\{P_1,P_{2s+2},P_{2s+3}\}$.

t = 10: t is even.

t = 11: Required sets of P_i's = set of P_i's as in the case t = 10 and $\{P_1,P_7,P_8\}$.

Obtain same P_i's from 2^{nd} to $(t-1)^{th}$ copy of K_{2n}. Notice that, in the case of t = 7 hence for t = 7,8,9,10, from the 1^{st} copy of K_{2n}, we have obtained the set $\{P_1,P_2,P_3,P_6\}$. Now obtain $\{P_1,P_2,P_3,P_8\}$ and from the 11^{th} copy obtain $\{P_1,P_6,P_7\}$. Now the pattern is obvious. If, for odd t, the required set of P_i's is $\{P_1,P_{2s},P_{2s+1}\}$, obtain from t^{th} copy the same set, else the required set is $\{P_1,P_{2s+1},P_{2s+2}\}$. Obtain from the 1^{st} copy of K_{2n} the set $\{P_1,P_2,P_3,P_{2s+2}\}$, from the t^{th} copy $\{P_1,P_{2s},P_{2s+1}\}$ and from other copies obtain same P_i's as in the case of t-1.

□

Lemma 3.10: *Let* K_{6s} *be a complete graph. Then*
(i) $P_s \cup P_{2s}$ *form* 4s *distinct triangles;*
(ii) P_{2s} *form* 2s *distinct triangles.*

Proof. Consider the triangles $\{a,a+s,a+2s\}$, $a = s+1,\cdots 2s;3s+1,\cdots,4s+1;5s+1,\cdots,6s$ and $\{a,a+2s,a+4s\}$ for $a = 1,\cdots,s$. Observe that $\{a,a+s,a+2s\}$ account for all the pairs of P_s and for the pairs $(a,a+2s)$ of P_{2s} except for $a = 1,\cdots,s;2s+1,\cdots,3s;4s+1,\cdots,5s$ and the triangles $\{a,a+2s,a+4s\}$ cover only these pairs.

For (ii), observe that the triangles $\{a,a+2s,a+4s\}$, $a = 1,\cdots,2s$ form the 2s triangles of P_{2s}. □

Lemma 3.11: *Let* X_i, Y_j *be the same as in Lemma 3.8, then the arrangement*

$$Y_4,Y_6,Y_j,Y_{2s},Y_{4s},X_1XX_2XX_3X\cdots X_{t-1}X,$$

where X *has occurred* (2t-4) *times, is* (2n-8) *distance apart.*

The proof is on a similar line as for Lemma 3.8.

4. Embedding theorems

In this section we will give some general recursive constructions. The following theorem is proved in Sarvate [11]:

Theorem 4.1: *If there exists a simple* BIBD(v,3,λ), $\lambda \le v-2$, v *odd, then it can be embedded into a simple* BIBD(2v+1,3,λ).

Theorem 4.2: *A simple* BIBD(v,3,3t) *can be embedded into a simple* BIBD(2v+3,3,3t), *for* $v \ge 3t+4$.

Proof. The case $t = 1$ is proved in [10,15]. We deal with $t > 1$. The structure of the incidence matrix of BIBD(2v+3,3t) is given in Figure 1 where $B_1 = I_v \times J_{1,3t(v+3)/2}$.

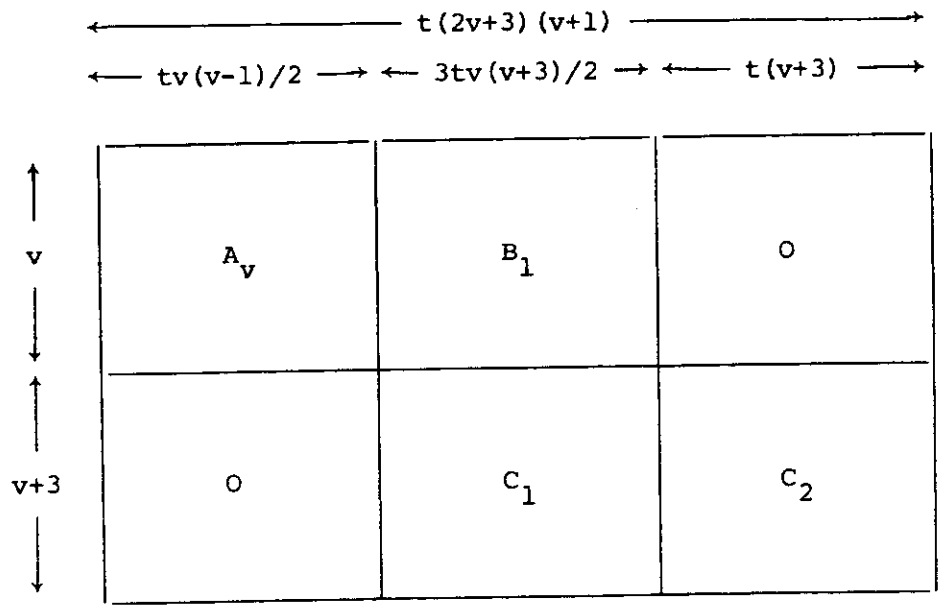


Fig. 1 The incidence matrix A_v of BIBD(V=2v+3,3,λ).

Apply Theorem 3.7 on the first t copies of K_{v+3} (v is odd), and obtain t disjoint sets of $(v+3)$ triangles and use them as columns of C_2. The arrangement given in Lemma 3.8 accounts for C_1. Notice that the arrangement is at least $(3t-1)$ distance apart as $3t \le v-4$ (and hence $3t-1 \le (v+3)-8$). □

Theorem 4.3: *If there exists a simple* BIBD(v,3,λ), $v \equiv 3 \pmod 6$, *then it can be embedded into a simple* BIBD(2v+3,3,λ), $v \ge \lambda+4$.

Proof. For $\lambda \le 6$, see [10,11,15]. For $\lambda \equiv 0 \pmod 3$ Theorem 4.2 gives the result. The structure of the incidence matrix is given in Figure 2, where $B_1 = I_v \times J_{1,\lambda(v+3)/2}$.

Let $\lambda = 3t+i$, $i = 1,2$. Obtain t sets of $(v+3)$ triangles using Theorem 3.9. Let $v+3 = 6s$. Obtain i times $2s$ triangles using Lemma 3.10. These triangles form columns of C_2. Arrangement of the one-factors, similar to Lemma 3.11, gives C_1. Notice that the arrangement is $v+3-8 = v-5 \ge \lambda-1$ distance apart.

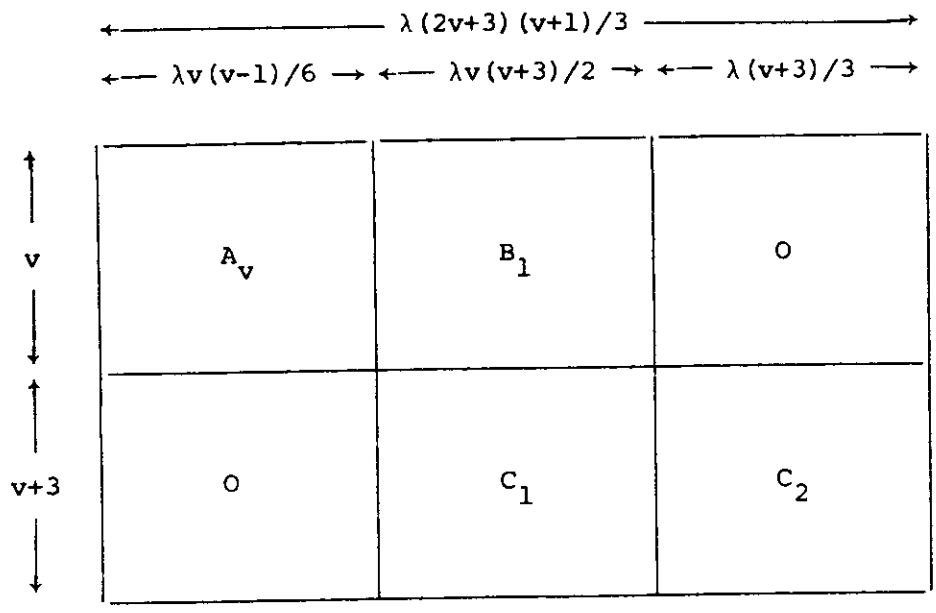


Fig. 2 The incidence matrix A_V of BIBD(V=2v+3,3,λ). □

Theorem 4.4: *If there exists a simple* BIBD(v,3,λ), $\lambda \le v-2$, v *odd, then it can be embedded into a simple* BIBD(2v+7,3,λ).

Proof. Let A_v denote the incidence matrix of the simple BIBD(v,3,λ). For V = 2v+7, the structure of the incidence matrix A_V is given in Figure 3.

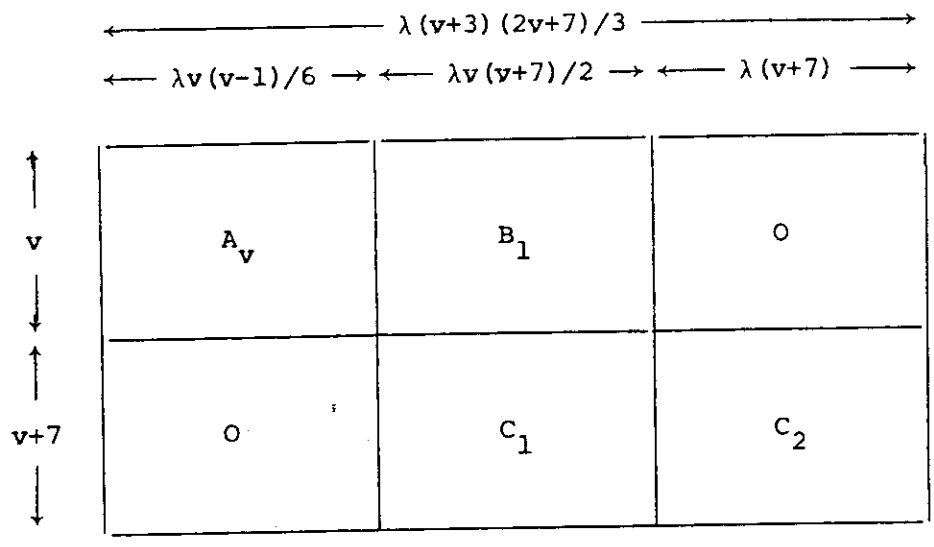


Fig. 3 The incidence matrix A_V of BIBD(V=2v+7,3,λ).

Here $B_1 = I_v \times J_{1,\lambda(v+7)/2}$. Consider λ copies of K_{v+7}. Obtain λ disjoint sets of $(v+7)$ triangles and $\lambda(2n-7)$ one-factors using Theorem 3.7. The columns of C_1 correspond to the arrangement given in Lemma 3.8 and the columns of C_2 correspond to $\lambda(v+7)$ triangles. Notice that $\lambda \leq v-2$ and the arrangement used for C_1 is $(v+7)-8 = (v-1)$ distance apart. □

Similarly we can prove

Theorem 4.5: *A simple* BIBD(v,3,6t), v *even, can be embedded into a simple* BIBD(2v+2,3,6t) *for* $v \geq 6t+5$.

Theorem 4.6: *A simple* BIBD(v,3,6t), v *even, can be embedded into a simple* BIBD(2v+4,3,6t) *for* $v \geq 6t+3$.

Theorem 4.7: *For* t *such that* (t,3) = 1,

(i) a simple BIBD(v,3,2t), $v \equiv 0 \pmod 6$, *can be embedded into a simple* BIBD(2v+6,3,2t);

(ii) a simple BIBD(v,3,2t), $v \equiv 4 \pmod 6$, $v \geq 2t+5$, *can be embedded into a simple* BIBD(2v+2,3,2t).

Notice that if $v \equiv 0 \pmod 6$, then $2v+2 \equiv 2 \pmod 6$, so a simple BIBD(2v+2,3,2t) does not exist. If $v \equiv 4 \pmod 6$, then $2v+2 \equiv 4 \pmod 6$, so a simple BIBD(2v+2,3,2t) exists, but $2v+6 \equiv 2 \pmod 6$, so a simple BIBD(2v+6,3,2t) does not exist.

Acknowledgement:

My sincere thanks to Dr. Jennifer Seberry for helpful guidance and encouragement.

References:

[1] de Launey, W., Sarvate, D.G. and Seberry, J., *Generalised Bhaskar Rao designs with block size 3 over* Z_4, Ars Combinatoria, 19A, (to appear).

[2] Doyen, J. and Rosa, A., *A bibliography and survey of Steiner systems*, Bollettino V.M.J. (4), 7, 1973, 392-419.

[3] Hanani, H., *Balanced incomplete block designs and related designs*, Discrete Mathematics, vol. 11, 1975, 255-361.

[4] Kohler, E., *k difference-cycles and the construction of cyclic t-designs*, Geometrics and Groups, Lecture Notes in Mathematics, 893, Springer-Verlag, 1981, 195-203.

[5] Lindner, C.C. and Rosa, A., *Construction of large sets of almost disjoint Steiner triple systems*, Can. J. Math., vol. 27, no. 2, 1975, 256-260.

[6] Lindner, C.C. and Rosa, A., *Steiner triple system having a prescribed number of triples in common*, Can. J. Math., vol. 27, no. 5, 1975, 1166-1175.

[7] Lu Jia-Xi, *On large sets of disjoint Steiner triple systems, vi*, Journal of Combinatorial Theory (A), 37, 1984, 189-192.

[8] Rosa, A., *A theorem on the maximum number of disjoint Steiner triple systems*, Journal of Combinatorial Theory (A), 18, 1975, 305-312.

[9] Rosa, A., *Intersection properties of Steiner systems*, Annals of Discrete Mathematics, 7, 1980, 115-128.

[10] Sarvate, D.G., *A note on equi-neighboured block designs*, Utilitas Mathematica, (to appear).

[11] Sarvate, D.G., *Block designs without repeated blocks*, Ars Combinatoria, (to appear).

[12] Schreiber, S., *Some balanced complete block designs*, Israel J. Math., vol. 18, 1974, 31-37.

[13] Stanton, R.G. and Collens, R.J., *A computer system for research on the family classification of BIBDs*, Colloquio Internazionale Sulle Teoric Combinatorie, (Roma 1973), Tomo I, Attidei Convegni Lincei, no. 17, Accad. Naz. Lincei, Rome, 1976, 133-169.

[14] Stanton, R.G. and Goulden, I.P., *Graph factorization, general triple systems and cyclic triple systems*, Aequationes Mathematicae, 22, 1981, 1-28.

[15] Street, A.P., *Some designs with block size three*, Combinatorial Mathematics, vii, Lecture Notes in Mathematics, 829, Springer-Verlag, 1980, 224-237.

[16] Teirlinck, L., *On the maximum number of disjoint triple systems*, J. Geometry, vol. 6/2, 1975, 93-96.

[17] Van Buggenhaut, J., *On the existence of 2-designs $S_2(2,3,v)$ without repeated blocks*, Discrete Mathematics, 8, 1974, 105-109.

[18] Van Buggenhaut, J., *Existence and construction of 2-designs $S_3(2,3,v)$ without repeated blocks*, J. Geom., 4, 1974, 1-10.

Chapter Five

Colourable Designs

The work in this chapter was done mainly with Dr. Jennifer Seberry. The exposition owes much to her.

5.1 Introduction

In a recent paper which appears in Chapter 8 of this present thesis, Sarvate and Seberry (1986) introduced a method for encrypting secret messages using crypto designs. These designs are often hard to find, but designs with some relaxed conditions can be used for encryption in a fashion similar to crypto designs. In this chapter we study a class of such crypto designs, which we call colourable designs (CDs). CDs have another important application besides encryption - they can be used to produce new group divisible designs.

The following definitions introduce an area of further research for which almost no constructions and existence results are known.

By an *(s,t)-crypto design* we mean a matrix M(0, a, b, ..., c) of zeros and some message symbols a, b, ..., c such that each s-set of message symbols occurs at least once in the rows and each t-set of message symbols occurs at least once in the columns.

By an *ideal crypto design* we mean a crypto design obtained by assigning (colouring) to each 1 in the incidence matrix of a BIBD (PBIBD) a message symbol so that at least one of the following properties holds:

(i) each t-set occurs at least once, but a minimum number, say C_1, of columns accounts for all the t-sets of the message symbols;

(ii) each s-set occurs at least once, but a minimum number, say R_1, of rows accounts for all the t-sets of the message symbols;

(iii) each s-set and t-set occurs at least once in the rows and columns respectively, but two minimum numbers R and C of rows and columns account for all the s-sets and t-sets of the message symbols respectively.

In a crypto design the number of t-sets per column is equal to $\binom{k}{t}$ and the total number of t-sets is $\binom{c}{t}$, where c is the size of the message symbol set. Therefore we will need at least $\binom{c}{t} / \binom{k}{t}$ columns. Hence

$$\binom{c}{t} / \binom{k}{t} \leq C_1.$$

Naturally $C_1 \leq C$.

Similarly, we can see that

$$\binom{c}{s} / \binom{r}{s} \leq R_1 \leq R.$$

By a *colourable design* we mean a coloured incidence matrix of a BIBD or PBIBD with block size k and replication number r, which satisfies the following properties :

(i) the matrix is coloured with r symbols ;

(ii) all symbols in any row and in any column are different. If the underlying matrix is the incidence matrix of a BIBD(v, b, r, k, λ) we denote the colourable design by CD(v, b, r, k, λ) or by CD(v, k, λ). Similar notation is used for PBIBDs.

Naturally each row of the colourable design will be coloured by all the r symbols.

By an *r-colourable matrix* we mean a matrix with r non-zero entries in each row, which can be coloured by using r symbols, such that all coloured symbols in any row and in any column are different.

Latin squares (see Denes and Keedwell (1974)), graeco-latin designs (see, for example, Preece (1976), Seberry (1979), Street (1981), Sterling

and Wormald (1976) or Youden (1937)) and balanced Room squares (see Wallis, Street and Wallis (1972)) can immediately be used as coloured designs.

Coloured designs are used in Seberry (1987) and Rodger, Sarvate and Seberry (1987) to construct new families of BIBDs and GDDs. A general existence theorem is given in the attached reprint of Rodger, Sarvate and Seberry (1987) in the section 5.2. In the following sections, i.e. in the sections 5.3, 5.4, 5.5 and 5.6, we will give our own constructions as they may be useful in applications to encryption and also because the general existence theorem does not tell us that how to do the colouring.

5.2 Application and a general construction

Attached is a joint paper with C.A. Rodger and J. Seberry, which appeared in the J. Stat. Plan. and Inference. The paper owes its existence especially to J. Seberry. The following existence theorem was independently and almost simultaneously observed by this author and J. Hammer together, and by C.A . Rodger.

Theorem 5.2.1: *Any block design* (V, B) *with point set* V *and set of blocks* B *can be coloured with* R *colours where* R = max (r_v, k_b), *where* r_v *is the number of occurrences of treatment* v *and* k_b *is the number of elements in block* b.

Proof. Theorem 2.1 of the attached paper.

□

The following theorem is due to J. Seberry.

Theorem 5.2.2 : *If there exists a* CD(v, b, r, k, λ), *where* r-1 = q *is a prime power, then there exists a group divisible design*

GDD($v(r-1)^2$, $b(r-1)^2$, $r(r-1)$, $k(r-1)$, $\lambda_1 = r-1$, $\lambda_2 = \lambda$, $m = q^2$, $n = v$).

Proof. Theorem 3.1 of the attached paper.

□

The bulk of the paper is due to mutual discussion and this author produced the tables in the Appendix of the paper.

Colourable designs, new group divisible designs and pairwise balanced designs

C. A. Rodger, D. G. Sarvate, J. Seberry

1. Introduction

For the definitions of a balanced incomplete block design (BIBD), a partially balanced incomplete block design (PBIBD) and a mutually orthogonal Latin square we refer the reader to Raghavarao (1971). A *group divisible design* (GDD) is a BIBD with S being the set of symbols and $B = G \cup X$ being the set of blocks, where G is a partition of S and where each block in X intersects each block in G in at most one point.

In a recent paper Sarvate and Seberry (1986) introduced a method for encrypting secret messages using crypto designs. These designs are often hard to find, but designs with some relaxed conditions can be used for encryption similar to crypto

designs. In this note we study a class of such crypto designs, which we call coloured designs (CD). CD's have an important application besides encryption: they are used to produce new group divisible designs.

A matrix is *x-coloured* if each non-zero entry is replaced with one symbol from a given set of x symbols; it is properly x-coloured if each of the x symbols occurs at most once in each row and at most once in each column. A *coloured* design CD(v, b, r, k, λ) or a CD($v, b, r, k, \lambda_1, \lambda_2, \ldots$) is a properly r-coloured incidence matrix of a BIBD(v, b, r, k, λ) or a PBIBD($v, b, r, k, \lambda_1, \lambda_2, \ldots$) respectively. (This has been called a colourable design elsewhere (Seberry (1987), de Launey and Seberry (1987)).)

Of course each symbol occurs exactly once in each row of a coloured design.

Latin squares (see Denes and Keedwell (1974)), Graeco-Latin designs (see, for example, Preece (1976), Seberry (1979), Street (1981), Stirling and Wormald (1976)) and balanced Room squares (see Wallis, Street and Wallis (1972)) can immediately be used as coloured designs.

2. Main theorem

Theorem 2.1. *The incidence matrix of any block design, (V, B), with treatment set V and set of blocks B can be coloured with R colours where*

$$R = \max_{v \in V,\, b \in B} (r_v, k_b)$$

with r_v the number of occurrences of treatment v and k_b the number of elements in block b.

Proof. Form a bipartite graph, G, with vertex sets V and B. Join $i \in V$ to $j \in B$ if and only if $i \in j$. Then, since each symbol i occurs in $r_i \leq R$ blocks, each vertex i has degree r_i and since each block contains $k_j \leq R$ symbols, each vertex j has degree k_j. We can edge-colour G with $\Delta(G) = R$ colours. This edge-colouring induces a colouring of the design of the required form (that is, colour symbol i in block j with colour c iff the edge $\{i, j\}$ is coloured with c).

Corollary 2.2. *If there exists a* BIBD(v, b, r, k, λ) *or a* PBIBD($v, b, r, k, \lambda_1, \lambda_2, \ldots$), *then there exists a* CD(v, b, r, k, λ) *or a* CD($v, b, r, k, \lambda_1, \lambda_2, \ldots$) *respectively.*

Coloured designs are used in Seberry (1987b), and de Launey and Seberry (1987) to construct new families of BIBD's and GDD's.

3. Main application

The matrices described in the following proof can also be constructed from

generalized Hadamard matrices and latin squares but here we use a simpler formulation.

Theorem 3.1. *If there exists a* CD(v, b, r, k, λ) *where* $r-1=q$ *is a prime power, then there exists a group divisible design*

$$\mathrm{GDD}(vq^2, bq^2, (q+1)q, kq, \lambda_1=q, \lambda_2=\lambda, m=q^2, n=v).$$

Remark. We can apply the same technique as in the following proof for coloured PBIBD's to obtain families of PBIBD's with more associate classes.

Proof. Take the $q+1$ matrices of order q^2, $R_0, \ldots, R_q$, defined by Seberry (1986), (and which have appeared earlier in many forms; for example see Wallis (1971) and Glynn (1978)), which satisfy

$$\sum_{i=0}^{q} R_i R_i^{\mathrm{T}} = q^2 I + q^J, \qquad R_i R_j^{\mathrm{T}} = J, \qquad R_i J = qJ.$$

These matrices exist whenever q is a prime power. Now replace symbol i of the CD by R_i and each 0 by the zero matrix of order q^2 to obtain the result.

Example 1. Consider the CD(9, 12, 4, 3, 1) given in Table 1.

Table 1

a *b* *c*	*b* *c* *d*	*c* *a* *a*	*d* *d* *b*
c *d* *a*	*a* *b* *c*	*b* *c* *d*	*d* *a* *b*
c *a* *d*	*d* *d* *a*	*b* *b* *c*	*a* *c* *b*

Here $r-1=3=q$ (for notation, see Wallis (1971) and Seberry (1987b)), and hence we can define

$$T=\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad J_3=\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix},$$

and R_0, R_1, R_2, R_3 by

$$R_0=\begin{bmatrix} I & I & I \\ I & I & I \\ I & I & I \end{bmatrix}, \qquad R_1=\begin{bmatrix} I & T & T^2 \\ T^2 & I & T \\ T & T^2 & I \end{bmatrix},$$

$$R_2=\begin{bmatrix} I & T^2 & T \\ T & I & T^2 \\ T^2 & T & I \end{bmatrix}, \qquad R_3=\begin{bmatrix} J_3 & 0 & 0 \\ 0 & J_3 & 0 \\ 0 & 0 & J_3 \end{bmatrix}.$$

Now we replace a by R_0, b by R_1, c by R_2 and d by R_3 in the CD(9, 12, 4, 3, 1) to obtain the GDD(81, 108, 12, 9, 3, 1, 9, 9) given in Table 2, which is not listed in Clatworthy (1973) (Clatworthy lists GDD's with $r \le 10$).

Table 2

R_0 R_1 R_2	R_1 R_2 R_3	R_2 R_0 R_0	R_3 R_3 R_1
R_2 R_3 R_0	R_0 R_1 R_2	R_1 R_2 R_3	R_3 R_0 R_1
R_2 R_0 R_3	R_3 R_3 R_0	R_1 R_1 R_2	R_0 R_2 R_1

Corollary 3.2. (i) *If $q=3v-4\ge 5$ is a prime power then there exists a*

$$\mathrm{GDD}(q^2(q+4)/3,\ q^2(q+1)(q+4)/9,\ q(q+1),\ 3q,\ \lambda_1=q,\ \lambda_2=6,\ m=q^2,\ n=(q+4)/3).$$

(ii) *If $q=3t-1$ is a prime power then there exists a*

$$\mathrm{GDD}((2t+1)(3t-1)^2,\ t(2t+1)(3t-1)^2,\ 3t(3t-1),\ 3(3t-1),\ \lambda_1=3t-1,$$
$$\lambda_2=3,\ m=(3t-1)^2,\ n=2t+1).$$

(iii) *If $q=\lambda v-\lambda-1$ is a prime power then there exists a*

$$\mathrm{GDD}(vq^2,\ \lambda v(v-1)q^2/2,\ q(q+1),\ 2q,\ \lambda_1=q,\ \lambda_2=\lambda,\ m=q^2,\ n=v).$$

(iv) *If $q=(\lambda v-\lambda-3)/3$ is a prime power and 4 divides $\lambda v(v-1)$ then there exists a*

$$\mathrm{GDD}(vq^2,\ \lambda v(v-1)q^2/12,\ q(q+1),\ 4q,\ \lambda_1=q,\ \lambda_2=\lambda,\ m=q^2,\ n=v).$$

(v) *If $q=(\lambda v-\lambda-4)/4$ is a prime power and 5 divides $\lambda v(v-1)$ then except when $v=15$ and $\lambda=2$ there exists a*

$$\mathrm{GDD}(vq^2,\ \lambda v(v-1)q^2/20,\ q(q+1),\ 5q,\ \lambda_1=q,\ \lambda_2=\lambda,\ m=q^2,\ n=v).$$

Proof. (i) For all $v\ge 3$ there exists a CD(v, $v(v-1)$, $3(v-1)$, 3, 6).

(ii) For all $v=2t+1\ge 3$ there exists a CD(v, tv, $3t$, 3, 3).

(iii) For all v there exists a CD(v, $\lambda v(v-1)/2$, $\lambda(v-1)$, 2, λ).

(iv) If 4 divides $\lambda v(v-1)$ and 3 divides $\lambda(v-1)$ then there exists a CD(v, $\lambda v(v-1)/12$, r, 4, λ).

(v) If 5 divides $\lambda v(v-1)$ and 4 divides $\lambda(v-1)$ then there exists a CD$(v, \lambda v(v-1)/20, r, 5, \lambda)$ unless $v=15$ and $\lambda=2$.

For example, using $v=3$ in Corollary 3.2(i), there exists a

$$\text{GDD}(75, 150, 30, 15, \lambda_1=5, \lambda_2=6, m=25, n=3).$$

Using $t=1$ and then 2 in Corollary 3.2(ii) shows that there exists a

$$\text{GDD}(12, 12, 6, 6, \lambda_1=2, \lambda_2=3, m=4, n=3)$$

which is SR68 in Clatworthy and a

$$\text{GDD}(125, 250, 30, 15, \lambda_1=5, \lambda_2=3, m=25, n=5).$$

Corollary 3.3. (i) *If $q=2v-3$ is a prime power then there exists a*

$$\text{GDD}(vq^2, v(v-1)q^2/2, 2(v-3)(v-1), 4(2v-3), \lambda_1=2v-3, \lambda_2=6, m=q^2, n=(q+3)/2).$$

(ii) *If $q=4u-1$ is a prime power then there exists a*

$$\text{GDD}((3u+1)q^2, u(3u+1)q^2, 4u(4u-1), \lambda_1=4u-1, \lambda_2=4, m=q^2, n=3u+1)$$

(iii) *If $q=4u-1$ is a prime power then there exists a*

$$\text{GDD}((q+2)q^2, q^2(q+1)(q+2)/4, q(q+1), 4q, \lambda_1=q, \lambda_2=3, m=q^2, n=q+2).$$

Proof. Use Corollary 3.2(iv) with (i) $\lambda=6$, (ii) $\lambda=4$ writing $v=3u+1$ and (iii) $\lambda=3$ writing $v=4u+1$.

For example, using $v=4$ and then 5 in Corollary 3.3(i), there exists a

$$\text{GDD}(100, 150, 30, 20, \lambda_1=5, \lambda_2=6, m=25, n=4)$$

and a

$$\text{GDD}(245, 490, 56, 28, \lambda_1=7, \lambda_2=6, m=49, n=5).$$

Using $u=1$ and then 2 in Corollary 3.3(ii) there exists a

$$\text{GDD}(36, 36, 12, 12, \lambda_1=3, \lambda_2=4, m=9, n=4)$$

and a

$$\text{GDD}(343, 2401, 196, 28, \lambda_1=7, \lambda_2=4, m=49, n=7).$$

Using $q=3$ and then 7 in Corollary 3.3(iii) there exists a SBIBD(45, 12, 3) and a

$$\text{GDD}(441, 1764, 56, 28, \lambda_1=7, \lambda_2=3, m=49, n=9).$$

Corollary 3.4. (i) *If $q=5u-2$ or $5u-1$ and is a prime power then there exists a*

$$\mathrm{GDD}(q^2(q+2), q^2(q+1)(q+2)/5, q(q+1), 5q, \lambda_1=q, \lambda_2=4, m=q^2, n=q+1).$$

(ii) *If $q=5u-1$ is a prime power then there exists a*

$$\mathrm{GDD}(q^2(4u+1), q^2u(4u+1), q(q+1), 5q, \lambda_1=q, \lambda_2=5, m=q^2, n=4u+1).$$

Proof. Use Corollary 3.2(v) with $\lambda=4$ writing v as $5u$ or $5u+1$ and with $\lambda=5$ writing $v=4u+1$ respectively.

Remark. If $q=4$ this gives a

$$\mathrm{GDD}(80, 80, 20, 20, \lambda_1=4, \lambda_2=5, m=16, n=5)$$

which can be easily extended to an SBIBD(85, 21, 5).

Remark. This method can always be used to give

$$\mathrm{SBIBD}\left(\frac{p^{n+1}-1}{p-1}, \frac{p^n-1}{p-1}, \frac{p^{n-1}-1}{p-1}\right)$$

but, as v v : v known, we do not pursue this construction.
designs with these parameters are already

Appendix 1 gives a listing of GDD's obtained by these methods using BIBD's listed in Mathon and Rosa (1985) for $r\leq 15$. We have a computer listing for $r\leq 41$.

4. Other designs

We note that a symmetric CD(v, k, λ) always exists whenever an SBIBD(v, k, λ) exists. Thus Theorem 3.1 can be reformulated as:

Theorem 4.1. *Let q be a prime power. Suppose an* SBIBD($q(q+1)/\lambda+1, q+1, \lambda$) *exists, then there exists a regular*

$$\mathrm{GDD}(q^3(q+1)/\lambda+q^3, q(q+1), \lambda_1=q, \lambda_2=\lambda, m=q^2, n=q(q+1)\lambda+1).$$

Trivially an SBIBD($q+2, q+1, q$) always exists and so does an SBIBD($q^2(q+2), q(q+1), q$) for q a prime power.

Also, suppose that we are interested in pairwise balanced designs: we note that an SBIBD(31, 6, 1) exists and a B BD(6, 9, 9, 6, 9) exists. These give regular

$$\mathrm{GDD}(31.25, 30, \lambda_1=5, \lambda_2=1)$$

and

$$\mathrm{GDD}(6.25, 9.25, 45, 30, \lambda_1=5, \lambda_2=9).$$

Thus we have a

$$\mathrm{PBD}(6.25, 40.25, 75, k_1 = 30, k_2 = 6, \lambda = 10).$$

For convenience, we state the generalization as a theorem noting that a B BD$(q+1, 2q-\lambda, 2q-\lambda, q+1, 2q-\lambda)$ always exists for $\lambda < 2q$. We used "BBD" for balanced block design.

Theorem 4.2. *Let q be prime power. Suppose an* SBIBD$(q(q+1)/\lambda + 1, q+1, \lambda)$ *exists; then there exists a pairwise balanced design*

$$\mathrm{PBD}(q^2(q+1), q^2(\lambda(q^2+q-1)+2q+1), q(3q+1-\lambda),$$
$$k_1 = q(q+1), k_2 = q+1, \lambda' = 2q).$$

Appendix 1

	BIBD parameters					GDD parameters						
No.	v	b	r	k	λ	$v1$	$b1$	$r1$	$k1$	λ_1	λ_2	m
1	7	7	3	3	1	28	28	6	6	2	1	4
2	4	4	3	3	2	16	16	6	6	2	–	–
3	9	12	4	3	1	81	108	12	9	3	1	9
4	13	13	4	4	1	117	117	12	12	3	1	9
5	7	7	4	4	2	63	63	12	12	3	2	9
6	5	5	4	4	3	45	45	12	12	3	–	–
7	6	10	5	3	2	96	160	20	12	4	2	16
8	16	20	5	4	1	256	320	20	16	4	1	16
9	21	21	5	5	1	336	336	20	20	4	1	16
10	11	11	5	5	2	176	176	20	20	4	2	16
11	6	6	5	5	4	96	96	20	20	4	–	–
12	13	26	6	3	1	325	650	30	15	5	1	25
13	7	14	6	3	2	175	350	30	15	5	2	25
14	10	15	6	4	2	250	375	30	20	5	2	25
15	25	30	6	5	1	625	750	30	25	5	1	25
16	31	31	6	6	1	775	775	30	30	5	1	25
17	16	16	6	6	2	400	400	30	30	5	2	25
18	15	35	7	3	1	540	1260	42	18	6	1	36
19	8	14	7	4	3	288	504	42	24	6	3	36
20	15	15	7	7	3	540	540	42	42	6	3	36
21	8	8	7	7	6	288	288	42	42	6	–	–
22	9	24	8	3	2	441	1176	56	21	7	2	49
23	25	50	8	4	1	1225	2450	56	28	7	1	49
24	13	26	8	4	2	637	1274	56	28	7	2	49
25	9	18	8	4	3	441	882	56	28	7	3	49
26	49	56	8	7	1	2401	2744	56	49	7	1	49
27	57	57	8	8	1	2793	2793	56	56	7	1	49
28	19	57	9	3	1	1216	3648	72	24	8	1	64
29	10	30	9	3	2	640	1920	72	24	8	2	64
30	7	21	9	3	3	448	1344	72	24	8	3	64

Note that GDD's with $r1$ greater than 10 are not listed in Clatworthy (1973).

Appendix 1 (continued)

	BIBD parameters					GDD parameters						
No.	v	b	r	k	λ	$v1$	$b1$	$r1$	$k1$	λ_1	λ_2	m
31	28	63	9	4	1	1792	4032	72	32	8	1	64
32	10	18	9	5	4	640	1152	72	40	8	4	64
33	46	69	9	6	1		BIBD unknown					
34	16	24	9	6	3	1024	1536	72	48	8	3	64
35	28	36	9	7	2	1792	2304	72	56	8	2	64
36	64	72	9	8	1	4096	4608	72	64	8	1	64
37	73	73	9	9	1	4672	4672	72	72	8	1	64
38	37	37	9	9	2	2368	2368	72	72	8	2	64
39	25	25	9	9	3	1600	1600	72	72	8	3	64
40	19	19	9	9	4	1216	1216	72	72	8	4	64
41	21	70	10	3	1	1701	5670	90	27	9	1	81
42	6	20	10	3	4	486	1620	90	27	9	4	81
43	16	40	10	4	2	1296	3240	90	36	9	2	81
44	41	82	10	5	1	3321	6642	90	45	9	1	81
45	21	42	10	5	2	1701	3402	90	45	9	2	81
46	11	22	10	5	4	891	1782	90	45	9	4	81
47	51	85	10	6	1		BIBD unknown					
48	21	30	10	7	3	1701	2430	90	63	9	3	81
49	81	90	10	9	1	6561	7290	90	81	9	1	81
50	91	91	10	10	1	7371	7371	90	90	9	1	81
51	31	31	10	10	3	2511	2511	90	90	9	3	81
52	12	44	11	3	2	1200	4400	110	30	10	2	100
53	12	33	11	4	3	1200	3300	110	40	10	3	100
54	45	99	11	5	1	4500	9900	110	50	10	1	100
55	12	22	11	6	5	1200	2200	110	60	10	5	100
56	45	55	11	9	2	4500	5500	110	90	10	2	100
57	100	110	11	10	1		BIBD unknown					
58	111	111	11	11	1		BIBD unknown					
59	56	56	11	11	2	5600	5600	110	110	10	2	100
60	23	23	11	11	5	2300	2300	110	110	10	5	100
61	25	100	12	3	1	3025	12100	132	33	11	1	121
62	13	52	12	3	2	1573	6292	132	33	11	2	121
63	9	36	12	3	3	1089	4356	132	33	11	3	121
64	7	28	12	3	4	847	3388	132	33	11	4	121
65	37	111	12	4	1	4477	13431	132	44	11	1	121
66	19	57	12	4	2	2299	6897	132	44	11	2	121
67	13	39	12	4	3	1573	4719	132	44	11	3	121
68	10	30	12	4	4	1210	3630	132	44	11	4	121
69	25	60	12	5	2	3025	7260	132	55	11	2	121
70	61	122	12	6	1		BIBD unknown					
71	31	62	12	6	2	3751	7502	132	66	11	2	121
72	21	42	12	6	3	2541	5082	132	66	11	3	121
73	16	32	12	6	4	1936	3872	132	66	11	4	121
74	13	26	12	6	5	1573	3146	132	66	11	5	121
75	22	33	12	8	4		BIBD unknown					
76	33	44	12	9	3	3993	5324	132	99	11	3	121

Appendix 1 (continued)

	BIBD parameters					GDD parameters						
No.	v	b	r	k	λ	$v1$	$b1$	$r1$	$k1$	λ_1	λ_2	m
77	121	132	12	11	1	14641	15972	132	121	11	1	121
78	133	133	12	12	1	16093	16093	132	132	11	1	121
79	45	45	12	12	3	5445	5445	132	132	11	3	121
80	27	117	13	3	1	3888	16848	156	36	12	1	144
81	40	130	13	4	1	5760	18720	156	48	12	1	144
82	66	143	12	6	1	7986	17303	132	66	11	1	121
83	14	26	13	7	6	2016	3744	156	84	12	6	144
84	27	39	13	9	4	3888	5616	156	108	12	4	144
85	40	52	13	10	3		BIBD unknown					
86	66	78	13	11	2	9504	11232	156	132	12	2	144
87	144	156	13	12	1		BIBD unknown					
88	157	157	13	13	1		BIBD unknown					
89	79	79	13	13	2	11376	11376	156	156	12	2	144
90	40	40	13	13	4	5760	5760	156	156	12	4	144
91	27	27	13	13	6	3888	3888	156	156	12	6	144
92	15	70	14	3	2	2535	11830	182	39	13	2	169
93	22	77	14	4	2	3718	13013	182	52	13	2	169
94	8	28	14	4	6	1352	4732	182	52	13	6	169
95	15	42	14	5	4	2535	7098	182	65	13	4	169
96	36	84	14	6	2	6084	14196	182	78	13	2	169
97	15	35	14	6	5	2535	5915	182	78	13	5	169
98	85	170	14	7	1		BIBD unknown					
99	43	86	14	7	2	7267	14534	182	91	13	2	169
100	29	58	14	7	3	4901	9802	182	91	13	3	169
101	22	44	14	7	4	3718	7436	182	91	13	4	169
102	15	30	14	7	6	2535	5070	182	91	13	6	169
103	169	182	14	13	1	28561	30758	182	169	13	1	169
104	183	183	14	14	1	30927	30927	182	182	13	1	169
105	31	155	15	3	1	6076	30380	210	42	14	1	196
106	16	80	15	3	2	3136	15680	210	42	14	2	196
107	11	55	15	3	3	2156	10780	210	42	14	3	196
108	7	35	15	3	5	1372	6860	210	42	14	5	196
109	6	30	15	3	6	1176	5880	210	42	14	6	196
110	16	60	15	4	3	3136	11760	210	56	14	3	196
111	61	183	15	5	1	11956	35868	210	70	14	1	196
112	31	93	15	5	2	6076	18228	210	70	14	2	196
113	21	63	15	5	3	4116	12348	210	70	14	3	196
114	16	48	15	5	4	3136	9408	210	70	14	4	196
115	13	39	15	5	5	2548	7644	210	70	14	5	196
116	11	33	15	5	6	2156	6468	210	70	14	6	196
117	76	190	15	6	1	14896	37240	210	84	14	1	196
118	26	65	15	6	3	5096	12740	210	84	14	3	196
119	16	40	15	6	5	3136	7840	210	84	14	5	196
120	91	195	15	7	1	17836	38220	210	98	14	1	196
121	16	30	15	8	7	3136	5880	210	112	14	7	196
122	21	35	15	9	6	4116	6860	210	126	14	6	196

Appendix I (continued)

	BIBD parameters					GDD parameters						
No.	v	b	r	k	λ	$v1$	$b1$	$r1$	$k1$	λ_1	λ_2	m
123	136	204	15	10	1		BIBD unknown					
124	46	69	15	10	3		BIBD unknown					
125	28	42	15	10	5		BIBD unknown					
126	56	70	15	12	3	10976	13720	210	168	14	3	196
127	71	71	15	15	3	13916	13916	210	210	14	3	196
128	36	36	15	15	6	7056	7056	210	210	14	6	196
129	31	31	15	15	7	6076	6076	210	210	14	7	196

References

Bose, R.C. (1939). On the construction of balanced incomplete block designs. *Ann. Eugenics* 9, 353–399.

Clatworthy, W.H. (1973). *Tables of Two-Associate-Class Partially Balanced Designs*, National Bureau of Standards Applied Mathematics Series 63. U.S. Government Printing Office, Washington, DC.

Denes, J. and A.D. Keedwell (1974). *Latin Squares and Their Applications*. Univ. Press, London.

De Launey, W. and J. Seberry (1987). New group divisible designs obtained via matrices associated with generalized Hadamard matrices (submitted).

De Launey, W., D.G. Sarvate and J. Seberry (1985). Generalised Bhaskar Rao designs with block size 3 over Z_4. *Ars Combinat.* 19A, 273–268.

Glynn, D.G. (1978). *Finite Projective Planes and Related Combinatorial Systems*. Ph.D. Thesis, University of Adelaide.

Hanani, H. (1975). Balanced incomplete block designs and related designs. *Discrete Math.* 11, 255–369.

Lam, C. and J. Seberry (1984). Generalized Bhaskar Rao designs. *J. Statist. Plann. Inference* 10, 83–95.

Mathon, R. and A. Rosa (1985). Tables of parameters of BIBDs with $r \leq 41$ including existence, enumeration, and resolvability results. *Ann. Discrete Math.* 26, 275–308.

Preece, D.A. (1976). Non-orthogonal Graeco–Latin designs. *Proceedings of the Fourth Australian Conference on Combinatorial Mathematics*, Lecture Notes in Mathematics No. 560. Springer, Berlin–Heidelberg–New York, 7–26.

Raghavarao, D. (1971). *Construction and Combinatorial Problems in Design of Experiments*. Wiley, New York.

Sarvate, D.G. and J. Seberry (1986). Encryption methods based on combinatorial designs. *Ars Combinat.*, 21A, 237–246.

Seberry, J. (1979). A note on orthogonal Graeco–Latin designs. *Ars Combinat.* 8, 85–94.

Seberry, J. (1984). Regular group divisible designs and Bhaskar Rao designs with block size three. *J. Statist. Plann. Inference* 10, 69–82.

Seberry, J. (1987a). A construction for Williamson type matrices. *Graphs and Combinat.*, to appear.

Seberry, J. (1987b). Generalized Hadamard matrices and colourable designs in the construction of regular GDD's with two and three association classes. *J. Statist. Plann. Inference* 15, 237–246.

Seberry, J. and A.L. Whiteman (1972), Some classes of Hadamard matrices with constant diagonal. *Bull. Austral. Math. Soc.* 7, 233–249.

Shrikhande, S.S. (1962). On a two parameter family of balanced incomplete block designs. *Sankhyā Ser. A* 24, 33–40.

Sterling, L.S. and N. Wormald (1976). A remark on the construction of designs for two-way elimination of heterogeneity. *Bull. Austral. Math. Soc.* 14, 383–388.

Street, D.J. (1981). Graeco latin and nested row and column designs. In: K.L. McAvaney, Ed., *Com-*

binatorial Mathematics VIII, Lecture Notes in Mathematics No. 884. Springer, Berlin-Heidelberg-New York, 304-313.

Wallis, J. (1971). Some results on configurations. *J. Austral. Math. Soc.* 12, 378-384.

Wallis, W.D., A.P. Street, and J. Seberry Wallis (1972). *Combinatorics: Room Squares, Sum Free Sets, Hadamard Matrices*, Lecture Notes in Mathematics No. 292. Springer, Berlin-Heidelberg-New York.

5.3 Recursive Colourability Theorems

In the style of Hanani (1975), Wilson (1975) and many others we first state a general recursive theorem, due to Dr. J. Seberry (personal communication). The proof of the theorem is based on the proofs of Theorem 3 of Seberry (1984) and Theorem 2.4 of Lam and Seberry.

Theorem 5.3.1: *Suppose there exists a* CD(v, b_3, r_3, k, λ), B, *and a* CD(u, b_2, r_1+r_2, k, λ), A, *with a colourable subdesign on w treatments*, X, *which is a* CD(w, b_1, r_1, k, λ) *or* w = 0, 1. *Further suppose that there exist* k-2 *mutually orthogonal Latin squares of order* u-w. *Then there exists a* CD(v_1, k, λ) *where* $v_1 = v(u-w)+w$ *with a colourable subdesign on* w *treatments*.

□

We will now develop Hanani's theory (1975) for CDs.

Theorem 5.3.2 : *Suppose we have a* BIBD(v, b, r, k, λ) *and* CD(k, b_1, r_1, j, μ). *Then there exists a* CD(v,j,$\lambda\mu$) *over* $r.r_1$ *colours*.

Proof. Let R_1, R_2, ..., R_r be disjoint coloured sets of r_1 symbols. Let Q_j be the CD(k,j,μ) obtained by using the colour set R_i, i = 1, 2, ..., r. Replace each block of the BIBD(v,k,λ) by the underlying BIBD(k,j,μ) of CD(k,j,μ). This is done by relabelling the points of each block, say B, of the BIBD(v, k, λ) in order by 1, 2, ..., k. Now, if the point which is labelled by, say s, has already appeared in, say, j-1 blocks of the BIBD(v, k, λ), before it appeared in said B, then replace s with the s^{th} row of Q_j.

□

Example 1 . Let the CD(3, 2, 1) be

$$\begin{bmatrix} a & b & 0 \\ b & 0 & a \\ 0 & a & b \end{bmatrix}$$

Let $R_i = \{a_i, b_i\}$; then

$$Q_i = \begin{bmatrix} a_i & b_i & 0 \\ b_i & 0 & a_i \\ 0 & a_i & b_i \end{bmatrix}$$

Let the BIBD(4, 3, 2) be

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

then a CD(4, 2, 2) is given by

$$\left[\begin{array}{ccc|ccc|ccc|ccc} a_1 & b_1 & 0 & a_2 & b_2 & 0 & a_3 & b_3 & 0 & 0 & 0 & 0 \\ b_1 & 0 & a_1 & b_2 & 0 & a_2 & 0 & 0 & 0 & a_3 & b_3 & 0 \\ 0 & a_1 & b_1 & 0 & 0 & 0 & b_2 & 0 & a_2 & b_3 & 0 & a_3 \\ 0 & 0 & 0 & 0 & a_1 & b_1 & 0 & a_2 & b_2 & 0 & a_3 & b_3 \end{array}\right]$$

Theorem 5.3.3 : *Suppose there exists a pairwise balanced design* PBD[K, λ; v], *where* $K = \{k_1, k_2, \ldots, k_b\}$ *and a* CD(k_i, j, μ) *for each* $k_i \in K$. *Then there exists a* CD(v, j, $\lambda\mu$).

Proof. We suppose that each CD(k_i, j, μ) is coloured with colours $d_{1i}, d_{2i}, \ldots, d_{ri}$ and that the final CD(v, j, λ) is to be coloured with colours $c_1, c_2, \ldots, c_r$.

Recall the construction of a BIBD(v, j, $\lambda\mu$) from a PBD[K, λ; v], where colouring is not considered: any block with k_i elements from the pairwise balanced design PBD[K, λ; v] has its k_i non-zero elements replaced by the

rows of the corresponding BIBD(k_j, b_j, r_j, j, μ) and the zero elements are replaced by the $1 \times b_j$ zero matrix (see for example Hanani(1975)). The number of elements in each block of the new design is j because only BIBD(k_j, j, μ)'s are used and the inner product of two distinct rows of the incidence matrix is $\lambda\mu$, because each original pair is now duplicated μ times.

We now consider the question of colouring the design. Consider the t^{th} block of the PBD[K, λ; v], Y. We suppose that the blocks of the required coloured design obtained from the previous t-1 blocks have been processed and coloured. If the t^{th} block has k_j elements, then replace it by the rows of the BIBD, X, underlying the CD(k_j, j, μ) (as explained in the above paragraph). Suppose that the nonzero entries in, say s^{th} row, obtained by the previous (t-1) blocks, are already coloured with colours c_1, ..., c_{sx}. We wish to colour the nonzero entries in the s^{th} row obtained by X, by r_j colours from $C_s = \{ c_{sx+1}, ..., c_r \}$.

We proceed as follows. We colour the first non-zero row obtained from the current block by $C_1 = \{c_{1x+1}, ..., c_r\}$ as follows : define a one-to-one map $f_1 : C_1 \rightarrow \{1, 2, ..., r_j\}$ and replace the non-zero elements by $f_1^{-1}(a)$, if d_{aj} is the corresponding non-zero entry (colour) in CD(k_j, j, μ) . Now let $C = C_1 \cap C_2$; define $f_2 : C_2 \rightarrow \{1,2, ... ,r_j\}$ such that $f_2(y) = f_1(y)$ for $y \in C$. Replace the non-zero entries of the second row by $f_2^{-1}(a)$ if d_{aj} is the corresponding entry of the CD(k_j, j, μ).

In general, we let $D = (C_1 \cap C_2 \cap .... \cap C_{n-1}) \cap C_n$ and define $f_n : C_n \rightarrow \{1, ..., r_j\}$ such that $f_n(y) = f_k(y)$ if $y \in C_k$, k = 1,..., n-1. We note that if $y \in C_j \cap C_k$, then $f_j(y) = f_k(y)$ so the mapping is well defined. We colour the non-zero entries of the n^{th} row, say y, by $f_n^{-1}(y)$ if d_{yj} is the colour of the corresponding entry of the CD(k_j, j, μ). Thus, in a finite

number of steps, k , all non-zero rows obtained from the t^{th} block of the PBD[K, λ; v] will be coloured. Note that all the required colours in each row have been used by the definition of the f_n 's.

We now show that in any column no colour has been used more than once. Suppose that in some column the same colours occur at the s_1^{th} and s_2^{th} rows. Then $f_{s_1}^{-1}(q) = f_{s_2}^{-1}(p)$ for some p and q. Without loss of generality, we assume $s_1 < s_2$ and consider $f_{s_1}(f_{s_1}^{-1}(q)) = f_{s_1}(f_{s_2}^{-1}(p))$. But, by the definition of f_{s_2} ,

$$f_{s_2}(f_{s_2}^{-1}(p)) = f_{s_1}(f_{s_2}^{-1}(p)) .$$

Thus,

$$q = f_{s_1}(f_{s_1}^{-1}(q)) = f_{s_1}(f_{s_2}^{-1}(p)) = f_{s_2}(f_{s_2}^{-1}(p)) = p ,$$

that is, the same colours d_{pi} and d_{qi} are used in a column of the CD(k_i, j, μ) which is a contradiction.

□

Theorem 5.3.4 : *If* $n \in GD(S, 1, R)$, mR is a subset of CD(k, λ) *and* mS is a subset of CGDD(k, λ, m), *then* $mn \in CD(k, \lambda)$, *where* CD(k, λ) *is the set of all* v's *for which a* CD(v, k, λ) *exists, and* CGDD(k, λ, μ) *is a coloured group divisible design*.

The proof of this theorem is on similar lines to the proof of Theorem 5.3.2 and Hanani (1975, Theorem 2.25).

□

Lemma 5.3.5 : *The residual design of a coloured design* CD(v, v, k, k, λ) *is a coloured design* CD(v-k, v-1, k, k-λ, λ).

Proof. The definitions of residual design (Raghavarao (1971)) and coloured design immediately give the result.

□

5.4 Colourability Construction Theorems

The dimensions of all matrices in this section will be assumed to be compatible and should be determined from the context.

Lemma 5.4.1 : (a) *If* A *and* B *are two colourable matrices over* r_1 *and* r_2 *distinct symbols, then*

$$[\,A : B\,] \quad \text{and} \quad \begin{bmatrix} A & B \\ B & A \end{bmatrix}$$

are colourable matrices over $r_1 + r_2$ *symbols* .

(b) *If* $A_1, A_2, \ldots, A_n$ *are colourable matrices over* $r_1, r_2, \ldots, r_n$ *symbols respectively, then*

$$\begin{bmatrix} A_1 & A_2 & \ldots & A_n \\ A_n & A_1 & & A_{n-1} \\ \vdots & & & \vdots \\ A_2 & \ldots & A_n & A_1 \end{bmatrix}$$

is colourable over $r_1 + r_2 + r_3 + \ldots + r_n$ *symbols*.

For the definitions of supplementary difference sets, cyclic and type 1 incidence matrices refer to Wallis, Street and Seberry Wallis (1972).

Let $S_1, S_2, \ldots, S_n$ be supplementary difference sets with elements from an additive group G of order v. Then the type 1 (or cyclic if G is cyclic) incidence matrices $A_1 = (a^1_{ij}), \ldots, A_n = (a^n_{ij})$ are given by

$$a^p_{ij} = \begin{cases} 1 \text{ if } s^p_j - s^p_i \in S_p, \; S_p = \{s^p_1, s^p_2, \ldots, s^p_{kp}\}, \\ 0 \text{ otherwise.} \end{cases}$$

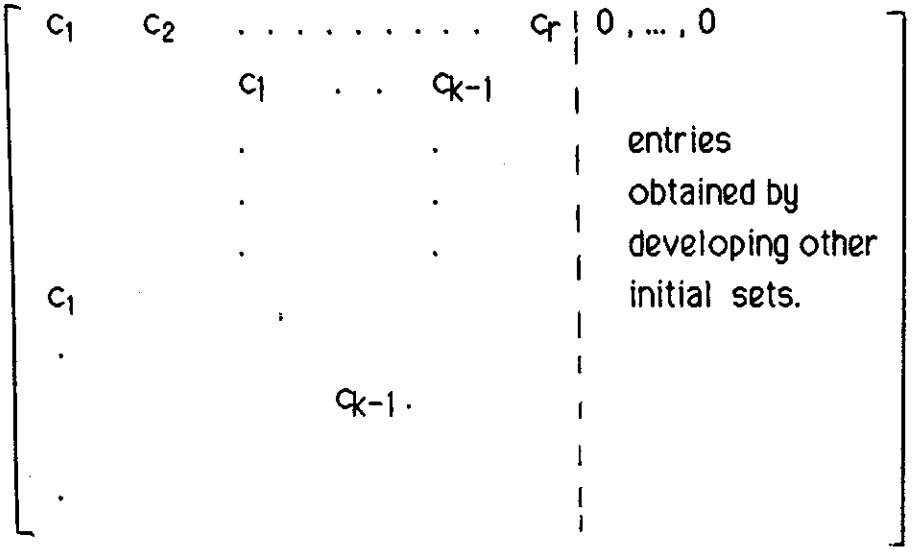
The idea of the following theorem arose in conversation with Dr. J. Seberry.

Theorem 5.4.2 : *Any design which is formed by developing supplementary difference sets to form its cyclic or type 1 incidence matrix is colourable and its complement is also colourable.*

Proof. (i) If the supplementary difference sets contain no element ∞, then one of the r colours is attached to an element of one of the initial sets and the same colour cycled with the element as it is cycled.

(ii) Suppose one initial set, say D contains the element ∞. We proceed by way of the incidence matrix to show how the design should be coloured. Attach r colours to the elements of the initial sets other than ∞ and cycle as before (see(i)). Notice that we also colour the k-1 elements of the set D.

Now attach a zeroth row containing r 1's and b-r 0's, viz. (1, ..., 1, 0, ..., 0) to the matrix obtained by developing k-1 elements of D other than ∞. Let us call this matrix C. We colour the r elements of the zeroth row with the r different colours. Thus we have the following auxiliary matrix of the required coloured design (we assume that the matrix C is in the begining of the incidence matrix of the design):



Now in (k-1) columns of C, there will be two elements labelled with the same colour. Let the colours used for labelling k-1 elements of D other than ∞ be $c_1, \ldots, c_{k-1}$, but, as the design has at least than 2k-1 colours (k-1 for k-1 elements of D other than ∞ and k for each subsequent initial set), we now interchange as follows : in the column where c_i, $i = 1, \ldots, k-1$, occurs we swap, in the row of the second c_i, the colour c_i with the colour c_{k+i-1}.

If a second, different, ∞ occurs the process can be repeated. This completes the proof.

□

Corollary 5.4.3 : *If there exists a cyclic* (v, k, λ) *difference set. Then there exists a* CD(v, k, λ).

Example 2. The BIBD(7, 7, 3, 3, 1) formed by developing the initial block {1, 2, 4} mod 7 is colourable :

A	B	0	D	0	0	0
0	A	B	0	D	0	0
0	0	A	B	0	D	0
0	0	0	A	B	0	D
D	0	0	0	A	B	0
0	D	0	0	0	A	B
B	0	D	0	0	0	A

and its complement BIBD(7, 7, 4, 4, 2) is colourable :

0	0	C	0	E	F	G
G	0	0	C	0	E	F
F	G	0	0	C	0	E
E	F	G	0	0	C	0
0	E	F	G	0	0	C
C	0	E	F	G	0	0
0	C	0	E	F	G	0

It is easy to see that we could have obtained a CD(7, 3, 1) and a CD(7, 4, 2) by using any cyclic latin square of order 7 as follows: Colour the nonzero $(i, j)^{th}$ entry of the incidence matrix of BIBD(7, 3, 1) by the $(i, j)^{th}$ entry of the Latin square. Similarly we get CD(7, 4, 2) from the incidence matrix of BIBD(7, 4, 2). Notice that every latin square of order n is a CD(n, n, n, n, n).

Example 3. We construct the CD(12, 6, 5), developed from the initial sets $(\infty, 1, 3, 4, 5, 9) = D$ and (0, 2, 6, 7, 8, 10). Attach colours a, b, c, d, e to k-1 (= 5) points of D. Attach colours f, g, h, i, j and k to the points of the second initial set. We get:

0	0 0 e 0 0 0 d c b 0 a	f k 0 j i h 0 0 0 g 0
1	a 0 0 e 0 0 0 d c b 0	0 f k 0 j i h 0 0 0 g
2	0 a 0 0 e 0 0 0 d c b	g 0 f k 0 j i h 0 0 0
3	b 0 a 0 0 e 0 0 0 d c	0 g 0 f k 0 j i h 0 0
4	c b 0 a 0 0 e 0 0 0 d	0 0 g 0 f k 0 j i h 0
5	d c b 0 a 0 0 e 0 0 0	0 0 0 g 0 f k 0 j i h
6	0 d c b 0 a 0 0 e 0 0	h 0 0 0 g 0 f k 0 j i
7	0 0 d c b 0 a 0 0 e 0	i h 0 0 0 g 0 f k 0 j
8	0 0 0 d c b 0 a 0 0 e	j i h 0 0 0 g 0 f k 0
9	e 0 0 0 d c b 0 a 0 0	0 j i h 0 0 0 g 0 f k
10	0 e 0 0 0 d c b 0 a 0	k 0 j i h 0 0 0 g 0 f

Now we attach to the above matrix a row of r (=11) 1's and b-r (=11) 0's(called the zeroth row). We colour the 1's in by all the colours a to k. We obtain:

∞	a b c d e f g h i j k	0 0 0 0 0 0 0 0 0 0 0
0	0 0 e 0 0 0 d c b 0 a	f k 0 j i h 0 0 0 g 0
1	a 0 0 e 0 0 0 d c b 0	0 f k 0 j i h 0 0 0 g
2	0 a 0 0 e 0 0 0 d c b	g 0 f k 0 j i h 0 0 0
3	b 0 a 0 0 e 0 0 0 d c	0 g 0 f k 0 j i h 0 0
4	c b 0 a 0 0 e 0 0 0 d	0 0 g 0 f k 0 j i h 0
5	d c b 0 a 0 0 e 0 0 0	0 0 0 g 0 f k 0 j i h
6	0 d c b 0 a 0 0 e 0 0	h 0 0 0 g 0 f k 0 j i
7	0 0 d c b 0 a 0 0 e 0	i h 0 0 0 g 0 f k 0 j
8	0 0 0 d c b 0 a 0 0 e	j i h 0 0 0 g 0 f k 0
9	e 0 0 0 d c b 0 a 0 0	0 j i h 0 0 0 g 0 f k
10	0 e 0 0 0 d c b 0 a 0	k 0 j i h 0 0 0 g 0 f

As we can see that in the first k-1 (=5) columns two colours are same. We interchange the colours as in the theorem and obtain the required CD(12, 6, 5):

∞	a b c d e f g h i j k	0 0 0 0 0 0 0 0 0 0 0
0	0 0 e 0 0 0 d c b 0 a	f k 0 j i h 0 0 0 g 0
1	f 0 0 e 0 0 0 d c b 0	0 a k 0 j i h 0 0 0 g
2	0 a 0 0 j 0 0 0 d c b	g 0 f k 0 e i h 0 0 0
3	b 0 a 0 0 e 0 0 0 d c	0 g 0 f k 0 j i h 0 0
4	c g 0 a 0 0 e 0 0 0 d	0 0 b 0 f k 0 j i h 0
5	d c b 0 a 0 0 e 0 0 0	0 0 0 g 0 f k 0 j i h
6	0 d h b 0 a 0 0 e 0 0	c 0 0 0 g 0 f k 0 j i
7	0 0 d c b 0 a 0 0 e 0	i h 0 0 0 g 0 f k 0 j
8	0 0 0 i c b 0 a 0 0 e	j d h 0 0 0 g 0 f k 0
9	e 0 0 0 d c b 0 a 0 0	0 j i h 0 0 0 g 0 f k
10	0 e 0 0 0 d c b 0 a 0	k 0 j i h 0 0 0 g 0 f

Example 4. CD(8, 3, 6), this example shows the application of the theorem when there are more than one initial sets with ∞ :

A BIBD(8,3,6) can be obtained by developing (modulo 7) the initial blocks $(\infty, 1, 6)$, $(\infty, 2, 5)$, $(\infty, 3, 4)$, $(0, 1, 2)$, $(0, 1, 4)$, $(0, 2, 4)$, $(1, 2, 4)$ and $(1, 2, 4)$. The CD(8, 3, 6) is obtained as follows :

$$
\begin{array}{l}
\infty \\ 0 \\ 1 \\ 2. \\ 3 \\ 4 \\ 5 \\ 6
\end{array}
\left[\begin{array}{cccccccccccccccc}
a_1 & a_2 & \ldots & a_7 & a_8 & \ldots & a_{13} & a_{14} & a_{15} & \ldots & a_{21} & 0 & \ldots & \ldots & \ldots & 0 \\
a_8 & & a_9 & & a_{14} & a_{15} & & & a_1 & a_2 & & a_3 & a_4 & a_5 & \ldots & \\
 & & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & &
\end{array}\right]
$$

develop the blocks with the colours assigned

We can write a CD(8,3,6) with colour set $\{a_1, \ldots, a_{21}\}$ as

$(\infty^*, 1_8, 6_9)$, $(\infty^*, 2_{15}, 5_{16})$, $(\infty^*, 3_1, 4_2)$, $(0_3, 1_4, 2_5)$,

$(0_6, 1_7, 4_{10})$, $(0_{11}, 2_{12}, 4_{13})$, $(1_{14}, 2_{17}, 4_{18})$, $(1_{19}, 2_{20}, 4_{21})$

where x_i means that the colour a_i is assigned to the entry x of the initial block, and '∞^*' means that the nonzero entries in the row corresponding to ∞ are coloured by $a_1, \ldots, a_{21}$. We again assume that the initial blocks with ∞ are developed first.

Example 5. A CD(s^2+s+1, $s+1$, 1) and its complement CD(s^2+s+1, s^2, s^2-s), where s is any prime power, exist because (s^2+s+1, $s+1$, 1) difference sets exist.

Example 6. CD(s, s, s-1, s-1, s-2) exist for all s.

Example 7. To illustrate how the methods are applied to type 1 matrices we give an example, using the additive group of a Galois Field, viz. CD(9,18,8,4,3) exist :

Consider the additive group $GF(3^2)$ which has elements $g_0 = 0$, $g_1 = 1$, $g_2 = 2$, $g_3 = x$, $g_4 = x+1$, $g_5 = x+2$, $g_6 = 2x$, $g_7 = 2x+1$, $g_8 = 2x+2$. Define the set $X = \{y: y = z^2 \text{ for some } z \in GF(3^2)\} = \{x+1, 2, 2x+2, 1\} = \{g_4, g_2, g_8, g_1\}$, using the irreducible equation $x^2 = x+1$. Let $Y = \{x, x+2, 2x, 2x+1\} = \{g_3, g_5, g_6, g_7\}$.

Let $A = (a_{ij})$ and $B = (b_{ij})$ be defined as follows:

$$a_{ij} = \begin{cases} t & \text{if } g_j - g_i = g_t \in X, \\ 0 & \text{otherwise} \end{cases}$$

$$b_{ij} = \begin{cases} s & \text{if } g_j - g_i = g_s \in Y, \\ 0 & \text{otherwise.} \end{cases}$$

Then [A :B] is the required CD, given below :

$$\left[\begin{array}{cccccccccccccccccc}
0 & 1 & 2 & 0 & 4 & 0 & 0 & 0 & 8 & 0 & 0 & 0 & 3 & 0 & 5 & 6 & 7 & 0 \\
2 & 0 & 1 & 0 & 0 & 4 & 8 & 0 & 0 & 0 & 0 & 0 & 5 & 3 & 0 & 0 & 6 & 7 \\
1 & 2 & 0 & 4 & 0 & 0 & 0 & 8 & 0 & 0 & 0 & 0 & 0 & 5 & 3 & 7 & 0 & 6 \\
0 & 0 & 8 & 0 & 1 & 2 & 0 & 4 & 0 & 6 & 7 & 0 & 0 & 0 & 0 & 3 & 0 & 5 \\
8 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 4 & 0 & 6 & 7 & 0 & 0 & 0 & 5 & 3 & 0 \\
0 & 8 & 0 & 1 & 2 & 0 & 4 & 0 & 0 & 7 & 0 & 6 & 0 & 0 & 0 & 0 & 5 & 3 \\
0 & 4 & 0 & 0 & 0 & 8 & 0 & 1 & 2 & 3 & 0 & 5 & 6 & 7 & 0 & 0 & 0 & 0 \\
0 & 0 & 4 & 8 & 0 & 0 & 2 & 0 & 1 & 5 & 3 & 0 & 0 & 6 & 7 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 8 & 0 & 1 & 2 & 0 & 0 & 5 & 3 & 7 & 0 & 6 & 0 & 0 & 0
\end{array}\right]$$

Theorem 5.4.4 : *If a* CD(4t-1, 4t-1, 2t-1, 2t-1, t-1) = C *and its complement* CD(4t-1, 4t-1, 2t, 2t, t) = D *exist, then a* CD(4t, 8t-2, 4t-1, 2t, 2t-1) = C_1 *exists*.

Proof. Let the incidence matrix N of a BIBD(4t, 8t-2, 4t-1, 2t, 2t-1) be partially coloured by using the colouring C and D over disjoint sets of colours R_1 and R_2 to get

$$N = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 & 0 & 0 & \ldots & 0 \\ & & C & & & & D & & \end{bmatrix}.$$

Now colour the (2t-1) non-zero entries of the first row of N with the corresponding non-zero entries of the first row of C and colour remaining 2t entries using 2t colours of R_2. Swap any (2t-1) non-zero entries of the first row of D with non-zero entries of the first row of C to get the required coloured design.

Example 7. a CD(8, 14, 7, 4, 3) :

Using the CD(7,7,3,3,1) and CD(7,7,4,4,2) of Example 1 we get a CD(8,14,7,4,3) as follows :

$R_1 = \{A, B, D\}$ $\qquad$ $R_2 = \{C, E, F, G\}$

$$\begin{bmatrix} A & B & C & D & E & F & G & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ C & E & 0 & F & 0 & 0 & 0 & 0 & 0 & A & 0 & B & D & G \\ 0 & A & B & 0 & D & 0 & 0 & G & 0 & 0 & C & 0 & E & F \\ 0 & 0 & A & B & 0 & D & 0 & F & G & 0 & 0 & C & 0 & E \\ 0 & 0 & 0 & A & B & 0 & D & E & F & G & 0 & 0 & C & 0 \\ D & 0 & 0 & 0 & A & B & 0 & 0 & E & F & G & 0 & 0 & C \\ 0 & D & 0 & 0 & 0 & A & B & C & 0 & E & F & G & 0 & 0 \\ B & 0 & D & 0 & 0 & 0 & A & 0 & C & 0 & E & F & G & 0 \end{bmatrix}$$

The construction given by Shrikhande (1962) can be extended for colourable designs as follows :

Theorem 5.4.5 : *If* $CD(v_i, b_i, r_i, k_i, \lambda_i) = N_i$, $i = 1, 2$ *and their colourable complements,* M_i, *exist , then a* $CD(v = v_1v_2, b = b_1b_2, r = r_1r_2+(b_1-r_1)(b_2-r_2), k = k_1k_2+(v_1-k_1)(v_2-k_2), \lambda = r-b/4)$ *exists, when* $b_i = 4(r_i-\lambda_i)$.

Proof. Let N_1 and N_2 be the coloured incidence matrices of the $CD(v_i, b_i, r_i, k_i, \lambda_i)$, $i = 1, 2$.

Suppose N_1 is coloured with the colours x_1 ,...., x_{r_1} and M_1 is coloured with the colours x_{r_1+1} ,...., x_{b_1} . Further, suppose N_2 is coloured with the colours y_1 ,...., y_{r_2} and M_2 is coloured with the colours y_{r_2+1} ,...., y_{b_2} .

The required coloured design is

$$N = N_1 \times N_2 + M_1 \times M_2 ,$$

where the $(i, j)^{th}$ element is coloured (x_s, y_t) according to the way N_1, M_1, N_2, M_2 are coloured, with the assumption that the zero element is never coloured. Thus N is coloured with the $r_1r_2+(b_1-r_1)(b_2-r_2f)$ colours, (x_s, y_t) where either $s \in \{1, \ldots , r_1\}$ and $t \in \{1, \ldots , r_2\}$ or $s \in \{r_1+1, \ldots , b_1\}$ and $t \in \{r_2+1, \ldots , b_2\}$.

□

5.5 The case k = 2

This simple case can be useful for practical purposes, for example sending secret messages and in the construction of GD designs with larger block size.

Theorem 5.5.1 : *The necessary conditions are sufficient for the existence of a* $CD(v, 2, \lambda)$.

Proof. Let N be the incidence matrix of BIBD(v, 2, 1). Without loss of generality, let

$$N = \begin{bmatrix} 1 & 1 & \cdots & 1 & & & & & & & & \\ 1 & & & & 1 & 1 & \cdots & 1 & \cdots & & & \\ & 1 & & & 1 & & & & & & & \\ & & & & & & & & & & & \\ & & \ddots & & & \ddots & & & & & & \\ & & & \ddots & & & \ddots & & & & & \\ & & & & \ddots & & & \ddots & & & 1 & \\ & & & 1 & & & & 1 & & & 1 & \end{bmatrix}.$$

Colour the first row by 1, 2, ... ,(v-1) = r, second row by 2, 3, ..., (v-1), 1, and so on. It is now easy to check that N is colourable.

Now let N_i be the CD(v, 2, 1) over symbol set $\{1_i, 2_i, \ldots, r_i\}$, then

$$[N_1 : N_2 : \ldots : N_\lambda]$$

gives a CD(v,2,λ).

□

Example 8. CD(5,2,1) :

$$N = \begin{bmatrix} 1 & 1 & 1 & 1 & & & & & & \\ 1 & & & & 1 & 1 & 1 & & & \\ & 1 & & & 1 & & & 1 & 1 & \\ & & 1 & & & 1 & & 1 & & 1 \\ & & & 1 & & & 1 & & 1 & 1 \end{bmatrix}$$

$$Q = \begin{bmatrix} 1 & 2 & 3 & 4 & & & & & & \\ 2 & & & & 3 & 4 & 1 & & & \\ & 3 & & & 4 & & & 1 & 2 & \\ & & 4 & & & 1 & & 2 & & 3 \\ & & & 1 & & & 2 & & 3 & 4 \end{bmatrix}$$

5.6 The case k = 3

First we give the necessary colourable GDDs.

Lemma 5.6.1: *(a)* $6 \in CGDD(3, \lambda, 2)$ $\lambda = 2, 3, 6$.

(b) $8 \in CGDD(3, \lambda, 2)$ $\lambda = 1, 2, 3, 6$.

Proof. (a) $6 \in CGDD(3, 2, 2)$:

$$\begin{bmatrix} 1 & 2 & 0 & 0 & 3 & 4 & 0 & 0 \\ 0 & 0 & 2 & 3 & 0 & 0 & 4 & 1 \\ 3 & 0 & 4 & 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 & 0 & 3 & 0 & 4 \\ 2 & 0 & 0 & 1 & 4 & 0 & 0 & 3 \\ 0 & 4 & 1 & 0 & 0 & 2 & 3 & 0 \end{bmatrix},$$

hence $6 \in CGDD(3,6,2)$.

$6 \in CGDD(3,3,2)$:

$$\begin{bmatrix} 1 & 2 & 0 & 0 & 3 & 4 & 0 & 0 & 5 & 6 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 0 & 3 & 4 & 0 & 0 & 5 & 6 \\ 2 & 0 & 3 & 0 & 4 & 0 & 5 & 0 & 6 & 0 & 1 & 0 \\ 0 & 3 & 0 & 4 & 0 & 5 & 0 & 6 & 0 & 1 & 0 & 2 \\ 4 & 0 & 0 & 5 & 6 & 0 & 0 & 1 & 2 & 0 & 0 & 3 \\ 0 & 5 & 6 & 0 & 0 & 1 & 2 & 0 & 0 & 3 & 4 & 0 \end{bmatrix}.$$

(b) $8 \in CGDD(3,1,2)$ and hence, for all λ, $8 \in CGDD(3,\lambda,2)$:

$$\begin{bmatrix} 1 & 2 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 3 & 0 & 0 \\ 3 & 0 & 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 3 & 0 & 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 3 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 & 0 & 3 \\ 0 & 1 & 0 & 0 & 0 & 2 & 3 & 0 \\ 0 & 0 & 1 & 3 & 0 & 0 & 0 & 2 \end{bmatrix}.$$

□

Theorem 5.6.2 : *Suppose there exists a* CD(v, 3, λ), $v \neq 2, 3, 7$; *then there exists a* CD(3v-2, 3, λ).

Proof. Let

$$B = \begin{bmatrix} X \\ A \end{bmatrix}$$

be the BIBD underlying the CD(v, 3, λ), where X is the first row of B. Write A_i when Ais coloured with the symbol sets $R_i = \{a_{(i-1)r+1}, \ldots, a_{(i-1)r+r}\}$, $i = 1, 2, 3$. Similarly write X_i when X is coloured with the symbol sets $R_i = \{a_{(i-1)r+1}, \ldots, a_{(i-1)r+r}\}$, $i = 1, 2, 3$.

Since $v \neq 2, 3, 7$ there exist two mutually orthogonal latin squares of order v-1. Use them as in Lam and Seberry (1984, Theorem 2.4) to form D of size $3(v-1) \times (v-1)^2$ which is a GDD$(3(v-1), (v-1)^2, v-1, 3, \lambda_1 = 0, \lambda_2 = 1)$. D is, in fact, consists of 3(v-1) permutation matrices of order v-1.

We now form the matrix

$$\begin{bmatrix} X_1 & X_2 & X_3 & 0 & \cdots & 0 \\ A_1 & 0 & 0 & & & \\ 0 & A_2 & 0 & D_1 & D_2 \cdots & D_\lambda \\ 0 & 0 & A_3 & & & \end{bmatrix}$$

Now X_1, X_2 and X_3 use $3r$ colours whereas each A_i uses r colours. $(D_1\ D_2\ \ldots\ D_\lambda) = (M_{ij})$ consists of $\lambda(v-1)$ permutation matrices, M_{ij},(see Seberry(1984)) of order $v-1$ per row. By the block design conditions, $\lambda(v-1) = 2r$. So colour the permutation matrices by the colouring scheme

$$\begin{bmatrix} a_{r+1}, & \ldots, & a_{2r}, & a_{2r+1}, & \ldots, & a_{3r} \\ a_{2r+1}, & \ldots, & a_{3r}, & a_1, & \ldots, & a_r \\ a_1, & \ldots, & a_r, & a_{r+1}, & \ldots, & a_{2r} \end{bmatrix}$$

to obtain the result.

□

Lemma 5.6.3 : *Designs* CD(6t+3, 3, 1) *exist for all* $t \geq 1$.

Proof. The incidence matrix of a BIBD(6t+3,3,1) is given by

$$N = \begin{bmatrix} I & A_1 & \ldots & A_t & 0 & \ldots & 0 & I & \ldots & I \\ I & I & \ldots & I & A_1 & \ldots & A_t & 0 & \ldots & 0 \\ I & 0 & \ldots & 0 & I & \ldots & I & A_1 & \ldots & A_t \end{bmatrix}$$

where $A_i = T^i + T^{-i}$ and $T = (t_{ij})$ is given by:

$$t_{ij} = \begin{cases} 1 & \text{if } j-i \equiv 1 \pmod{2t+1}, \\ 0 & \text{otherwise.} \end{cases}$$

We obtain the required CD over $3t+1$ colours

$\{a_1, \ldots, a_{t+1}, b_1, \ldots, b_t, b_{-1}, \ldots, b_{-t}\}$ by colouring N as follows :

$$\begin{bmatrix} a_1 I & (bA)_1 & (bA)_2 & \ldots & (bA)_t & 0 & 0 & 0 & \ldots & 0 & a_2 I & \ldots & a_{t+1} I \\ a_2 I & a_1 I & a_3 I & \ldots & a_{t+1} I & (bA)_1 & (bA)_2 & (bA)_3 & \ldots & (bA)_t & 0 & \ldots & 0 \\ a_3 I & 0 & 0 & \ldots & 0 & a_1 I & a_2 I & a_4 I & \ldots & a_{t+1} I & (bA)_1 & \ldots & (bA)_t \end{bmatrix}$$

where $(bA)_i = b_i T^i + b_{-i} T^i$.

□

Corollary 5.6.4 : CD(6t+3, 3, λ) *exist for all* $\lambda, t \geq 1$ *and for all* $\lambda \geq 2$, $t \geq 0$.

Corollary 5.6.5 : CD(6t+1, 3, λ) *exist for* $t \equiv 1 \bmod 3$.

Proof. Use Theorem 5.6.2 and Lemma 5.6.3.

□

The existence of a BIBD(v, 3, 1), for $v = 6t+1$, by difference sets in cyclic groups of order 6t+1 was established by Peltesohn(1939) and, for $v = 12t+7$, by difference sets in elementary abelian groups by Bose(1939). Hence, using Theorem 5.4.2 we get:

Lemma 5.6.6 : CD(6t+1, 3, 1) *exists for all* $t \geq 1$.

□

Corollary 5.6.7 : CD(6t+1, 3, λ) *exists for all* λ, $t \geq 1$.

de Launey, Sarvate and Seberry (1985) have proved that

$\{v : v \equiv 0,1 \bmod 3 \text{ and } v > 3\}$ is subset of B(K,1) where
K = {4, 6, 7, 9, 10, 12, 15, 18, 19, 24, 27, 30, 39, 51}. In Table A we have given CD(k_i, 3, 2) for k_i in K, $k_i \neq 1, 3 \bmod 6$ as it is done in Corollaries 5.6.4 and 5.6.5, hence we get:

Lemma 5.6.8 : a CD(v, 3, 2) *exists for* $v \equiv 0,1 \bmod 3$, $v > 3$.

□

Lemma 5.6.9 : CD(2u+1, 3, 3) *exist for all* u, *positive integers* .

Proof . By Lemma 5.3 of Hanani (1975), $v \in B(K_3, 1)$, where $K_3 = \{3, 4, 5, 6, 8\}$. In view of Theorem 5.3.3, it is sufficient to show that CD(k_i, 3, 6) exist for $k_i \in K_3$. Lemma 5.6.9 gives a CD(3, 3, 6) and a CD(5, 3, 6). Example 3 gives CD(8, 3, 6).

□

Lemmas 5.6.4, 5.6.7, 5.6.8, 5.6.9 and 5.6.10 give:

Theorem 5.6.11 : *The necessary conditions are sufficient for the existence of a* CD(v, 3, λ) *for all* λ.

□

Table A. CD(v, 3, 2) for initial values of v.

v = 4 Theorem 5.4.2: initial block (0,1,2).

v = 6

$$\begin{bmatrix} a & b & c & d & e & 0 & 0 & 0 & 0 & 0 \\ 0 & a & 0 & 0 & b & c & 0 & d & e & 0 \\ b & 0 & a & 0 & 0 & 0 & c & 0 & d & e \\ 0 & c & 0 & a & 0 & e & 0 & b & 0 & d \\ 0 & 0 & b & 0 & a & d & e & 0 & c & 0 \\ c & 0 & 0 & b & 0 & 0 & d & e & 0 & a \end{bmatrix}$$

v = 10 = 3.4 -2 Theorem 5.6.2.

v = 12 Theorem 5.4.2; initial blocks (∞, 0, 2), (0, 1, 7), (0, 2, 8) and (0, 1, 8).

v = 18 Theorem 5.4.2; initial blocks (∞, 0, 4), (0, 4, 10), (0, 1, 15), (0, 5, 8), (0, 7, 9) and (0, 5, 6).

v = 24 = 6.4 Theorem 5.3.1.

v = 30 Theorem 5.4.2; initial blocks (∞, 0, 8), (0, 2, 14), (0, 4, 10) and (0, i, 19-i), i = 1, 3, 5, 7, 9, 11, 13.

Table B. CD(v, 3, 3) for initial values of v.

v = 3

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$$

v = 5

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 0 & 0 & 0 & 0 \\ 6 & 1 & 2 & 0 & 0 & 0 & 3 & 4 & 5 & 0 \\ 3 & 0 & 0 & 1 & 2 & 0 & 4 & 5 & 0 & 6 \\ 0 & 4 & 0 & 5 & 0 & 3 & 6 & 0 & 1 & 2 \\ 0 & 0 & 4 & 0 & 6 & 1 & 0 & 2 & 3 & 5 \end{bmatrix}$$

v = 7, 13 Corollary 5.6.7.

v = 9, 15 Corollary 5.6.4.

v = 11 Theorem 5.4.2; initial blocks (0, i, 11-i), i = 1, 2, ..., 4.

v = 17 Theorem 5.4.2; initial blocks (0, i, 17-i), i = 1, 2, ..., 8.

CHAPTER 6
SOME CONSTRUCTIONS OF PBIBDs AND BIBDs

6.1 Construction of PBIBDs from directed graphs

In Chapter 1 a construction was given for PBIBDs using n-partite graphs (Hammer and Sarvate (198?)). Now, we replace the complete graph in the study of Alltop (1966) by a complete directed graph and get a PBIBD(E, β) with five association classes, where E, the set of points, is the set of edges of the complete directed graph G on n vertices and $\beta = \{ B\alpha : \alpha \in S_n \}$, where B is a set of edges of a subgraph of G and S_n is the symmetric group acting on the n vertices of G. Let T denote the set of 2-subsets of E. Then the action of S_n decomposes T into five orbits T_i, $i = 1, \ldots, 5$, where points of T_i are isomorphic to { (a, b), (b, a) }, { (a, b), (a, c) }, { (b, a), (c, a) }, { (a, b), (c, a) }, { (a, b), (c, d) } respectively, where a, b, c and d are all distinct. Let n_i represent the number of points in T_i. Note that

$$n_1 = n(n-1)/2,$$

$$n_2 = n_3 = n(n-1)(n-2)/2,$$

$$n_4 = n(n-1)(n-2)$$

and $$n_5 = n(n-1)(n-2)(n-3)/2.$$

Let u_i be the number of members of T_i contained in B. Let t_i be a member of T_i and let λ_i denote the number of blocks in β containing t_i. If t is any member of T_i, t is also contained in exactly λ_i members of β. Since S_n acts as an automorphism group of (E, β) and S_n is transitive on T_i, (E, β) is a PBIBD(v, b, r, k, λ_1, λ_2, λ_3, λ_4, λ_5) where

$$v = \binom{n}{2},$$

$$| B | = n!/g,$$

$$g = | \{ \alpha \in S_n : B\alpha = B \} |$$

and $$\lambda_i = bu_i / n_i.$$

All λ_i's will coincide if

$$n = u_2/u_1 + 2$$
$$= u_5/u_2 + 3$$

and $$2u_2 = u_4.$$

An example, where the conditions hold, has not yet been found.

Example: Let B be the set of edges of cycle $(a_1, a_2, \ldots, a_k)$ where (a_i, a_{i+1}) and (a_{i+1}, a_i) both are edges of the cycle. Then $u_1 = u_2 = u_3 = k$, $u_4 = 2k$ and $u_5 = 2k(k-3)$. Hence we get a PBIBD(5) with parameters

$(2\binom{n}{2}, n!/(2k(n-k)), r, 2k, 2bk/(n(n-1)), 2bk/(n(n-1)(n-2)),$
$2bk/(n(n-1)(n-2)), 2bk/(n(n-1)(n-2)), 4bk(k-3)/(n(n-1)(n-2)(n-3))).$

Taking $n = 7$ and $k = 4$ we get a PBIBD with $v = 42$, $b = 105$, $r = 20$, $k = 8$ and two distinct λ's 20 and 4.

□

6.2 Construction of BIBDs

Two of the constructions given in the attched paper, ("On a BIBD construction", Ars Combinatoria, 22, 1986, 165-169) give as special cases, series of BIBDs and PBIBDs with the same parameters as those given by Sinha(1979, 1984)

Some combinatorial identities are used to prove that the parameters are the same. For the sake of completeness, the shorter proofs provided by Dr. D. R. Breach, are given.

(a). $$\binom{v}{k} - 2\binom{v-1}{k-1} + 2\binom{v-2}{k-2}$$

$$= \text{coefficient of } x^k \text{ in } [\,(1+x)^v - 2x(1+x)^{v-1} + 2x^2(1+x)^{v-2}\,]$$

$$= \text{coefficient of } x^k \text{ in } [\,(1+x^2)(1+x)^{v-2}\,]$$

$$= \binom{v-2}{k} + \binom{v-2}{k-2}.$$

(b). $$\binom{v}{k} - 3\binom{v-1}{k-1} + 3\binom{v-2}{k-2}$$

$$= \text{coefficient of } x^k \text{ in } [\,(1+x)^v - 3x(1+x)^{v-1} + 3x^2(1+x)^{v-2}\,]$$

$$= \text{coefficient of } x^k \text{ in}$$

$$(1+x)^{v-3}[\,(1+x)^3 - 3x(1+x)^2 + 3x^2(1+x) - x^3 + x^3\,]$$

$$= \text{coefficient of } x^k \text{ in } (1+x)^{v-3}\,[\,(1+x-x)^3 + x^3\,]$$

$$= \binom{v-3}{k} + \binom{v-3}{k-3}.$$

□

The detailed calculations to get the expression for Λ_2 in Theorem 1 of the attached paper are as follows:

We consider the pair ((a,b), (c,d)) where a, b, c and d are all distinct points in V. The pair will occur in those blocks of Y, which are obtained from a block of X, say B, which satisfies one of the following:

(i) a, b, c, d are in the block B : the number of such blocks is λ_4;

(ii) (a,b) is in the block B but not (c,d) : the number of such blocks is $\lambda_2 - 2\lambda_3 + \lambda_4$;

(iii) (c,d) is in the block B but not (a,b) : the number of such blocks is $\lambda_2 - 2\lambda_3 + \lambda_4$;

(iv) none of a, b, c and d is in the block B : we observe that the number of such blocks is equal to

b - {4(the number of blocks of X in which some point, say a, occurs but none of other points b, c and d) + 6(the number of blocks of X in which a pair, say (a,b), occurs but not the other pair (c,d)) + 4(the number of blocks

of X in which a triple, say (a,b,c) occurs but not the remaining point d) + (the number of blocks of X in which the quadruple (a,b,c,d) occurs)}

The above expression is equal to

$$b - \{4(r-3\lambda_2+3\lambda_3-\lambda_4) + 6(\lambda_2-2\lambda_3+\lambda_4) + 4(\lambda_3-\lambda_4) + \lambda_4\}.$$

Hence we obtain

$$\Lambda_2 = \lambda_4 + 2(\lambda_2-2\lambda_3+\lambda_4) + b-\{4(r-3\lambda_2+3\lambda_3-\lambda_4)+6(\lambda_2-2\lambda_3+\lambda_4)+4(\lambda_3-\lambda_4)+\lambda_4\}$$

$$= b - 4r + 8\lambda_2 - 8\lambda_3 + 4\lambda_4$$

$$= b - 3r + 3\lambda_2 - r + 5\lambda_2 - 8\lambda_3 + 4\lambda_4.$$

On a BIBD construction

Dinesh G. Sarvate

It is shown that methods of Saha [3] and Sinha [4, 5] can be adapted so that triangular PBIBDs and BIBDs can be obtained from a 4-design instead of from the full design of all k-subsets of a given set.

Theorem 1: *Let* X = BIBD (v, b, r, k, λ_2, λ_3, λ_4) *be a 4-design. Then* Y = PBIBD($V = \binom{v}{2}$, B = b, $R = b - 2r + 2\lambda_2$, $K = \binom{k}{2} + \binom{v-k}{2}$, $\Lambda_1 = b - 3r + 3\lambda_2$, $\Lambda_2 = b - 4r + 8\lambda_2 - 8\lambda_3 + 4\lambda_4$) *exists.*

Proof. It is well known that the parameters r, λ_2, λ_3 and λ_4 of a 4-design satisfy

$$r = (v-1)(v-2)(v-3)\lambda_4/(k-1)(k-2)(k-3) \quad \ldots \quad 1.1$$

$$\lambda_2 = (v-2)(v-3)\lambda_4/(k-2)(K-3) \quad \ldots \quad 1.2$$

$$\lambda_3 = (v-3)\lambda_4/(k-3) \quad \ldots \quad 1.3$$

Let the points of the PBIBD Y be the pairs of points of X. Each block B of X gives a block B' of Y, constructed in the following way : The points in B' are the pairs of points in B and the pairs of points in V-B. (V-B is the complement of B)

A pair (a,b) occurs λ_2 times in X and either the point a or the point b but not both occurs in $2r - \lambda_2$ blocks of X. Hence (a,b) occurs in $R = b - (2r - \lambda_2) + \lambda_2 = b - 2r + 2\lambda_2$ blocks of Y.

Consider a triple (a,b,c) of V. It occurs λ_3 times in X, therefore ((a,b),(a,c)) occurs $\lambda_3 + b - (3r - 3\lambda_2 + \lambda_3) = b - 3r + 3\lambda_2$ times in Y. We will first check this:

We observe that,

(a,b,c) occurs	:	λ_3 times in X,
(a,b) but not c occurs	:	$\lambda_2 - \lambda_3$ times, as (a,b) has already occurred λ_3 times.
a but not b or c occurs	:	$r - (\lambda_3+(\lambda_2-\lambda_3)+(\lambda_2-\lambda_3))$ times, i.e. $r - 2\lambda_2 + \lambda_3$ times.

Therefore the number of blocks without a, b, c is $b-(\lambda_3+3(\lambda_2-\lambda_3)+3(r-2\lambda_2+\lambda_3)) = b - (3r-3\lambda_2+\lambda_3)$, hence the pairs of the type ((a,b),(a,c)) will occur

$$\Lambda_1 = \lambda_3 + b - (3r - 3\lambda_2 + \lambda_3)$$

times as ((a,b),(a,c)) will occur when either all of a, b and c are in a block of X or none of a, b and c is in a block of X. (In the second case ((a,b),(a,c)) occurs in a block of Y because a, b and c will be in the complement of the block of X). Note that this is an application of the principle of inclusion and exclusion.

Now we consider the pair ((a,b),(c,d)) where a, b, c and d are all distinct points in V. The pair will occur in those blocks of Y,which are obtained from a block of X, say B, which satisfies one of the following:

(i) a, b, c and d are in the block B,

(ii) (a,b) is in the block B but not (c,d),

(iii) (c,d) is in the block B but not (a,b),

(iv) none of a, b, c and d is in the block B.

Hence we get

$$\Lambda_2 = b - 3r + 3\lambda_2 - r + 5\lambda_2 - 8\lambda_3 + 4\lambda_4$$
$$= \Lambda_1 - (r - 5\lambda_2 + 8\lambda_3 - 4\lambda_4),$$

Which proves the theorem.

□

EXAMPLE 1: Consider the Steiner quintuple system on 11 points(see for example page 74 of Biggs and White[1] or page 775 of Hughes[2]). This design has $\lambda_4 = 1$ and hence $\lambda_3 = 4$, $\lambda_2 = 12$, $r = 30$ and $b = 66$. We get a PBIBD(V=55, B=66, R=30, K=25, Λ_1=12, Λ_2=14).

The series of PBIBDs obtained in the above Theorem will give a series of BIBDs if $\Lambda_1 = \Lambda_2$ i.e. if

$$r - 5\lambda_2 + 8\lambda_3 - 4\lambda_4 = 0.$$

Using 1.1,1.2 and 1.3 we get

$$v^3 - v^2(1 + 5k) + (2 + k + 8k^2)v - 2k - 4k^3 = 0.$$

We observe that $v = k$ is a solution and hence we have

$$(v - k)(v^2 - (1+4k)v + 4k^2 + 2) = 0,$$

hence we get $v = (1 + 4k \pm \sqrt{(8k - 7)}) / 2$.

Suppose $\sqrt{(8k - 7)} = 2s + 1$, $s \geq 0$ integer, then

$$8k = (2s+1)^2 + 7$$

and 8 divides $(2s+1)^2 + 7$ agreeing with the fact that k is an integer. Let $k = ((2s+1)^2 + 7)/8$ for $s \geq 1$, then $v = s^2 + 2s + 3$ or $s^2 + 2$. Hence we have

THEOREM 2: *If* $v = s^2+2s+3$ *or* $s=s^2+2$, $s\geq1$, *and if a 4-design with parameters* $v, b, r, k=((2s+1)^2+7)/8, \lambda_2, \lambda_3, \lambda_4$ *exists, then there exists a* $BIBD(V=\binom{v}{2}, B=b, R=b-2r+2\lambda_2, K=\binom{k}{2}+\binom{v-k}{2}, \Lambda= b-3r+3\lambda_2)$.

□

In particular, when s is even, say equal to 2w, then we have $v = 4w^2 + 4w + 3$ or $v = 4w^2 + 2$ and $k = 2w^2 + w + 1$. Hence as a special case when we take the set of all k-subsets of $\{1,2, \ldots ,v\}$ as a 4-design, we get

COROLLARY3: *There exists a series of BIBDs with parameters*

$(V = \binom{v}{2}, B = \binom{v}{k}, R = \binom{v}{k} - 2\binom{v-1}{k-1} + 2\binom{v-2}{k-2}, K = \binom{k}{2} + \binom{v-k}{2}, \Lambda = \binom{v}{k} - 3\binom{v-1}{k-1} + 3\binom{v-2}{k-2})$, *where* $v = 4w^2 + 4w + 3$ *or* $4w^2 + 2$ *and* $k = 2w^2 + w + 1$.

□

We observe that the parameters of the series obtained in the Corollary 3 are the same as those given by K.Sinha[4] because

$$\binom{v}{k} - 2\binom{v-1}{k-1} + 2\binom{v-2}{k-2} = \binom{v-2}{k} + \binom{v-2}{k-2} \text{ and}$$

$$\binom{v}{k} - 3\binom{v-1}{k-1} + 3\binom{v-2}{k-2} = \binom{v-3}{k} + \binom{v-3}{k-3}.$$

THEOREM 4 : *Let* $D_1 = (v, b_1, r_1, k, \lambda_2, \lambda_3, \lambda_4)$ *and* $D_2 = (v-k, b_2, r_2, k, \lambda_2', \lambda_3', \lambda_4')$ *be 4-designs. Then there exists a PBIBD* $D = (V=\binom{v}{2}, B = b_1b_2, R = \lambda_2b_2 + (b_1 - (2r_1 - \lambda_2))\lambda_2', K = 2\binom{k}{2} = k(k-1), \Lambda_1 = b_2.\lambda_3 + \lambda_3'(b_1 - 3r + 3\lambda_2 - \lambda_3), \Lambda_2 = b_2\lambda_4 + 2(\lambda_2 - 2\lambda_3 + \lambda_4)\lambda_2' + (b_1 - 4r + 6\lambda_2 - 4\lambda_3 + \lambda_4)\lambda_4')$.

PROOF : The set of the points of D is the set of all the pairs from {1,2,...v}, which gives $V = \binom{v}{2}$. The blocks are constructed in the following way: Let B_1 be a block of D_1. Consider the (v - k)-set $(V - B_1)$. Now construct a BIBD isomorphic to D_2 with points in $V - B_1$. Construct b_2 blocks of D, where each block consists of pairs of points in B_1 together with pairs of points in the blocks of D_2. In this way each block of D_1 gives b_2 blocks of D. Hence $b = b_1 b_2$. The block size K of D is $2\binom{k}{2} = k(k-1)$.

Now consider any pair (a,b) (i.e. a point of D), (a,b) has occurred λ_2 times in D_1 and 'a' (also 'b') has occurred r_1 times and hence in the construction of blocks of D, 'a' and 'b' together have been used $b_1 - (2r_1 - \lambda_2)$ times as points of D_2. Therefore (a,b) as a point of D occurs $\lambda_2 b_2 + (b_1 - (2r_1 - \lambda_2))\lambda_2'$ times.

Any pair of 2-sets, (i.e. any pair of points of D) having a point in common, are first associates and any pair of disjoint 2-sets are second associates. The counting arguments similar to those of Theorem 1 give the values of Λ_1 and Λ_2.

□

If D_1 is the set of all k-sets of a v-set and D_2 is the set of all k-sets of a (v-k)-set, then counting the repeated blocks only once, we get the result of Sinha[5].

The first construction of Saha[3] suggested the following theorem:

THEOREM 5: *Suppose there exists a t-design , T, with parameters* v, b, r, k, $\lambda_1, \lambda_2, \ldots, \lambda_t$, *then given an integer s such that* $2s \leq t$, *there exists P, a* PBIBD($V=\binom{v}{s}$, B=b, R=λ_s, K=$\binom{k}{s}$, $\Lambda_1=\lambda_{s+1}, \ldots, \Lambda_i=\lambda_{s+i}, \ldots, \Lambda_s=\lambda_{2s}$).

PROOF: The points of the required PBIBD, P, are the s-tuples of the points of the given t-design, T. For each block X of T construct a block of P consisting of all s-tuples of X. If two s-tuples θ and Φ have (s-i) points of

T in common, then they are called the i^{th} associates, for i = 1, 2, ..., s. Θ and Φ contain (s-i+2i)= s+i distinct points of T and hence, as each (s+i)-tuple occurs in λ_{s+i} times in T, we have $\Lambda_i=\lambda_{s+i}$.

□

COROLLARY 6: *If there exists a* t-(v,k,λ_t) *design,* $t \geq 4$, *then there exists a* PBIBD($\binom{v}{2}$, B = b, R = λ_2, K = $\binom{k}{2}$, $\Lambda_1 = \lambda_3$, $\Lambda_2 = \lambda_4$).

EXAMPLE 2: Consider the Steiner quintuple system on 11 points(see example 1). We get a PBIBD(V=55,B=60,R=12,K=10,Λ_1=4,Λ_2=1). Note that this design is not a quasi-multiple of a smaller design.

ACKNOWLEGEMENT: My sincere thanks are due to Dr. J. Seberry for her kind supervision. I am thankful to the referee for useful suggestions.

REFERENCES:

[1] N. L. Biggs and A. T. White, Permutation Groups and Combinatorial Structures, London Mathematical Society Lecture Note Series **33**, Cambridge University Press, 1979.

[2] D. R. Hughes, On t-designs and groups, *Am. J. Math*, **87**, 1965, 761-778.

[3] G. M. Saha, On construction of T_m -type PBIB designs, *Ann. Inst. Statist. Math.*, **25** (3), 1973, 605-616.

[4] K. Sinha, A series of BIB designs, *J. Australian Math. Soc.* (Ser. A), **27**, 1979, 88-90.

[5] K. Sinha, A BIBD arising from a construction for PBIBDs, *Ars Combinatoria*, **18**, 1984, 217-219.

CHAPTER 7
ORTHOGONAL DESIGNS

A transversal design TD(n, t) is a GDD with n groups, each of size t, and block size n.

Let B(K) denote the set of integers v for which there exists a PBD(v, K, 1).

Let S and K be sets of positive integers. Let s and t be integers. We denote by ${}_sS^t$ the set $\{v : s \le v \le t\} \cap S$. The notation ${}_sS$ and S^t stand for the sets $\{v : v \ge s\} \cap S$ and $\{v : 0 \le v \le t\} \cap S$ respectively. Define $[v_0]SOK = \{v \mid v = v_0 s+k$ where $s \in S, k \in K$ and $s \ge k\}$.

7.1 Generalized Bhaskar Rao designs

The results proved in the attached papers

(a) "Generalized Bhaskar Rao designs with block size 3 over Z_4", (with de Launey and Seberry) Ars Combinatoria, 19A, 1985, 273-285

and

(b) "Non-existence of certain GBRDs", (with de Launey), Ars Combinatoria, 18, 1984, 5-20

include the following:

Theorem 7.1.1: *The necessary conditions are sufficient for the existence of a GBRD with block size 3 over Z_4, except possibly when* $v = 27$ *or* 39 *and* $\lambda = 4$.

Proof. Theorem 2.4 of (a).

□

Theorem 7.1.2: *Neither a* GBRD(10, 4, 2) *over* Z_2 *nor a* GBRD(7, 4, 4) *over* $Z_2 \times Z_2$ *exists*.

Proof. Sections 2 and 4 of (b).

□

The proof of Theorem 7.1.1 depends on constructing small GBRDs and about one third of that work was by this author. The results on the GBRD(10, 4, 2) over Z_2 were checked with the help of J. Seberry. To prove that the GBRD(7, 4, 4) over Z_4 does not exists, it was necessary to prove that all four non-equivalent BIBD(7, 4, 4)s can not be signed by $Z_2 \times Z_2$. A exhaustive computer search was conducted to obtain a GBRD(7, 4, 4) over $Z_2 \times Z_2$ for two of the BIBD(7, 4, 4)s. It turned out that these two designs can not be signed by $Z_2 \times Z_2$. By "exhaustive computer search" is meant that a computer program has been written and used to check each possibility of signing the rows of the two BIBDs. The result on the non-existence of a GBRD(7, 4, 4) over $Z_2 \times Z_2$ has also been obtained by Gibbons and Mathon (1986).

After the Lemma 4.2 in the paper (b), it is shown how the two of the four inequivalent BIBD(7, 4, 4) can not be signed over $Z_2 \times Z_2 = \{1, a, b, ab\}$. The explanation of the working for the first of the two BIBDs (given under the heading "a" below Lemma 4.2 of paper(b)) follows:

Suppose that x_{ij} denotes the (i, j)th entry of the signed matrix. Without loss of generality we assume:

$\text{ratio}(x_{1\,i}, x_{1j}) = r(x_{1i}, x_{1j}) = 1$ {see definition 4.1 of the paper (b)};

$r(x_{21}, x_{22}) = a$; $r(x_{2\,10}, x_{2\,13}) = 1$;

$r(x_{31}, x_{32}) = b$;

$r(x_{41}, x_{42}) = ab$.

Hence we have:

$r(x_{23}, x_{26}) = a$; { as $r(x_{1i}, x_{1j}) = 1$ and Lemma 4.2(i)}

$r(x_{34}, x_{37}) = b$; { as $r(x_{1i}, x_{1j}) = 1$ and Lemma 4.2(i)}

$r(x_{45}, x_{48}) = ab$; { as $r(x_{1i}, x_{1j}) = 1$ and Lemma 4.2(i)}

Now $r(x_{55}, x_{58}) = a$ or b { as $r(x_{1i}, x_{1j}) = 1$, $r(x_{45}, x_{48}) = ab$ and Lemma 4.2(ii)}

and $r(x_{54}, x_{57}) = a$ or ab { as $r(x_{1i}, x_{1j}) = 1$, $r(x_{34}, x_{37}) = b$ and Lemma 4.2(ii)}.

Hence we have $r(x_{55}, x_{58}) = r(x_{54}, x_{57}) = a$.

We have $r(x_{4\ 10}, x_{4\ 13}) = b$ { as $r(x_{2\ 10}, x_{2\ 13}) = 1$, $r(x_{21}, x_{22}) = a$, $r(x_{41}, x_{42}) = ab$ and Lemma 4.2(i)}.

Now no value of $r(x_{5\ 10}, x_{5\ 13})$ can be found to satisfy Lemma 4.2 (i) and (ii). Because $r(x_{55}, x_{58})r(x_{45}, x_{48}) = b$ and $r(x_{4\ 10}, x_{4\ 13}) = b$ implies $r(x_{5\ 10}, x_{5\ 13}) = 1$ {Lemma 4.2(i)} and $r(x_{2\ 10}, x_{2\ 13}) = 1$ implies $r(x_{5\ 10}, x_{5\ 13}) \neq 1$ {Lemma 4.2(ii)}

Generalised Bhaskar Rao designs with block size 3 over Z_4

Warwick de Launey, Dinesh G. Sarvate, Jennifer Seberry

0. Introduction

Although a considerable amount of work has been done on generalised Bhaskar Rao designs, little is known about the existence of these designs over groups which are not elementary abelian. This paper considers the group Z_4 and finds that designs exist for Z_4 for parameters for which they do not exist for $Z_2 \times Z_2$ and vice versa.

Suppose we have a matrix W with elements from an abelian group

$G = \{h_1, h_2, \ldots, h_g\}$, where $W = h_1A_1 + h_2A_2 + \ldots + h_gA_g$; here $A_1, \ldots, A_g$ are $v \times b$ (0,1) matrices, and the Hadamard product $A_i * A_j$ $(i \neq j)$ is zero. Suppose $(a_{i1}, \ldots, a_{ib})$ and $(b_{j1}, \ldots, b_{jb})$ are the ith and jth rows of W; then we define WW^+ by

$$(WW^+)_{ij} = (a_{i1}, \ldots, a_{ib}) \cdot (b_{j1}^{-1}, \ldots, b_{jb}^{-1})$$

with . designating the scalar product. Then W is a *generalised Bhaskar Rao design or GBRD* if:

(i) $WW^+ = rI + \sum_{i=1}^{m} (c_iG)B_i$;

(ii) $N = A_1 + \ldots + A_g$ satisfies $NN^T = rI + \sum_{i=1}^{m} \lambda_i B_i$,

that is, N is the incidence matrix of a PBIBD(m), and (c_iG) gives the number of times a complete copy of the group G occurs.

Such a matrix will be denoted by $GBRD_G(v,b,r,k;\lambda_1,\ldots,\lambda_m;c_1,\ldots,c_m)$. In this paper we shall only be concerned with $m = 1$, $c = \lambda/g$, and $B_1 = J - I$. In this case N is the incidence matrix of a PBIBD(1), that is, a BIBD. Hence, the equations become:

(i) $WW^+ = rI + \frac{\lambda G}{g}(J - I)$;

(ii) $NN^T = (r-\lambda)I + \lambda J$.

Thus W is a $GBRD_G(v,b,r,k,\lambda)$. Since $\lambda(v-1) = r(k-1)$ and $bk = vr$, we sometimes use the notation $GBRD(v,k,\lambda;G)$.

These matrices are generalisations of generalised weighing matrices and may be used in the construction of PBIBDs.

We use the following notation for the initial blocks of a GBRD. We say $(a_\alpha, b_\beta, \ldots, c_\gamma)$ is an initial block, when the Latin letters are developed mod n and the Greek subscripts are the elements of the group, which will be placed in the incidence matrix in the positions indicated by the Latin letters. Thus we place α in the $(i,a-1+i)$th position of the incidence matrix, β in the $(i,b-1+i)$th position, and so on.

We form the difference table of the initial block $(a_\alpha, b_\beta, \ldots, c_\gamma)$ by placing in the position headed by x_α (Column) and by row y_β the element $(x-y)_{\delta\eta^{-1}}$ where $(x-y)$ is mod n and $\delta\eta^{-1}$ is in the abelian group.

A set of initial blocks will be said to form a *GBR difference set* (if there is one initial block) or *GBR supplementary difference sets*

(if more than one) if in the totality of elements

$$(x-y)\,\delta\eta^{-1} \pmod{n, G}$$

each non-zero element a_h, $a \pmod n$, $h \in G$, occurs $\lambda/|G|$ times.

For any other definition or notation the reader is referred to de Launey and Seberry [1]. Let $|G| = g$.

For a GBRD$(v,k,\lambda;G)$ to exist $\lambda \equiv 0 \pmod g$ and there must exist a BIBD(v,k,λ). So the parameters v,k,λ must satisfy the constraints,

(i) $v \geq k$

(ii) $\lambda \equiv 0 \pmod g$

(iii) $\lambda(v-1) \equiv 0 \pmod{(k-1)}$

(iv) $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$.

In view of these constraints a GBRD$(v,3,4t;Z_4)$ can exist only when one of the following is true,

(a) $t \equiv 0 \pmod 3$, $v \geq 3$,

(b) $t \not\equiv 0 \pmod 3$, $v \equiv 0,1 \pmod 3$ and $v \geq 3$.

Moreover a theorem of Drake [2, Theorem 1.10] ensures that no GBRD$(3,3,4t;Z_4)$ exists when t is odd. We show that, with the possible exception of the cases given in the abstract, these necessary conditions are also sufficient.

§1. A Small Generating Set

In this section and the next we make extensive use of Wilson's notation [6, Sections 1 and 2] concerning PBD-closure theory. In the next section we will need a small generating set for

$$V = \{v > 3 \mid v \equiv 0,1 \pmod 3\}.$$

Notation 1.1: Let S and K be sets of positive integers. Define

$$[v_0]\ S \oplus K = \{v \mid v = v_0 s + k \text{ where } s \in S,\ k \in K \text{ and } s \geq k\}.$$

Let a and b be integers. Then let ${}_aS^b$ denote the set

$$\{v \mid a \leq v \leq b\} \cap S. \qquad \square$$

The following theorem appears in de Launey and Seberry [1, Theorem 1.2.14].

Theorem 1.2: *Let $v_0 \geq 2$ be an integer. Let S be an increasing infinite sequence such that for all $t \in S$ there exists a $TD(v_0+1,t)$. Let K be a set of positive integers containing v_0 and v_0+1. Let $k_0 = \min_{k \in K} \{k\}$ and suppose there exists a $TD(v_0+1,t_0)$ for some t_0*

not necessarily in S. *Then*

(i) $\mathbb{B}\left(\{t_0\} \cup {}_{t_0}S^{v_0t_0+k_0-1} \cup T \cup K\right) \supseteq [v_0]\, S \oplus K$, *where*

$$T = \{t \in {}_{v_0t_0+k_0}S \mid t \notin [v_0]_{t_0} S \oplus K\} .$$

(ii) $\mathbb{B}\left(\{t_0\} \cup {}_{t_0}S^{v_0t_0+k_0-1} \cup U \cup K\right) \supseteq \{v \geq v_0t_0+k_0\}$, *where*

$$U = \{t \mid t \geq v_0t_0+k_0 \text{ and } t \notin [v_0]_{t_0} S \oplus K\} . \qquad \square$$

This theorem allows us to calculate small generating sets for sets of the form $\{v \geq k \mid v \notin U\}$, where K is a finite set of integers $u \geq k$ [1, Lemma 1.2.16]. We extend the theorem so that we can calculate small generating sets for sets of the form $\{v \geq k \mid v \equiv 0,1 \pmod 3,\ v \notin U\}$.

Now slightly altering a construction appearing in Wilson's paper [6, Lemma 5.1] we have the following result.

Lemma 1.3: *Let* K *be a set of positive integers. Suppose there exists a* GDD *on* v *points with block sizes from* $\{4,5\}$ *and group sizes from* K. *Then*

$$3v \in \mathbb{B}\left(\{3k \mid k \in K\}, \cup \{4\}\right)$$

and

$$3v+1 \in \mathbb{B}\left(\{3k+1 \mid k \in K\} \cup \{4\}\right) . \qquad \square$$

But the construction of the PBD's in the proof of Theorem 1.2 [1, Theorem 1.2.14] relies in the first place on the construction of GDD's with block sizes from $\{v_0, v_0+1\}$ and group sizes from ${}_{t_0}S^{v_0t_0+k_0-1} \cup T \cup K \cup \{t_0\}$ in case (i) and from ${}_{t_0}S^{v_0t_0+k_0-1} \cup U \cup K \cup \{t_0\}$ in case (ii). So putting $v_0 = 4$ we have the following result.

Theorem 1.4: *Let* S *be an increasing infinite sequence such that for all* $t \in S$ *there exists a* $TD(5,t)$. *Let* K *be a set of positive integers. Let* $k_0 = \min_{k \in K}\{k\}$ *and suppose there exists a* $TD(5,t_0)$ *for some* t_0 *not necessarily in* S. *Then*

(i) $\{3v \mid v \in [4]\, S \oplus K\} \subseteq \mathbb{B}\left(\{4\} \cup \{3v \mid v \in {}_{t_0}S^{4t_0+k_0-1} \cup T \cup K \cup \{t_0\}\}\right)$

and

$$\{3v+1 \mid v \in [4] S \oplus K\} \subseteq \mathbb{B}\left(\{4\} \cup \{3v+1 \mid v \in {}_{t_0}S^{4t_0+k_0-1} \cup T \cup K \cup \{t_0\}\}\right)$$

where

$$T = {}_{t_0+k_0}S \setminus ([4]_{t_0}S + K) ,$$

(ii) $\{3v \mid v \geq 4t_0+k_0\} \subseteq \mathbf{B}\left(\{4\} \cup \{3v \mid 3v \mid v \in {}_{t_0}S^{4t_0+k_0-1} \cup U \cup K \cup \{t_0\}\}\right)$

and

$$\{3v+1 \mid v \geq 4t_0+k_0\} \subseteq \mathbf{B}\left(\{4\} \cup \{3v+1 \mid v \in {}_{t_0}S^{4t_0+k_0-1} \cup U \cup K \cup \{t_0\}\}\right)$$

where

$$U = \{v \geq 4t_0+k_0\} \setminus ([4]_{t_0}S \oplus K) .$$ □

We apply this theorem to prove the following result.

Theorem 1.5: *The following set inequalities hold*:

(i) $\{v \mid v \equiv 0 \pmod 3,\ v>3\} \subseteq \mathbf{B}\left(\{4,10\} \cup \{3v \mid v = 2,3,\ldots,11,13,17\}\right)$;

(ii) $\{v \mid v \equiv 0,1 \pmod 3 \text{ and } v>3\} \subseteq \mathbf{B}\left(\{4,6,7,9,10,12,15,18,19,24,27,30,39,51\}\right)$.

Proof. We apply Theorem 1.4 with

$S = \{4,5,7,8,9,11,12,13,16,17\} \cup \{v \equiv \pm 1 \pmod 6 \mid v \geq 17\}$,

$K = \{2,3,4,5,6,7,\ldots,17\}$,

$t_0 = 4$.

When $v \geq 70$, $v - 4t \in \{2,3,\ldots,17\}$ for some $t \geq 17$, $t \in S$. So $\{v \mid v \geq 70\} \subseteq [4]_t S \oplus K$. It is then a simple matter to check that

$$[4]_{t_0} S \oplus K = \{v \geq 18 \mid v \neq 21,26,27,28,29\} .$$

So $U = \{21,26,27,28,29\}$ and hence

$$\{3v \mid v \geq 18\} \subseteq \mathbf{B}\left(\{4\} \cup \{3v \mid v = 2,3,\ldots,17,21,26,27,28,29\}\right) .$$

Now $3v \in \mathbf{B}(\{4,6,9\})$ for $v \in \{12,14,15,16,21,26,27,28\}$ (see Appendix A), while $87 \in \mathbf{B}(\{6,9,10\})$ (use TD(10,9)). Thus

$$\{3v \mid v \equiv 0 \pmod 3,\ v>3\} \subseteq \mathbf{B}(\{4,10\} \cup \{3v \mid v = 2,3,\ldots,11,13,17\})$$

Now $\{3v+1 \mid v \geq 4\} = \mathbf{B}\{4,7,10,19\}$ and $21,\ 33 \in \mathbf{B}(\{4,6,9\})$ (add suitable blocks and points to TD(4,5) and TD(4,8) respectively), so

$$\{v \mid v \equiv 0,1 \pmod 3,\ v>3\} \subseteq \mathbf{B}(\{4,6,7,9,10,12,15,18,19,24,27,30,39,51\}).$$ □

Because we do not as yet have designs for $v \in \{27,39\}$ we prove the following theorem.

Theorem 1.6: *The following set inequality holds*

$$\{v \mid v \equiv 0,1 \pmod 3,\ v>3\} \setminus \{27,39\} \subseteq \mathbf{B}(\{4,6,7,9,10,12,15,18,19,24,30,51\}).$$

Proof. Apply Theorem 1.4 with

$S = \{4,5,7,8,11,12,16,17\} \cup \{v \equiv \pm \pmod 6 \mid v \geq 17\}$,

$K = \{2,3,\ldots,8,10,11,12,14,\ldots,17,21,25\}$,

$t_0 = 4$.

When $v \geq 70$ there exists a $k \in \{2,3,\ldots,8,10,11,12,14,\ldots,17,21,25\}$ and $t \in S$ such that

$$v = 4t + k \quad \text{and} \quad t \geq k$$

except when

(i) $v = 4t + 9$ and $t = 17$, 23 or 29, or

(ii) $v = 4t + 13$ and $t = 19$.

When $18 \leq v \leq 70$, $v \in [4]\ S \oplus K$ except when

$$v \in \{21,26,27,28,29,41,42,43,45,57,61,62,63,65\} .$$

So $U = \{21,26,27,28,29,41,42,43,45,57,61,62,63,65,77,89,101,125\}$.

But using the designs given in Appendix A

$$\{3v \mid v \in U\} \subseteq \mathbb{B}(\{4,6,7,9,10,12,13,15,18,19,21,31\})$$
$$\subseteq \mathbb{B}(\{4,6,7,9,10,12,15,18,19\}). \quad \ldots\ldots\ldots (1.1)$$

Note that $21 \in \mathbb{B}(\{4,6\})$ (add a point to TD(4,5)) and that $31 \in \mathbb{B}(\{4,10\})$ [6, see the proof of Theorem 5.1(ii)].

Let $V = \{v \mid v \equiv 0 \pmod 3,\ v > 3,\ v \neq 27,39\}$ and apply Theorem 1.4(ii). Then $V \subseteq \mathbb{B}(\{4\} \cup \{3v \mid v \in \{2,3,\ldots,8,10,11,12,14,\ldots,17,21,25\}\} \cup U)$. But then, by (1.1),

$$V \subseteq \mathbb{B}(\{4,6,7,9,10,12,15,18,19,21,24,30,33,36,42,\ldots,51,63,75\}).$$

Finally $\{36,42,45,48,63\} \subseteq \mathbb{B}(\{4,6,9,12,15\})$ (Table 1, Appendix A), $21, 33 \in \mathbb{B}(\{4,6,9\})$ (see the proof of Theorem 1.5), $75 \in \mathbb{B}(\{4,15\})$ (Appendix A), and $\{3v+1 \mid v \geq 1\} \subseteq \mathbb{B}(\{4,7,10,19\})$. The result then follows. □

§2. The Constructions

Lemma 2.1: *There exists a* GBRD$(v,3,4;Z_4)$ *for all* $v \equiv 0,1 \pmod 3$, $v \geq 4$, *except possibly when* $v = 27,39$.

Proof. The necessary conditions give $v \equiv 0,1 \pmod 3$. Drake's theorem [2,Theorem 1.10] ensures that $v \geq 4$ but since the number of blocks, $2v(v-1)/3$, is divisible by 4 the Seberry, Street, Rodger theorem (theorem 1,4; or see [5]) gives no new conditions.

By Theorem 1.6 we need to establish existence for

$$v \in \{4,6,7,9,10,12,15,18,19,24,30,51\} .$$

The required designs for $v = 4,6,9,10$ and 15 are given in Appendix B. The designs for $v = 7,12,18$ and 30 can be obtained by developing the initial blocks indicated:

$v = 7$ develop the initial blocks

$(0_1,1_1,6_i)$, $(0_1,2_{-1},5_{-i})$, $(0_1,3_1,4_i)$, $(0_1,1_{-1},3_{-1})$ (mod $7,Z_4$);

$v = 12$ develop the initial blocks

$(\infty_1,3_1,9_i)$, $(\infty_1,6_{-1},7_i)$, $(1_1,3_1,4_{-i})$, $(3_{-1},5_{-1},9_1)$, $(1_1,4_1,5_1)$,

$(2_1,6_{-1},8_1)$, $(6_1,7_{-1},10_{-i})$, $(2_1,8_{-i},10_{-1})$(mod $11,Z_4$);

$v = 18$ develop the initial blocks

$(0_1,a_1,(17-a)_i)$, $a = 1,3,5,7$,

$(0_1,b_1,(17-b)_{-i})$, $b = 2,4,6,8$,

$(0_1,2_1,6_1)$, $(0_1,3_{-1},8_1)$, $(\infty_1,0_1,1_{-1})$, $(\infty,0_i,7_{-i})$(mod 17, Z_4);

$v = 30$ develop the initial blocks

$(0_1,a_1,(29-a)_i)$, $a = 1,3,\ldots,13$ (odd numbers),

$(0_1,b_{-1},(29-b)_{-i})$, $b = 4,6,\ldots,14$ (even numbers),

$(0_1,2_{-1},15_1)$, $(0_1,2_1,10_1)$, $(0_1,3_{-1},12_1)$, $(0_1,4_1,11_{-1})$, $(0_1,1_{-1},6_1)$,

$(\infty_1,0_1,2_i)$, $(\infty_1,0_{-i},4_{-1})$ (mod $29,Z_4$).

Finally $19 = 6(4-1) + 1$, $24 = 4 \times 6$ and $51 = 10(6-1) + 1$. So a composition theorem applies [1,Theorem 1.1.3] to give designs for $v = 19$, 24 and 51. □

Theorem 2.2: *There exists a* GBRD$(v,3,8;Z_4)$ *for all* $v \geq 3$.

Proof. By Hanani's theorem (see Proposition 5.1 of [6]) and the construction of Theorem 2.2 of Lam and Seberry [3] we only need to establish the existence of GBRD$(v,3,8;Z_4)$ for $v = 3,4,6$. The design for $v = 3$ is

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & i & 1 & i & -1 & -i & -1 & -i \\ i & 1 & -i & -1 & i & -1 & -i & -1 \end{bmatrix}$$

and the designs for $v = 4$ and 6 are two copies of the suitable designs with $\lambda = 4$ given in Appendix B. Hence we have the result. □

Theorem 2.3: *There exists a* $GBRD(v,3,12;Z_4)$ *for all* $v \geq 4$.

Proof. By Drake's Theorem [1, Theorem 1.10]we cannot obtain this design for $v = 3$. Now combining Hanani's Theorem (as stated in [1, Corollary 1.1.2(ii)]) with Theorem 2.2 of Lam and Seberry [3] we only need to establish existence for $v \in K_4^2 = \{4,5,6,7,8,9,10,11,12, 14,15,18,19,22,23\}$. Now these designs can be obtained in the following manner

v	Construction
4	3 copies of design for $\lambda = 4$.
5	Use $SBIBD(5,4,3)$ and $GBRD(4,3,4;Z_4)$ in Theorem 2.2 of [3].
6	3 copies of design for $\lambda = 4$.
7	3 copies of design for $\lambda = 4$.
8	Use $BIBD(8,4,3)$ with $GBRD(4,3,4;Z_4)$.
9	3 copies of design for $\lambda = 4$.
10	3 copies of design for $\lambda = 4$.
11	Use $SBIBD(11,6,3)$ and $GBRD(6,3,4;Z_4)$.
12	3 copies of design for $\lambda = 4$.
14	Remove one row of $SBIBD(15,7,3)$ to obtain a $PBD(\{7,6\},14,3)$, use with $GBRD(u,3,4;Z_4)$, $u \in \{6,7\}$.
15	3 copies of design for $\lambda = 4$ or use $SBIBD(15,7,3)$ and $GBRD(7,3,4;Z_4)$.
18	Use $PBD(\{6,9\},18,3)$ (found from an $SBIBD(25,12,3)$ by de Launey and Seberry [1], Lemma 1.3.7, by removing the first seven rows) with $GBRD(u,3,4;Z_4)$, $u \in \{6,9\}$.
19	$6(4-1)+1$ and so Theorem 3 of Seberry [4] applies.
22	$7(4-1)+1$ and so Theorem 3 of Seberry [4] applies.
23	Develop the following initial blocks $(0_1,(2t+1)_1,(22-2t)_i)$, $(0_1,(2t)_{-1},(23-2t)_{-i})$, $t = 1,\ldots,5$ all thrice, $(0_1,1_{-i},2_{-i})$ thrice, $(0_1,5_{-1},7_{-1})$ three times, $(0_1,1_{-1},11_{-1})$ twice, $(0_1,3_{-1},9_{-1})$ twice, $(0_1,1_{-1},9_{-1})$, $(0_1,3_{-1},11_{-1})$, $(0_1,4_1,8_1)$, $(0_1,4_1,10_1)$ (mod $23,Z_4$).

Hence we have the result. □

Note: A straightforward construction for a GBRD(27,3,12;Z_4) can be obtained by using the PBD({6,9},27,3) of Lemma 1.3.5 of de Launey and Seberry and a GBRD(u,3,4;Z_4) $u \in \{6,9\}$.

Theorem 2.4: *The necessary conditions*

$$2tv(v-1) \equiv 0 \pmod 3,$$

$$t \equiv 1,5 \pmod 6 \Rightarrow v \neq 3,$$

are sufficient for the existence of a GBRD(v,3,4t;Z_4) *except possibly for* (v,t) = (27,1) and (39,1).

Proof. The necessary conditions follow from the necessary conditions for block designs and the non-existence for $v = 3$, $t \equiv 1,5 \pmod 6$ from Drake's Theorem [2].

To establish existence we distinguish four cases:

1. $2 \nmid t$, $3 \nmid t$: then the necessary condition is $v \equiv 0,1 \pmod 3$ and the result follows, except for $v = 27$ or 39 by taking multiple copies of the designs given in Theorem 2.1. For $v = 27$ or 39 we note GBRD(v ,3,8;Z_4) and GBRD(v ,3,12;Z_4) exist and so multiple copies give the designs for $v = 27$ or 39 and $t > 1$;
2. $2 \mid t$, $3 \nmid t$: then the necessary condition is $v \equiv 0,1 \pmod 3$, $v \geq 3$, but this is established in Theorem 2.2;
3. $2 \nmid t$, $3 \mid t$: then the necessary condition is $v \geq 4$ (by Drake's Theorem [2, Theorem 10.1] and this is established in Theorem 2.3;
4. $2 \mid t$, $3 \mid t$: here there is no condition of v. By part 2. of this theorem we only have to consider the cases $v = 3$ and $\lambda = 12s$, s even but these can be obtained using multiples of the GBRD(3,3,8;Z_4) of part 3.

Hence we have the result. □

Appendix A

Notation. By TD(r,t) we denote a *transversal design* on r groups each of size t. □

Table 1 gives designs needed for Theorem 1.5. In particular it lists GDDs which have been constructed to satisfy Lemma 1.3. See Street and Rodger for the construction involving GBRDs. The constructions involving point and block removals from certain designs are quite standard [6, Remarks 3.5 and 3.6]. Table 2 gives PBD designs needed in Theorem 1.6. Any references given in a table give a place where a design used in a construction can be found. The reader should note MacNeish's Theorem [6, Theorem 3.2].

Table 1. (GDD's on 3v points satisfying Lemma 1.3.)

v	
12	Obtain a GDD by removing a point from SBIBD(13,4,1).
14	Use GBRD(7,4,2;Z_2) de Launey and Seberry [1,Theorem 4.1.1].
15	GBRD(5,4,3;Z_3) [1, Lemma 5.1.1].
16	Use TD(4,4).
21	

0000	1111	0000	0000	0000	0000
I	0	I	A	A^3	A^2
I	A^2	0	I	A	A^3
I	A^3	A^2	0	I	A
I	A	A^3	A^2	0	I
I	I	A	A^3	A^2	0

where $I = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$ and $A = \begin{pmatrix} & 1 & & \\ & & 1 & \\ & & & 1 \\ 1 & & & \end{pmatrix}$.

26	GBRD(13,4,2;Z_2)	[1, Theorem 4.1.1],
27	GBRD(9,4,3;Z_3)	[1, Lemma 5.1.1],
28	Use TD(4,7).	

Table 2. (PB-design on v points)

v				
123	TD(10,13)	$\in$	123	$\mathbb{B}$({6,9,10,13}).
126	TD(10,13)	$\in$	126	$\mathbb{B}$({9,10,13}).
129	TD(10,13)	$\in$	129	$\mathbb{B}$({9,10,12,13}).
171	TD(9,19)	$\in$	171	$\mathbb{B}$({9,19}).
183	TD(10,19)	$\in$	183	$\mathbb{B}$({9,10,12,19}).
186	TD(10,19)	$\in$	186	$\mathbb{B}$({9,10,15,19}).
189	TD(10,19)	$\in$	189	$\mathbb{B}$({9,10,18,19}).
195	TD(7,31)	$\in$	195	$\mathbb{B}$({6,7,9,31}).

□

Finally 75 and 135 $\in \mathbb{B}(\{4,15\})$. There exist a GBRD(4,4,5;Z_5) [1, Theorem 2.2(iii)(b)] and a GBRD(u,4,3;Z_3) for $u \in \{5,9\}$ [1, Theorem 5.1.1] so there exists a GBRD(u,4,15;Z_{15}) for $u \in \{5,9\}$ and hence a GDD with u groups of size 15 and with all blocks of size 4. It follows that 75 and 135 $\in \mathbb{B}(\{4,15\})$.

Appendix B

We use the notation - for -1 and $\bar{i}$ for $-i$, $e = (1,1,1)$ and

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Then the following designs exist.

GBRD$(4,3,4;Z_4)$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & i & - & -i & 0 & - & 1 \\ 1 & - & 0 & i & 0 & -i & 1 & i \\ 0 & 1 & - & 0 & i & -i & i & i \end{bmatrix}$$

GBRD$(6,3,4;Z_4)$

$$\left[\begin{array}{cccccccccc|cccccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & - & i & 0 & \bar{i} & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & - & 0 & 0 & i & \bar{i} & 0 & - & 0 & 0 & i & \bar{i} & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & - & i & 0 & 0 & 0 & \bar{i} & 1 & \bar{i} & 0 & 0 & 0 & i & \bar{i} & i & 0 & 1 \\ 0 & 1 & 0 & - & 0 & 0 & i & \bar{i} & 0 & 0 & 0 & 1 & - & 0 & \bar{i} & 0 & i & 0 & \bar{i} & \bar{i} \\ 0 & 0 & 1 & 0 & 0 & 0 & - & 0 & \bar{i} & i & 0 & 0 & i & \bar{i} & 0 & 1 & 0 & i & \bar{i} & i \end{array}\right]$$

GBRD$(9,3,4;Z_4)$

$$\left[\begin{array}{ccc|ccc|ccccccccc} A & I & 0 & B & & & I & I & I & iI & I & I & iI & I & I & iI \\ 0 & A & I & & B & & I & -I & -iI & T & -T & iT & -I & T^2 & iT^2 & T^2 \\ I & 0 & A & & & B & I & iT & T & -T^2 & iI & -I & I & -iT^2 & -T^2 & T \end{array}\right]$$

GBRD$(10,3,4;Z_4)$

$$\left[\begin{array}{ccc|ccc|cc|cccccccc} e & -e & ie & -e & e & -ie & & & & & & & & & \\ I & I & & iI & iI & & A & I & B & & I & I & iI & I & I & iI & I & I \\ I & & I & T^2 & & T^2 & & A\ I & & B & -I & -iT & T & -T & iT & -I & T^2 & iT^2 \\ & I & I & & T & T & I & A & & B & iT & T & -T^2 & iI & -I & I & -iT^2 & -T^2 \end{array}\right]$$

where $A = \begin{bmatrix} & 1 & - \\ - & & 1 \\ 1 & - & \end{bmatrix}$ and $B = \begin{bmatrix} i & 1 & 1 \\ 1 & i & 1 \\ 1 & 1 & i \end{bmatrix}$.

GBRD(15,3,4;Z_4) has blocks with Z_4 = {1,2,3,4}

$1_1\ 2_1\ 3_1$	$1_1\ 6_3\ 8_2$	$2_1\ 3_2\ 4_1$	$2_1\ 8_4\ 14_2$	$3_1\ 5_2\ 11_1$
$1_1\ 2_2\ 4_1$	$1_1\ 6_4\ 9_2$	$2_1\ 3_3\ 11_1$	$2_1\ 9_2\ 10_1$	$3_1\ 5_3\ 12_1$
$1_1\ 2_3\ 5_1$	$1_1\ 7_2\ 10_3$	$2_1\ 3_4\ 12_1$	$2_1\ 9_3\ 13_4$	$3_1\ 5_4\ 15_3$
$1_1\ 2_4\ 6_1$	$1_1\ 7_4\ 11_2$	$2_1\ 4_2\ 5_1$	$2_1\ 9_4\ 15_1$	$3_1\ 6_2\ 11_4$
$1_1\ 3_2\ 7_1$	$1_1\ 8_3\ 12_2$	$2_1\ 4_3\ 12_2$	$2_1\ 10_2\ 13_3$	$3_1\ 6_3\ 14_1$
$1_1\ 3_3\ 8_1$	$1_1\ 8_4\ 13_2$	$2_1\ 5_2\ 6_1$	$2_1\ 10_3\ 14_4$	$3_1\ 6_4\ 15_2$
$1_1\ 3_4\ 9_1$	$1_1\ 9_3\ 14_2$	$2_1\ 5_4\ 15_2$	$2_1\ 10_4\ 15_3$	$3_1\ 7_1\ 11_2$
$1_1\ 4_2\ 10_1$	$1_1\ 9_4\ 15_2$	$2_1\ 6_3\ 7_1$	$2_1\ 11_2\ 12_4$	$3_1\ 7_2\ 13_1$
$1_1\ 4_3\ 11_1$	$1_1\ 10_2\ 11_3$	$2_1\ 6_4\ 12_3$	$2_1\ 11_4\ 14_3$	$3_1\ 7_3\ 14_2$
$1_1\ 4_4\ 12_1$	$1_1\ 10_4\ 12_3$	$2_1\ 7_2\ 8_1$	$2_1\ 11_3\ 15_4$	$3_1\ 8_1\ 12_3$
$1_1\ 5_2\ 13_1$	$1_1\ 11_4\ 13_3$	$2_1\ 7_3\ 13_1$	$3_1\ 4_1\ 6_1$	$3_1\ 8_2\ 13_3$
$1_1\ 5_3\ 14_1$	$1_1\ 12_4\ 14_3$	$2_1\ 7_4\ 14_1$	$3_1\ 4_3\ 10_1$	$3_1\ 8_4\ 14_3$
$1_1\ 5_4\ 15_1$	$1_1\ 13_4\ 15_3$	$2_1\ 8_2\ 9_1$	$3_1\ 4_2\ 15_1$	$3_1\ 9_1\ 10_3$
$1_1\ 6_2\ 7_3$	$1_1\ 14_4\ 15_4$	$2_1\ 8_3\ 13_2$	$3_1\ 5_1\ 10_2$	$3_1\ 9_3\ 14_2$
$3_1\ 9_4\ 14_4$	$4_1\ 9_2\ 14_3$	$5_1\ 8_2\ 11_3$	$6_1\ 9_4\ 14_2$	$8_1 10_1\ 15_1$
$3_1 10_4\ 13_4$	$4_1\ 9_4\ 15_3$	$5_1\ 8_3\ 14_4$	$6_1\ 10_2\ 13_1$	$8_1 11_1\ 15_3$
$3_1 12_4\ 15_4$	$4_1\ 10_2\ 14_4$	$5_1\ 9_1\ 11_2$	$6_1\ 10_3\ 15_4$	$9_1 10_1\ 11_3$
$4_1\ 5_1\ 7_1$	$4_1\ 11_4\ 14_2$	$5_1\ 9_2\ 12_4$	$6_1\ 13_4\ 15_2$	$9_1 11_1\ 12_4$
$4_1\ 5_2\ 8_1$	$4_1\ 8_3\ 11_2$	$5_1\ 9_4\ 13_2$	$7_1\ 8_1\ 9_3$	$10_1 11_4\ 12_1$
$4_1\ 5_3\ 9_1$	$4_1 12_1\ 13_2$	$5_1 13_1\ 14_1$	$7_1\ 8_2\ 12_2$	$10_1 12_2\ 14_4$
$4_1\ 6_2\ 10_1$	$4_1 12_3\ 15_2$	$5_1 14_2\ 15_1$	$7_1\ 8_3\ 15_4$	$10_1 13_3\ 14_1$
$4_1\ 6_4\ 11_1$	$5_1\ 6_1\ 10_1$	$6_1\ 7_1\ 12_1$	$7_1\ 9_2\ 11_1$	$11_1 12_1\ 13_3$
$4_1\ 6_3\ 13_1$	$5_1\ 6_2\ 11_1$	$6_1\ 7_4\ 14_4$	$7_1\ 9_4\ 12_4$	$11_1 13_2\ 14_1$
$4_1\ 7_2\ 13_3$	$5_1\ 6_3\ 12_1$	$6_1\ 8_3\ 11_1$	$7_1\ 9_1\ 15_1$	$11_1 13_1\ 15_1$
$4_1\ 7_3\ 14_1$	$5_1\ 7_2\ 10_4$	$6_1\ 8_1\ 14_1$	$7_1 10_4\ 11_4$	$11_1 14_2\ 15_4$
$4_1\ 7_4\ 15_1$	$5_1\ 7_4\ 12_2$	$6_1\ 8_2\ 15_1$	$7_1 10_1\ 15_3$	$12_1 13_4\ 14_1$
$4_1\ 8_2\ 9_3$	$5_1\ 7_3\ 13_3$	$6_1\ 9_1\ 12_2$	$8_1\ 9_1\ 10_2$	$12_1 13_1\ 15_2$
$4_1\ 8_4\ 13_4$	$5_1\ 8_1\ 10_3$	$6_1\ 9_2\ 13_2$	$8_1 10_4\ 12_2$	$12_1 14_2\ 15_3$

References

[1] W. de Launey and Jennifer Seberry, Generalised Bhaskar Rao designs of block size 4, *Congressus Numerantium* 40, (1984), 229-294.

[2] D.A. Drake, Partial λ-geometries and generalized Hadamard matrices over groups, *Canad. J. Math.*, 31, (1979), 617-627.

[3] Clement Lam and Jennifer Seberry, Generalized Bhaskar Rao designs, *J. Statistical Planning and Inference* 10, (1984), 83-95.

[4] Jennifer Seberry, Regular group divisible designs and Bhaskar Rao designs with block size three, *J. Statistical Planning and Inference* 10, (1984), 69-82.

[5] Deborah J. Street and C.A. Rodger, Some results on Bhaskar Rao designs, *Combinatorial Mathematics VII*. Edited by R.W. Robinson, G.W. Southern and W.D. Wallis, Lecture Notes in Mathematics, Vol. 829, (Springer Verlag, Berlin-Heidelberg, New York), (1980), 238-245.

[6] R.M. Wilson, Construction and uses of pairwise balanced designs, *Combinatorics*. Edited by M. Hall Jr. and J.H. van Lint, (Mathematisch Centrum, Amsterdam), (1975), 18-41.

Non-existence of certain GBRDs

W. de Launey and D. G. Sarvate

1. Introduction and Basic Definitions.

Bhaskar Rao designs have been studied by a number of authors including Bhaskar Rao [1, 2], Seberry [13, 14], Singh [15], Sinha [16], Street [17], Street and Rodger [18] and Vyas [19]. Generalised Bhaskar Rao designs were introduced by Seberry [14], and have subsequently been studied by Lam and Seberry [9], and de Launey and Seberry [3, 4]. In this paper we are concerned with the non-existence and uniqueness of certain generalised Bhasker Rao designs. Such questions fall under the general problem of signing (0,H)- matrices (matrices whose non-zero entries are taken from a group H, 0 does not belong to H) over another group G. A computer program to deal with this problem when H = {1} has been developed by Rudi Mathon [10]. Before proceeding we make two basic definitions.

Definition 1.1. Let G be a group. Let X be a matrix whose non-zero entries are taken from G. Let N be the (0,1)-matrix obtained by replacing every non-zero entry of X by a 1. Then X is a GBRD(v, b, r, k, λ; G) if

(i) $XX^* = rI_v$ over $R(G)/G(R(G))$,

(ii) $NN^T = (r-\lambda)I_v + \lambda J_v$.

Where $R(G)/G(R(G))$ is the group ring, $R(G)$, of the group G over the ring of integers factored out by the ideal $G(R(G)) = [\Sigma g]R(G)$, (where sum is over all $g \in G$), and X^* is obtained from X^T by replacing each non-zero entry by its inverse.

We observe that any GBRD(v, b, r, k, λ; G), X, is therefore based on a BIBD(v, b, r, k, λ), N and hence that the parameters v, b, r, k, λ satisfy the equations

$$\lambda(v-1) = r(k-1) \text{ and } bk = vr. \qquad (1)$$

Because of these equations we write $GBRD(v,k,\lambda;G)$ in place of $GBRD(v,b,r,k,\lambda)$.

On the other hand, one may begin with a $BIBD(v,k,\lambda)$ and replace its non-zero entries by elements of G to obtain a $GBRD(v,k,\lambda;G)$. We generalise and formalise this process in the next definition.

Definition 1.2. Let G and H be groups. Let N be a $(0,H)$-matrix. Suppose the entries, $h \in H$, of N may be replaced by hg, some $g \in G$, so as to produce a $(0,H\times G)$-matrix, X, such that $XX^* = \text{diag}(r_1,r_2,\ldots,r_v)$ over $R(H\times G)/H\times G(R(H\times G))$. Then N is said to be *signable* over G.

We observe that taking the image of each of the entries of X under the homomorphism $hg \to h$ would produce N. Taking the homomorphism $hg \to g$ in the same way would produce a matrix signed over G.

Even when one leaves aside all but matrices based on $BIBD$'s, there is little theory dealing with the signing of $(0,H)$-matrices over a group G. Apart from the use of a non-existence theorem proved by Street and Rodger [18] and Seberry [14, Theorem 1] there is as yet no approach other than an enumerative search when proving the non-existence of $GBRD$'s based on non-symmetric designs. In the case of symmetric designs, Mullin [11] has listed a number of non-existence conditions, while de Launey [5] has proved the following strong multiplicative result.

Theorem 1.3. (de Launey) *Let G' be the commutator subgroup of G. Let p be a prime dividing $|G/G'|$. Let $s = p_1^{k_1},\ldots,p_t^{k_t}$ be the prime decomposition of s, let $n > s$ be odd, and suppose that for some i,*

i) *k_i is odd,*

ii) *there exists a k such that $p_i^k \equiv -1 \pmod p$,*

Then no $SBIBD(n,s,\lambda)$ can be signed over G. □

Even when the matrix is based on a $SBIBD$ where there are a number of strong non-existence theorems, Schellenberg, employing what amounts to an enumerative search in the case of $SBIBD(16,6,2)$ has shown that the theory is deficient [12].

Rudi Mathon has shown by a computer search, that only one of the four $SBIBDS(19,9,4)$ can be signed over Z_2 and that design in only one way. Based on this information one can quickly prove no $GW(19,9,4;Z_2\times Z_2)$ exists (a generalised weighing matrix (GW) is a $GBRD$ with $v = b$). Although this has been proved using the computer program mentioned above we include our simple proof. Again there is no theory ruling out the existence of this design. (The arguments used to prove

Theorem 1.3 do not rule out the existence of this design.)

The main purpose of this paper concerns non-symmetric designs. Two generalised Bhaskar Rao designs, $GBRD(v,k,\lambda;G)$, satisfying (1) and the conditions, $r > k$, $|G| \mid \lambda$, are already known not to exist. These designs are the $GBRD(10,4,2;Z_2)$ and the $GBRD(5,4,6;Z_6)$. It is also proved that the $GBRD(7,4,;Z_2 \times Z_2)$ does not exist. A consequence of the non-existence of these designs is that new small generating sets had to be found in [4] to deal with the question of existence of $GBRD(v,k,\lambda;G)$'s when $k = 4$. One is then forced to construct more designs on more points if one is to successfully apply the Hanani-Wilson theory on PBD's.

In Section 1 we prove and discuss the non-existence of $BRD(10,4,2)$. In Section 2 we show that the $GBRD(5,4,6;Z_2)$ is unique and that this cannot be signed over Z_3. We then deduce that no $GBRD(5,4,6;Z_6)$ exists. In the last section we show that none of the four inequivalent $BIBD(7,4,4)$ can be signed over $Z_2 \times Z_2$ and that the unique $BRD(19,9,4)$ cannot be signed over Z_2. In Section 1,2 and 3 we also give signed $PBD[\{2,3,4\},7,2]$, $PBD[\{3,4\},4,6]$, and $PBD[\{3,4\},6,4]$.

2. Non-Existence of $BRD(10,4,2)$.

In [6] it is proved that if a $BIBD(v,k,2)$ has the parameters of a residual design then it is in fact a residual design. Any $BIBD(10,4,2)$ is therefore a residual design of some $BIBD(16,6,2)$,. Hussain [7] has shown that there are three inequivalent $BIBD(16,6,2)$ and Schellenberg [12] has shown that none of these can be signed over Z_2 to give a Bhaskar Rao design $BRD(16,6,2)$. It is simple to show that a generalised weighting matrix, $GW(v,k,\lambda;G)$, gives a $GBRD(v-k,k-\lambda,\lambda;G)$. In particular a $BRD(\frac{1}{2}k(k-1)+1,k,2)$ gives a $BRD(\frac{1}{2}k(k-3)+1,k-2,2)$. The question therefore arises as to whether the theorem in [6] can be extended to include Bhaskar Rao designs. In proving that no $BRD(10,4,2)$ exists we show that the $BIBD(16,6,2)$ and their residual designs do not rule out the possibility of such an extension.

Peter Gibbons [8], having observed that each of the $BIBD(16,6,2)$ has a transitive automorphism group, proved that there are three inequivalent $BIBD(10,4,2)$. We include these designs in Table 1 below. Noting that, in any attempt to sign these $BIBD$ over Z_2, one can assume that the first element in each row and column has a positive sign, one can quickly check that none of these designs can be signed over Z_2. Seven rows of the second $BIBD(10,4,2)$ may be signed to give the $PBD(\{4,3,2\},7,2)$ below. Such signed designs have a use in connection with supplementary difference sets (also called difference families). Let $a = \pm 1$ in the matrix below.

PBD($\{4,3,2^3\}$, 7, 2)

1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
1	0	-	0	0	0	-	0	0	0	1	1	1	0	0
1	0	0	-	0	0	0	-	0	0	-	0	0	1	1
0	0	1	0	-	0	0	a	$\bar{a}$	0	0	1	0	a	0
0	0	1	-	0	0	0	0	a	$\bar{a}$	0	0	1	0	-
0	1	0	0	-	0	0	0	0	1	$\bar{a}$	0	a	$\bar{a}$	0
0	0	0	0	1	-	a	a	0	0	0	0	a	0	a

Table 1
Three inequivalent *BIBD*(10,4,2)

(a)

1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	1	1	1	1	0	0	0	0	0
1	0	1	0	0	0	1	0	0	0	1	1	1	0	0
1	0	0	1	0	0	0	1	0	0	1	0	0	1	1
0	1	0	0	1	0	0	0	1	0	1	1	0	1	0
0	0	1	0	1	0	0	1	0	1	0	0	1	1	0
0	0	0	1	1	0	1	0	0	1	0	1	0	0	1
0	0	0	1	0	1	1	0	1	0	0	0	1	1	0
0	0	1	0	0	1	0	1	1	0	0	1	0	0	1
0	1	0	0	0	1	0	0	0	1	1	0	1	0	1

(b)

1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	1	1	1	1	0	0	0	0	0
1	0	1	0	0	0	1	0	0	0	1	1	1	0	0
1	0	0	1	0	0	0	1	0	0	1	0	0	1	1
0	0	1	0	1	0	0	1	1	0	0	1	0	1	0
0	0	1	1	0	0	0	0	1	1	0	0	1	0	1
0	1	0	0	0	1	0	0	1	0	1	1	0	0	1
0	1	0	0	1	0	0	0	0	1	1	0	1	1	0
0	0	0	0	1	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	1	0	0	1	0	1	0	1	0

(c)

1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	1	1	1	1	0	0	0	0	0
1	0	1	0	0	0	1	0	0	0	1	1	1	0	0
1	0	0	1	0	0	0	1	0	0	1	0	0	1	1
0	0	1	0	1	0	0	1	1	0	0	1	0	1	0
0	0	1	1	0	0	0	0	1	1	0	0	1	0	1
0	1	0	0	0	1	0	0	1	0	1	0	1	1	0
0	0	0	1	0	1	1	0	0	1	0	1	0	1	0
0	1	0	0	1	0	0	0	0	1	1	1	0	0	1
0	0	0	0	1	1	1	1	0	0	0	0	1	0	1

3. The Uniqueness of the $GBRD(5,4,6;Z_2)$ and the Non-Existence of the $GBRD(5,4,6;Z_6)$.

The proofs in this section amount to exhaustive searches and space does not permit us to give all the details. Our main purpose is to state the results (since they are needed for [4]) and, to include our reasoning and our partitioning of the possibilities, so that the interested reader may, pen in hand, check our procedure. Note that we use '-' in place of '-1'.

We first show that the $GBRD(5,4,6;Z_2)$ is unique. To do this we need only prove that, up to equivalence, the unique $BIBD(5,4,6)$

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1	1	1
1	1	1	1	0	0	1	1	1	1
1	1	1	1	1	1	0	0	1	1
1	1	1	1	1	1	1	1	0	0

can be signed over Z_2 in precisely one way. Without loss of generality we have the following partial array.

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1				
1				0	0				
1						0	0		
1								0	0

The only other possibility is, up to equivalence, the array below.

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	-	1	-	1	-
1	-	1	-	0	0	1	-	-	1
1		-	1	1	-	0	0	-	1
1								0	0

But then position (4,2) cannot be signed. Now we group the possibilities into two not necessarily disjoint classes according to whether they may be brought to the following form.

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	-	-	-
1				0	0	1			
1						0	0		
1								0	0

One obtains the classes below.

Class 1.

0	0	1	1	1	1	1	1	1	1		0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	-	-	-		1	1	0	0	1	1	1	-	-	-
1	1	1	-	0	0	-	1	1	-		1	1	1	-	0	0	-	-	1	1
1						0	0				1						0	0		
1								0	0		1								0	0
				(i)											(ii)					

Class 2.

0	0	1	1	1	1	1	1	1	1		0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	-	-	-		1	1	0	0	1	1	1	-	-	-
1	-	-	-	0	0	1	-	1	1		1	-	-	-	0	0	1	1	1	-
1						0	0				1						0	0		
1								0	0		1								0	0
				(i)											(ii)					

We note that the possibility

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	-	-	-
1	-			0	0	-			
1						0	0		
1								0	0

is accounted for by class 2. (Multiply row 3 by -1 and swap the first and second columns). Class 2 also accounts for the possibilities in Class 1. If a design is in Class 1 (ii) then applying the 'signed' permutation $(\bar{1},\bar{5},\bar{3},\bar{2},\bar{6},4)$ $(\bar{7},8)$ to its columns, the 'signed' permutation $(1,\bar{3},\bar{2})$ to its rows (and possibly negating rows 4 and 5) will produce a design in Class 2 (i). Using the permutations $(\bar{1},\bar{5},\bar{3},\bar{2},\bar{6},4)$ $(\bar{7},10)$ $(8,9)$ and $(1,\bar{3},\bar{2})$ $(4,5)$ with rows 4 or 5 possibly negated will convert Class 1 (i) to Class 2 (ii). We now deal with the possible designs which contain one of the two configurations in Class 2.

It can be shown quickly that if the first three rows are signed as in Class 2 (i) then the fourth cannot be signed. Hence no designs fall in Class 2 (i). According to whether the (4,2) position is 1 or -1, matrices falling in Class 2 (ii) are signed as below.

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	-	-	-
1	-	-	-	0	0	1	1	-	1
1	1	1	1	-	-	0	0	-	1
1								0	0

(a)

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	-	-	-
1	-	-	-	0	0	1	1	-	1
1	-	1	-	1	-	0	0	1	-
1								0	0

(b)

Possibility (a) cannot be completed but possibility (b) has the two completions below.

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	-	-	-
1	-	-	-	0	0	1	1	-	1
1	-	1	-	1	-	0	0	1	-
1	1	1	-	-	1	-	1	0	0

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	-	-	-
1	-	-	-	0	0	1	1	-	1
1	-	1	-	1	-	0	0	1	-
1	1	-	1	1	-	-	1	0	0

The second matrix may be converted to the first by applying the 'signed' permutations $(\bar{1})$ (3,5,4,6) (7,9) (8,10) and $(\bar{2},\bar{3})$ $(\bar{4},\bar{5})$ to the columns and rows respectively. This completes the proof of the uniqueness of $GBRD(5,4,6;Z_2)$.

We now show this design cannot be signed over Z_3. Let $X = (x_{ij})$ be a possible signing of the above matrix. We may assume $x_{2,10} = -^1$ while $x_{22} = 1^1$ and $x_{i1} = x_{1j} = 1^1$ for $i = 1,2,...,5$, $j = 3,4,...,10$. If $x_{2,10} \neq -^1$ multiply row 2 by a suitable group element and then adjust the rest of the matrix. Once the design is signed, the elements of Z_3 can be squared to obtain another signing of the design over Z_3. Thus we can force $x_{28} = -^w$. The entries x_{37}, x_{38}, x_{39}, and x_{29} are then forced. The rest of our proof is summarized in Table 2, below. The purpose of the table is to give a partition of the possibilities which the reader may work through to complete the proof. For each case the maximal sets of signed rows are given. The proof is complete when these sets are shown to be the only maximal sets.

0	0	1^1	1^1	1^1	1^1	1^1	1^1	1^1	1^1
1^1	1^1	0	0	1	1	1	$-^w$	$-^{w^2}$	$-^1$
1^1	-	1	1	0	0	$-^1$	$-^{w^2}$	$-^w$	1
1^1	-	1	-	-	1	0	0	1	-
1^1	1	-	1	-	1	-	1	0	0

Table 2

$x_{32} = -^1, x_{27} = 1^w$

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1^w	$-^w$	$-^{w^2}$	$-^1$
1	$-^1$	1^{w^2}	1^1	0	0	$-^1$	$-^{w^2}$	$-^w$	1^w

$x_{33} = 1^{w^2}$

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1^1	1^{w^2}	1^w	$-^w$	$-^{w^2}$	$-^1$
1	$-^1$	1^1	1^{w^2}	0	0	$-^1$	$-^{w^2}$	$-^w$	1^w
1	$-^w$	1^{w^2}	$-^w$	$-^1$	1^1	0	0	1^w	$-^{w^2}$

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1^{w^2}	1^1	1^w	$-^w$	$-^{w^2}$	$-^1$
1	$-^1$	1^1	1^{w^2}	0	0	$-^1$	$-^{w^2}$	$-^w$	1^w
1	$-^{w^2}$	1^w	$-^1$	$-^{w^2}$	1^{w^2}	0	0	1^1	$-^w$

$x_{33} = 1^1$

$x_{32} = -^1, x_{27} = 1^{w^2}$

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1^1	1^w	1^{w^2}	$-^w$	$-^{w^2}$	$-^1$
1	$-^1$	1^1	1^w	0	0	$-^1$	$-^{w^2}$	$-^w$	1^{w^2}
1	$-^w$	1^{w^2}	$-^{w^2}$	$-^1$	1^1	0	0	1^w	$-^w$

$x_{33} = 1^1$

0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1^1	1^{w^2}	$-^w$	$-^{w^2}$	$-^1$
1	$-^1$	1^w	1^1	0	0	$-^1$	$-^{w^2}$	$-^w$	1^{w^2}

$x_{33} = 1^w$

$$\begin{array}{cccccccccc} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1^{1} & -^{w} & -^{w^2} & -^{1} \\ 1 & -^{w} & 1^{1} & 1^{w} & 0 & 0 & -^{1} & -^{w^2} & -^{w} & 1^{w^2} \end{array}$$

$$x_{33} = 1^{1}$$

$$\begin{array}{cccccccccc} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1^{w} & 1^{w^2} & 1^{1} & -^{w} & -^{w^2} & -^{1} \\ 1 & -^{w} & 1^{w} & 1^{1} & 0 & 0 & -^{1} & -^{w^2} & -^{w} & 1^{w^2} \\ 1 & -^{w^2} & 1^{1} & -^{1} & -^{w^2} & 1^{w} & 0 & 0 & 1^{w^2} & -^{w} \end{array}$$

$$x_{33} = 1^{w}$$

$$x_{32} = -^{w},\ x_{27} = 1^{w}$$

$$\begin{array}{cccccccccc} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1^{w} & -^{w} & -^{w^2} & -^{1} \\ 1 & -^{w} & 1^{w^2} & 1^{w} & 0 & 0 & -^{1} & -^{w^2} & -^{w} & 1^{1} \end{array}$$

$$x_{33} = 1^{w^2}$$

$$\begin{array}{cccccccccc} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1^{1} & 1^{w^2} & 1^{w} & -^{w} & -^{w^2} & -^{1} \\ 1 & -^{w} & 1^{w} & 1^{w^2} & 0 & 0 & -^{1} & -^{w^2} & -^{w} & 1^{1} \\ 1 & -^{1} & 1^{w^2} & -^{1} & -^{w} & 1^{1} & 0 & 0 & 1^{w} & -^{w^2} \end{array}$$

$$x_{33} = 1^{w}$$

$$x_{32} = -^{w},\ x_{27} = 1^{1}$$

$$\begin{array}{cccccccccc} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1^{1} & -^{w} & -^{w^2} & -^{1} \\ 1 & -^{w} & 1^{1} & 1^{w} & 0 & 0 & -^{1} & -^{w^2} & -^{w} & 1^{w^2} \end{array}$$

$$x_{33} = 1^{1}$$

$$
\begin{array}{cccccccccc}
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 1^{w} & 1^{w^2} & 1^{1} & -^{w} & -^{w^2} & -^{1} \\
1 & -^{w} & 1^{w} & 1^{1} & 0 & 0 & -^{1} & -^{w^2} & -^{w} & 1^{w^2} \\
1 & -^{w^2} & 1^{1} & -^{1} & -^{w^2} & 1^{w} & 0 & 0 & 1^{w^2} & -^{w}
\end{array}
$$

$x_{33} = 1^{w}$

$x_{32} = -^{w^2}$, $x_{27} = 1^{w^2}$

$$
\begin{array}{cccccccccc}
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 1^{1} & 1^{w} & 1^{w^2} & -^{w} & -^{w^2} & -^{1} \\
1 & -^{w^2} & 1^{w} & 1^{w^2} & 0 & 0 & -^{1} & -^{w^2} & -^{w} & 1^{1} \\
1 & -^{1} & 1^{1} & -^{1} & -^{w} & 1^{w^2} & 0 & 0 & 1^{w} & -^{w^2}
\end{array}
$$

$x_{33} = 1^{w}$

$$
\begin{array}{cccccccccc}
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 1^{w} & 1^{1} & 1^{w^2} & -^{w} & -^{w^2} & -^{1} \\
1 & -^{w^2} & 1^{w^2} & 1^{w} & 0 & 0 & -^{1} & -^{w^2} & -^{w} & 1^{1} \\
1 & -^{w} & 1^{1} & -^{w} & -^{1} & 1^{w} & 0 & 0 & 1^{w^2} & -^{w^2}
\end{array}
$$

$x_{33} = 1^{w^2}$

---

4. Signing Certain *BIBD*'s over Z_2 or $Z_2 \times Z_2$.

In this section we will observe that all four *BIBD*(7,4,4) can be signed over Z_2. Then we will show that these designs cannot be signed over $Z_2 \times Z_2$. But before doing so we will prove that the *BRD*(19,9,4), found by Rudi Mathon cannot be signed over Z_2. The following design, $X = (x_{ij})$, is the *BRD*(19,9,4) in question. (Signed over Z_2)

	1	1	1	1	1	1	1	1	1								
1		1	1	-			-						-	1		1	-
1	1		1		-			-					1		-	-	1
1	1	1				-			-				-	1		1	-	
1	-	-			1	1	-				1	-					-	1
1		-		1		1		-		-		1				1		-
1			-	1	1				-	1	-					-	1	
1	-			-				1	1		-	1		1	-			
1		-			-		1		1	1		-	-		1			
1			-			-	1	1		-	1		1	-				
					-	1		1	-	1				-	-		-	-
				1		-	-		1		1		-		-	-		-
				-	1		1	-				1	-	-		-	-	
		1	-					-	1		-	-	1				-	-
	-		1				1		-	-		-		1		-		-
	1	-					-	1		-	-				1	-	-	
		-	1		1	-					-	-		-	-	1		
	1		-	-		1				-		-	-		-		1	
	-	1		1	-					-	-		-	-				1

In attempting to sign over . . .

Z_2, we observe that either $x_{2,15}$ and $x_{4,15}$ are signed differently, or $x_{2,18}$ and $x_{4,18}$ are signed differently. At the same time either $x_{2,15}$ and $x_{4,15}$ are signed the same or $x_{2,18}$ and $x_{4,18}$ are signed the same. Without loss of generality we may suppose the first pair are signed differently and the second are signed the same. Because we may suppose the non-zero entries in column 1 are all signed the same, we have that $x_{8,15}$ and $x_{10,15}$ are signed differently and $x_{5,18}$ and $x_{7,18}$ are signed the same. This forces $x_{5,12}$ and $x_{7,12}$ to be signed differently and this forces $x_{8,12}$ and $x_{10,12}$ to be signed differently giving a contradiction. Given that X is the only $BRD(19,9,4)$ there is therefore no $GW(19,9,4;Z_2\times Z_2)$.

We now consider the $BIBD(7,4,4)$ designs. The four inequivalent $BIBD(7,4,4)$ can be signed over Z_2 as follows.

1	1	1	1	1	1	1	1								
1	1	-			-				-	1		-	1		
1	1		-			-		1		-	1		-		
1	1			-			-	-	1		-	1			
			-	1		1	1		1	1		1	1		(i)
		1		-	1	-		1	1		-		-		
		-	1		-		1	1		1	-	-			

1	1	1	1	1	1	1	1								
1	1	-			-				-	1		-	1		
1	1		-			-		1		-	1		-		
1	1			-			-	-	1		-	1			
			-	1		-	1		1	1		1	1		(ii)
		1		-	1		-	1		1	1		1		
		-	1		-	1		1	1		1	1			

1	1	1	1	1	1	1	1								
1	1	-			-				1	1		1	1		
1	1		-			-		1				-	1		
1	1			-			-	-	-		-	-			
			1	-	1		-	1		1		1	-		(iii)
		1		-	1	-		-	1		1		1		
		1	-			1	-		1	-	-	1			

1	1	1	1	1	1	1	1								
1			-	1	-				-	1		1	1		
1		1		-		-		1		-	1		1		
1		-	1				-	-	1		1	1			
	1	-			-	1		1	1			-	1		(iv)
	1		-			-	1		1	1	1		-		
	1			-	1		-	1		1	-	1			

We now turn our attention to the question of signing these *BIBD* over $Z_2 \times Z_2$. To begin with we make a definition and prove a simple lemma.

Definition 4.1. Let $x,y \in Z_2 \times Z_2$. We say the *ratio* of x and y is xy. Let $r(x,y)$ denote the ratio of x and y. We note that $r(x,y) = r(y,x)$.

Lemma 4.2. *Let* $A = [a_1,a_2,a_3,a_4]$ *and* $B = [b_1,b_2,b_3,b_4]$ *with* $a_i,b_i \in Z_2 \times Z_2$ *for all* $1 \le i \le 4$. *Suppose* $\{a_1b_1,a_2b_2,a_3b_3,a_4b_4\} = Z_2 \times Z_2$. *Then we have:*

(i) $r(a_1,a_2)r(b_1,b_2) = r(a_3,a_4)r(b_3,b_4)$,

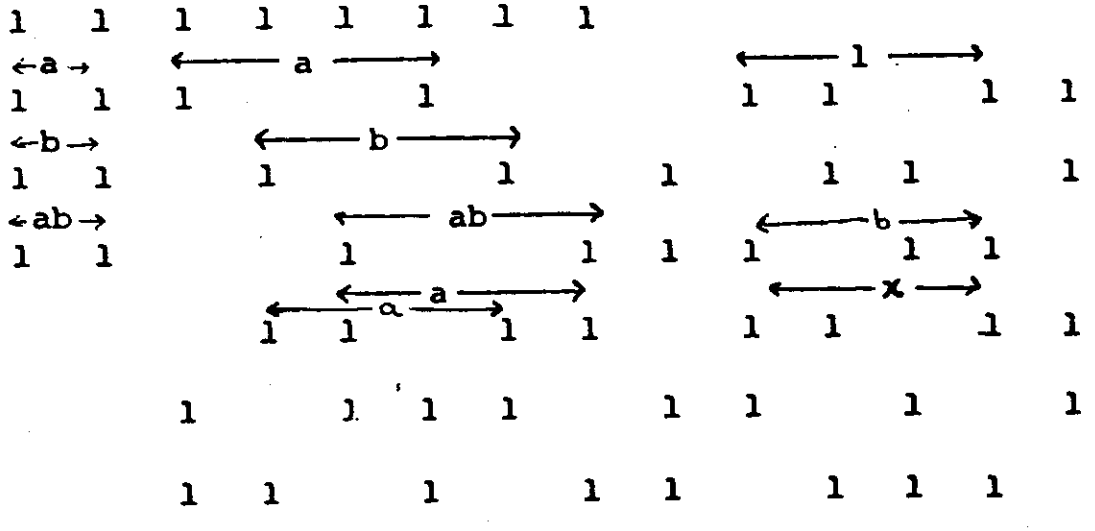
(ii) $r(a_1,a_2) \neq r(b_1,b_2)$ *and* $r(a_3,a_4) \neq r(b_3,b_4)$.

Proof. (i) We note $a_1b_1\ a_2b_2\ a_3b_3\ a_4b_4 = 1$.

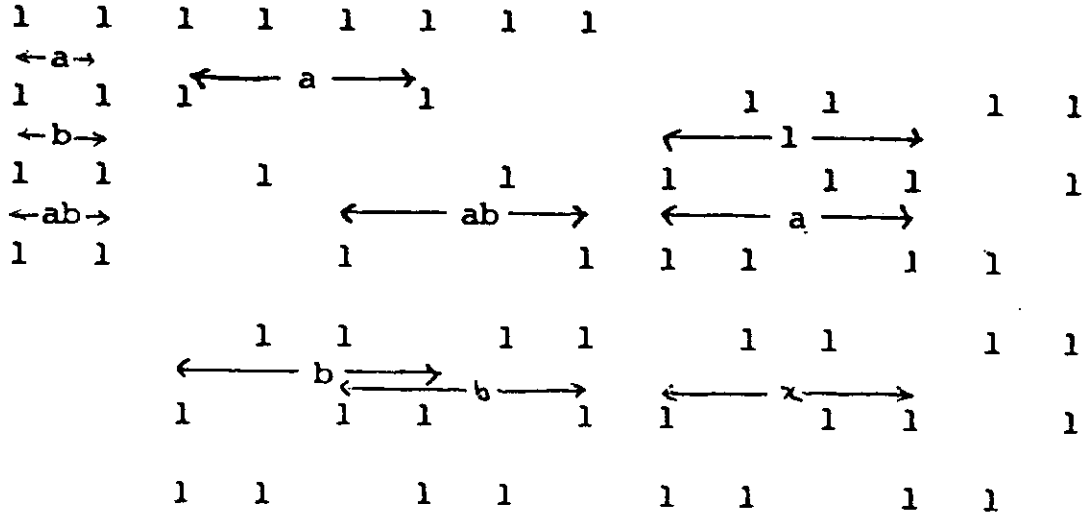
(ii) $r(a_1,a_2) = r(b_1,b_2)$, say, then $a_1b_1 = a_2b_2$, giving a contradiction. □

This lemma allows us to show quickly that two of the four inequivalent designs cannot be signed over $Z_2 \times Z_2$. Suppose the designs below can be signed over $Z_2 \times Z_2$. Then without loss of generality we would have the ratios as shown in the matrices below. The labelled arrow denotes the ratio of the signed entries under the arrow head. The signed entries are not shown, because the proof requires the ratios only.

(a)



(b)



In both cases no value $x \in Z_2 \times Z_2$ can be found to satisfy all the requirements imposed by Lemma 4.2 and the structure of the matrix concerned.

This shows designs (i) and (ii) cannot be signed over $Z_2 \times Z_2$. One of the authors has carried out an exhaustive computer search for a signing over $Z_2 \times Z_2$ of either one of the remaining designs. Such a search has produced no such signing. Hence these designs cannot be signed either. The search has produced several sets of six rows signed over $Z_2 \times Z_2$. Thus we have $PBD[\{4,3\},6,4]$ which can be signed over $Z_2 \times Z_2$. An example for each of designs (iii) and (iv) is included below.

e	e	e	e	e	e	e	e							
e	a	b			ab				e	e		e	e	
e	b		ab			a		e		a	e		b	
e	ab			b			a	ab	a		b	ab		
		e	b			ab	a		ab	a				
		e		a	ab	b		b	a		e		ab	

six rows of *BIBD*(7,4,4) (iii)

e	e	e	e	e	e	e	e							
e			a	b	ab				e	e		e	e	
e		b		a		ab		e		b	e		a	
e		ab	b		b		a	b	b		ab	a		
		a				ab		b	ab			b	e	
			ab			a	b		e	ab	ab		a	

six signed rows of *BIBD*(7,4,4) (iv).

In all there are 8 sets of signed six rows of design (iii) and only 2 sets of signed six rows for design (iv).

Acknowledgement: We wish to thank Dr. Jennifer Seberry for her valuable help and encouragement.

References.

[1] M. Bhaskar Rao, *Group divisible family of PBIB designs*, J. Indian Stat. Assoc., 4 (1966), 14-28.

[2] M. Bhaskar Rao, *Balanced orthogonal designs and their application in the construction of some BIB and group divisible designs*, Sankhya (A), 32 (1970), 439-448.

[3] W. de Launey and J. Seberry, *Bhaskar Rao designs of block size 4*, Proceedings of the Calcutta Conference, 1982, (to appear).

[4] W. de Launey and J. Seberry, *Generalized Bhaskar Rao designs of block size 4*, Congressus Numerantium, Vol. 41 (1984) 229-294.

[5] W. de Launey, *Non existence of generalised weighing matrices*, Ars Combinatoria, Vol. 17A (1984) 117-132.

[6] Marshall Hall Jr., *Combinatorial Theory*, Blaisdell, Waltham, Mass., 1967.

[7] Q.M. Hussain, *On the totality of the solutions for the symmetrical incomplete block designs* $\lambda = 2$, $k = 5$ *or* 6, Sankhya, Vol. 7, Part 2, pp. 204-208 (1945).

[8] Peter Gibbons, *Computing Techniques for the Construction and Analysis of Block Designs*, Ph.D. Dissertation, University of Toronto, 1975.

[9] C. Lam and J. Seberry, *Generalised Bhaskar Rao designs*, J. of Statistical Planning and Inference 10 (1984) 83-95.

[10] Rudi Mathon, Private Communication, 1983.

[11] R.C. Mullin, *A note on balanced weighing matrices*, Combinatorial Mathematics III, ed. Anne Penfold Street and W.D. Wallis, Lecture Notes in Mathematics, Vol. 452,

Springer Verlag, Berlin-Heidelberg-New York, (1974), 28-41.

[12] Paul J. Schellenberg, *A computer construction for balanced orthogonal matrices*, Proceedings of the Sixth South Eastern Conference on Combinatorics, Graph Theory, and Computing, Congressus Numerantium XIV, Utilitas Math., (1975), 513-522.

[13] J. Seberry, *Regular group divisible designs and Bhaskar Rao designs with block size three*, J. Statistical Planning and Inference 10 (1984) 69-82.

[14] J. Seberry, *Some families of partially balanced incomplete block designs*, Combinatorial Mathematics IX, edited by E.J. Billington, Sheila Oates - Williams and A.P. Street, Lecture Notes in Mathematics, Vol. 952, Springer Verlag, Berlin-Heidelberg-New York, (1981).

[15] S.J. Singh, *Some Bhaskar Rao designs and application for* $k = 3$, $\lambda = 2$, University of Indore Research J. Science 7 (1982), 8-15.

[16] K. Sinha, *Partially balanced incomplete block designs and partially balanced weighing designs*, Ars Combinatoria, 6 (1978), 91-96.

[17] D.J. Street, *Bhaskar Rao designs from cyclotomy*, J. Austral. Math. Soc., 29 (A) (1981), 425-430.

[18] D.J. Street and C.A. Rodger, *Some results on Bhaskar Rao designs*, Combinatorial Mathematics, VII, edited by R.W. Robinson, G.W. Southern and W.D. Wallis, Lecture Notes in Mathematics, Vol. 829, Springer Verlag, Berlin-Heidelberg-New York (1980), 238-245.

[19] R. Vyas, *Some Bhaskar Rao designs and applications for* $k = 3$, $\lambda = 4$, University of Indore Research J. Science 7 (1982), 16-25.

Department of Applied Mathematics
University of Sydney
N.S.W. 2006
Australia

7.2 Orthogonal designs

A joint paper with J. Hammer and J. Seberry is attached:

"A note on orthogonal designs" (preprint).

In this paper a construction of weighing matrices, given by Kharaghani (1985), is extended and some new constructions for weighing matrices, orthogonal design and Hadamard matrices are obtained. About one third of the work is done by this author.

A Note on Orthogonal Designs

J. Hammer, D.G. Sarvate, Jennifer Seberry

1. Introduction

Let $W = [w_{ij}]$ be a matrix of order n with $w_{ij} \in \{0,1,-1\}$. W is called a *weighing matrix* of weight p and order n, if $WW^T = W^TW = pI_n$, where I_n denotes the identity matrix of order n. Such a matrix is denoted by W(n,p). If squaring all its entries gives an incidence matrix of a SBIBD then W is called a *balanced* weighing matrix.

An *orthogonal design* (OD), say A, of order n and type $(s_1, s_2, ..., s_t)$ on the commuting variables $(\pm x_1, ..., \pm x_t)$ and 0, is a square matrix of order n with entries from $(\pm x_1, ..., \pm x_t)$ and 0. Each row and column of A contains s_k entries equal to x_k in absolute value, the remaining entries in each row and column being equal to 0. Any two distinct rows of A are orthogonal. In other words

$$AA^T = (s_1x_1^2 + ... + s_tx_t^2) I_n .$$

An Hadamard matrix $W = [w_{ij}]$ is a $W(n, n)$ i.e. it is a square matrix of order n with entries $w_{ij} \in \{1, -1\}$ which satisfies

$$WW^T = W^TW = n I_n$$

OD's have been used to construct new Hadamard matrices. For details see Geramita and Seberry (1979).

Kharaghani(1985) defined $C_k = [w_{ki}.w_{kj}]$ and with that obtained skew symmetric and symmetric $W(n^2+sn,p^2)$ from $W(n,p)$, where s is any positive integer such that n+s is even. Each C_k is a symmetric $\{0, 1, -1\}$ matrix of order n. We define C_k by the Kronecker product and by extending Kharaghani's method we obtain some new constructions of weighing matrices and orthogonal designs.

2. Some properties of C_k's

The C_k's can be defined as a Kronecker product of the k^{th} row of W with its transpose. In other words, if R_k denotes the k^{th} row of W, then $C_k = R_k \times R_k^T$. Similarly, we define C_k's corresponding to the OD, A , as follows:

Let U be a weighing matrix obtained from A by replacing all the variables of A by 1. Let A_k and U_k denote the k^{th} rows of A and U respectively. Then $C_k = A_k \times U_k^T$.

LEMMA 2.1 : Let V_i be the ith row of an SBIBD(v, p, λ). Consider

$$X = [V_1 \times V_1^T , \ldots , V_n \times V_n^T]$$

then

$$XX^T = p((p-\lambda)I + \lambda J).$$

PROOF: $X X^T = V_1 V_1^T \times V_1^T V_1, \ldots , V_n V_n^T \times V_n^T V_n$

$$= p\sum_i V_i^T V_i$$
$$= p((p-\lambda)I + \lambda J).$$

□

COROLLARY 2.2: *Given a balanced* W(n,p), *based on an* SBIBD(n,p,λ), *consider*

$$X = [\, C_1' : C_2' : \ldots C_n' \,]$$

where C_i' *is obtained from* C_i *by squaring all its entries. Then the inner product of any two distinct rows of X is* λp.

PROOF Observe that $C_i' = V_i \times V_i^T$.

□

3. A new construction of orthogonal designs

Many constructions in orthogonal design theory have been expressed in terms of Kronecker products of matrices: for example see Gastineau-Hills(1983) and Gastineau-Hills and Hammer(1983). The Kronecker product of two or more designs is not in general a design since products of variables appear, for example:

$$\begin{bmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{bmatrix} \times \begin{bmatrix} y_1 & y_2 \\ y_2 & -y_1 \end{bmatrix} = \begin{bmatrix} x_1y_1 & x_2y_1 & x_1y_2 & x_2y_2 \\ -x_2y_1 & x_1y_1 & -x_2y_2 & x_1y_2 \\ x_1y_2 & x_2y_2 & -x_1y_1 & -x_2y_1 \\ -x_2y_2 & x_1y_2 & x_2y_1 & -x_1y_1 \end{bmatrix} = \begin{bmatrix} z_1 & z_2 & z_3 & z_4 \\ -z_2 & z_1 & -z_4 & z_3 \\ z_3 & z_4 & -z_1 & -z_2 \\ -z_4 & z_3 & z_2 & -z_1 \end{bmatrix}$$

(where $z_1 = x_1y_1$, $z_2 = x_2y_1$, $z_3 = x_1y_2$, $z_4 = x_2y_2$) is not orthogonal, if we take z_1, z_2, z_3 and z_4 as independent. However it is a different matter if we take a Kronecker product of an OD with a weighing matrix.

A construction of Kharaghani can be extended to give the following result:

THEOREM 3.1. *If there exists an* OD, A , *of type* $(s_1, s_2, \ldots, s_r)$, *where*

$$w = \sum_{k=1}^{r} s_k,$$

and order n on the variables $(\pm x_1, \ldots, \pm x_r, 0)$ *then there exist n matrices* $C_1, \ldots, C_n$ *of order n satisfying*

$$\sum_{i=1}^{n} C_i C_i^T = \sum_{k=1}^{r} s_k w x_k^2 I_n$$

$$C_k C_j^T = 0, \; k \neq j.$$

PROOF. Let $A = (a_{ij})$ be the OD. Replace all the variables of A by 1 making it a (0, 1, -1) weighing matrix $U = (u_{ij})$ of order n and weight w. Write A_k and U_k for the k^{th} rows of A and U respectively. Form

$$C_k = A_k \times U_k^T.$$

Then

$$C_k C_j^T = (A_k \times U_k^T)(A_j \times U_j^T)^T$$

$$= (A_k A_j^T \times U_k^T U_j)$$

$$= 0 \qquad \text{if } k \neq j \text{ because A is an orthogonal design.}$$

Now

$$\sum_{k=1}^{n} C_k C_k^T = \sum_{k=1}^{n} (A_k \times U_k^T)(A_k^T \times U_k)$$

$$= \sum A_k A_k^T \times U_k^T U_k$$

$$= \sum s_j x_j^2 (\Sigma U_k^T U_k)$$

$$= \sum s_j x_j^2 (w I_n) \quad \text{by the properties of U.}$$

□

EXAMPLE 3.2. Let

$$A = \begin{bmatrix} -a & b & c & -d \\ b & a & d & c \\ c & -d & a & -b \\ -d & -c & b & a \end{bmatrix} ; U = \begin{bmatrix} -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$$

Then

$$C_1 = \begin{bmatrix} a & -a & -a & a \\ -b & b & b & -b \\ -c & c & c & -c \\ d & -d & -d & d \end{bmatrix}^T , C_2 = \begin{bmatrix} b & b & b & b \\ a & a & a & a \\ d & d & d & d \\ c & c & c & c \end{bmatrix}^T$$

$$C_3 = \begin{bmatrix} c & -c & c & -c \\ -d & d & -d & d \\ a & -a & a & -a \\ -b & b & -b & b \end{bmatrix}^T , C_4 = \begin{bmatrix} d & d & -d & -d \\ c & c & -c & -c \\ -b & -b & b & b \\ -a & -a & a & a \end{bmatrix}^T .$$

Thus we have

THEOREM 3.3. *Suppose there exists an* $OD(s_1, \ldots, s_r)$, *where* $w = \Sigma s_i$, *of order n. Then there exists an* $OD(s_1w, s_2w, \ldots, s_rw)$ *of order* $n(n+k)$ *for* $k \geq 0$ *an integer.*

PROOF. Form $C_1, \ldots, C_n$ as in the previous theorem. Form a Latin square of order $n+k$ and replace n of its elements by $C_1, \ldots, C_n$ and the other elements by the $n \times n$ zero matrix.

□

For instance, using Theorem 3.3 we can construct an OD(4, 4, 4, 4) of order $4n$, for $n \geq 4$. Using inequivalent Latin squares in Theorem 3.3 will yield inequivalent ODs.

COROLLARY 3.4. *If there is an* OD(t, t, t, t) *in order 4t, then there is an* OD($4t^2$, $4t^2$, $4t^2$, $4t^2$) *in every order* $4t(4t+k)$, $k \geq 0$ *an integer.*

But this construction can be used in other ways.

EXAMPLE 3.5. Write 1, 2, 3, 4 for $C_1, \ldots, C_4$. Define

$$A_1 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 4 & 2 & 3 \\ 3 & 4 & 2 \\ 2 & 3 & 4 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 3 & 1 & 4 \\ 1 & 4 & 3 \\ 4 & 3 & 1 \end{bmatrix}, \quad A_4 = \begin{bmatrix} 2 & 1 & 4 \\ 1 & 4 & 2 \\ 4 & 2 & 1 \end{bmatrix}.$$

Then $A_k A_j^T = A_j A_k^T$. Thus A_1, A_2, A_3, A_4 can be used to replace the variables of any OD(t, t, t, t).

□

Hence we have:

THEOREM 3.6. *Suppose there is an* OD(t, t, t, t) *in order n. Then there exists an* OD(12t, 12t, 12t, 12t) *in order 12n.*

PROOF. Use the OD(1, 1, 1, 1) in order 4 to form $C_1, \ldots, C_4$ of order 4. Substitute these in $A_1, \ldots, A_4$ of Example 3.5 to obtain Williamson-type matrices of order 12, on 4 variables each repeated 12 times. Use these to replace the variables of the OD(t, t, t, t) to get the result.

□

Now if we had started to construct $C_1, \ldots, C_{4s}$ of order 4s from an OD(s,s,s,s) in order 4s we would have each of 4 variables occuring $4s^2$ times in each row of $[C_1 : C_2 : \ldots : C_{4s}]$. But we can use these to form Williamson type matrices in a number of ways:

Let A_i, be a circulant matrix with first row (i+1, i+2, ..., i+s), i = 0, s, 2s, and 3s. These four matrices can be substituted in an OD(t ,t, t, t). Hence we have:

THEOREM 3.7. *If there exists an* OD(s, s, s, s) *in order 4s and an* OD(t, t, t, t) *in order 4t, then there exists an* OD($4s^2t$, $4s^2t$, $4s^2t$, $4s^2t$) *in order* $16s^2t$.

Now if we write i for B_i we can proceed exactly as in Example 3.5 so we have

THEOREM 3.8. *If there exists an* OD(s, s, s, s) *in order 4s and an* OD(t, t, t, t) *in order 4t, then there exists an* OD($12s^2t$, $12s^2t$, $12s^2t$, $12s^2t$) *in order* $48s^2t$.

□

Consider the OD(5, 5, 5, 5) in order 20. The construction gives $C_1, C_2, \ldots, C_{20}$ of order 20 and hence an OD(300, 300, 300, 300) in order 1200.

EXAMPLE 3.10. We suppose as before that 1,2,3,4 are matrices of order n such that $ij^T = 0$ and $\Sigma\, ii^T = \Sigma\, nx_i^2 I_n$.

Define

$$A_1 = \begin{bmatrix} 3 & 1 & 2 & -2 & 1 \\ 1 & 3 & 1 & 2 & -2 \\ -2 & 1 & 3 & 1 & 2 \\ 2 & -2 & 1 & 3 & 1 \\ 1 & 2 & -2 & 1 & 3 \end{bmatrix}, \qquad A_2 = \begin{bmatrix} 1 & 3 & 4 & -4 & 3 \\ 3 & 1 & 3 & 4 & -4 \\ -4 & 3 & 1 & 3 & 4 \\ 4 & -4 & 3 & 1 & 3 \\ 3 & 4 & -4 & 3 & 1 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 4 & 1 & 2 & 2 & -1 \\ 1 & 2 & 2 & -1 & 4 \\ 2 & 2 & -1 & 4 & 1 \\ 2 & -1 & 4 & 1 & 2 \\ -1 & 4 & 1 & 2 & 2 \end{bmatrix}, \qquad A_4 = \begin{bmatrix} 2 & 3 & 4 & 4 & -3 \\ 3 & 4 & 4 & -3 & 2 \\ 4 & 4 & -3 & 2 & 3 \\ 4 & -3 & 2 & 3 & 4 \\ -3 & 2 & 3 & 4 & 4 \end{bmatrix}.$$

Then $A_iA_j^T = A_jA_i^T$ and $\Sigma\, A_iA_i^T = \Sigma\, 5x_i^2 I_{5n}$.

Thus if B_i are as described after Theorem 3.7 we have

THEOREM 3.11. *Suppose there is an* OD(s, s, s, s) *in order 4s and an* OD(t, t, t,t) *in order 4t. Then there is an* OD($20s^2t$, $20s^2t$, $20s^2t$, $20s^2t$) *in order* $80s^2t$.

4. Method used to form inequivalent Hadamard matrices

CONSTRUCTION 4.1. Let H be Hadamard of order n. Form C_i, i = 1,2, ... , n, from H as before. Let L and M be Hadamard matrices of order t. Then

$$(L \times C_i)\,(M \times C_j) = 0,\ i \neq j.$$

So if H_1, ... , H_n are Hadamard matrices of order t (inequivalent or just different equivalence operations applied to one) then the matrices

$$H_{i_1} \times C_1,\ H_{i_2} \times C_2, \ldots H_{i_n} \times C_n\ ,\ i_j \in \{1,2, \ldots , n\}$$

can be put into a Latin square of order n to form Hadamard matrices of order n^2t. The method can give many inequivalent Hadamard matrices. For example, if there are s inequivalent Hadamard matrices of order t and m inequivalent Latin squares of order n, then there will be at least s^{n+1} inequivalent Hadamard matrices of ordr n^2t. This method can be generalized to produce inequivalent weighing matrices and orthogonal designs.

5. Method used with coloured designs to form rectangular weighing matrices.

In a recent paper Rodger, Sarvate and Seberry (1987) have studied coloured BIBDs showing every BIBD can be coloured. By definition a coloured BIBD is the incidence matrix of the BIBD(v, b, r, k, λ) whose nonzero entries are replaced by r fixed symbols such that each row and column has no repeated symbol. Consider a coloured symmetric BIBD(v,k, λ) and a W(k, p). If we replace the i^{th} symbol by C_i for i = 1,2, ... , k and the 0 entries by the k by k zero matrix, we get W(vk, p^2). In general, if we consider a coloured BIBD(v, b, r, k, λ) and there exists a weighing matrix W(r, p) then we form the C_i, i = 1, ... , r and replace the i^{th} colour by C_i and zeros by the zero matrix of order r. This matrix, B, has size vr x vr, rp

nonzero elements in each row and pk non-zero elements in each column. Hence we have:

THEOREM 5.1. *Suppose there is a* BIBD (v, b, r, k, λ) *and a* W(r, p). *Then there is a* (0, 1, -1) *matrix B with rp nonzero elements in each row and pk nonzero elements in each column such that*

$$BB^T = rpI.$$

In particular, if the BIBD *is symmetric then we have a* $W(vk,p^2)$.

□

Remark. If we replace entries of an n-dimensional latin cube by suitable C_i's then we will get n-dimensional orthogonal designs.

References:

H. M. Gastineau-Hills (1983), Kronecker products of systems of orthogonal designs, *Combinatorial Mathematics* X, Proceedings, Adelaide 1982, edited by L.R.A. Casse, Lecture Notes in Mathematics, **1036** Springer-Verlag, Berlin, Heidelberg, New York, Tokyo,189-205.

H. M. Gastineau-Hills and J. Hammer (1983), Kronecker products of systems of higher dimensional orthogonal designs, *Combinatorial Mathematics* X, Proceedings, Adelaide 1982, edited by L.R.A.Casse, Lecture Notes in Mathematics, **1036**, Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 206-216.

A. V. Geramita and J. Seberry (1979), *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York-Basel.

H. Kharaghani (1985), New classes of weighing matrices, *Ars Combinatoria*, **19**, 69-73.

C.A. Rodger, D. G. Sarvate and J. Seberry (1987), Colourable designs, new group divisible designs and pairwise balanced designs, *J. Stat. Planning and Inference* **15**, 379-389.

J. Seberry (1984), Regular group divisible designs and Bhaskar Rao designs with block size three, *J. Stat. Planning and Inference*, **10**, 69-82.

CHAPTER 8

APPLICATIONS TO ENCRYPTION

There are essentially only two operations involved in the classical encryption of a message: substitution and transposition. In addition, the message may be accordioned by either introducing or removing superfluous symbols. The simplest of all encryption schemes is monoalphabetic substitution, in which each letter of the message is replaced by a fixed substitute. When encrypting by simple transposition, a permutation P of n symbols is the key and each successive block of n symbols in the message is rearranged using P. To strengthen substitution encryption, one may use not one but several monoalphabetic substitutions, with the "key" including a specification of which substitution is to be used for each symbol of the cipher. A well known example is the Vigenere ciphers, in which the substitutions are simple cyclic shifts of the original alphabet (see Simmons(1979)).

8.1 Encryption using combinatorial designs

Some ideas where designs can be used in encryption are presented in the attached published paper

"Encryption methods based on combinatorial designs", Ars Combinatoria, 21A, 237-246.

The version of the paper attached here has been slightly modified to make the ideas clearer. Further research can be done in calculating the complexity and increasing the efficiency and security of the ideas developed in this paper. The methods described have the attraction of yielding large compression. The ideas were developed by J. Seberry and this author in close and continuous association, hence it is impossible to indicate which idea is from which author.

Encryption Methods Based on Combinatorial Designs

Dinesh G. Sarvate and Jennifer Seberry

1. Introduction.

We explore some possible ways combinatorial designs might be used as secret codes. We are motivated to use designs as:

(1) combinatorial designs are often hard to find;

(2) the algorithms for encryption and decryption are of reasonable length,

(3) combinatorial designs have very large numbers of designs in each equivalence class lending themselves readily to selection using a secret key.

We hope our ideas will encourage much more research into applications of combinatorial cryptography. Cryptosecurity can be enhanced by using different methods for producing sequences of random permutations (see Sloane[1983]) and also by permuting the encoded message with a random permutation using a secret key (see Ayoub[1981]).

Where we have considered combinatorial designs which are well known we refer the reader to standard texts such as Hall [1967] , Raghavarao[1971] or Wallis,Street and Wallis[1972] for definitions and constructions. For less frequently used or less well known designs a definition or reference is given.

All these methods lend themselves to further opacity if random number generators are used to apply permutations at any or all stages of encryption. An excellent survey of random number generators can be found in Sloane [1983].

2. Encryption method using mutually orthogonal Latin Squares.

Suppose we have a set of k mutually orthogonal Latin squares of order n. A key is used which chooses a pair of the k-set at random. Encryption is now achieved by transmitting for message i,j the element in the (i,j) th position of the selected pair of orthogonal squares.

Example. The following are three 4 X 4 mutually orthogonal Latin squares:

$$A = \begin{bmatrix} 1&2&3&4 \\ 2&1&4&3 \\ 3&4&1&2 \\ 4&3&2&1 \end{bmatrix}, \quad B = \begin{bmatrix} 1&2&3&4 \\ 4&3&2&1 \\ 2&1&4&3 \\ 3&4&1&2 \end{bmatrix}, \quad C = \begin{bmatrix} 1&2&3&4 \\ 3&4&1&2 \\ 4&3&2&1 \\ 2&1&4&3 \end{bmatrix}$$

Suppose the key chooses the third and first Latin squares. Then to transmit the message 1,4 we send the (1,4) th element of the third and first Latin squares i.e. 4,4.

Decryption is achieved by looking at which row and columns of the squares contain the pair 4,4 and that is the (1,4) th position.

Extra security is ensured by:

(a) permutations of the rows and columns of the Latin squares as a set;

(b) permutations of the elements within one or more of the Latin squares;

(c) the key can be used to change the pair of Latin squares after every two byte message if required;

(d) the key can be used to change the size of the pairs of the Latin squares after every two byte message if required;

(e) the key can be used to choose another inequivalent and non-isomorphic pair at any stage.

Mutually orthogonal Latin squares of size n can used to send any of the n^2 possible two byte messages.

Longer messages use *orthogonal F-squares and n-dimensional arrays.*

We illustrate via an example. Suppose A, B, C are, as before, pairwise mutually orthogonal Latin squares then

$$A_1 = \begin{bmatrix} A & A \\ A & A \end{bmatrix}, \quad B_1 = \begin{bmatrix} B & B \\ B & B \end{bmatrix}, \quad C_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 & 4 & 3 & 2 & 1 \\ 4 & 3 & 2 & 1 & 3 & 4 & 1 & 2 \\ 2 & 1 & 4 & 3 & 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 & 4 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 & 2 & 1 & 4 & 3 \\ 2 & 1 & 4 & 3 & 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 & 3 & 4 & 1 & 2 \end{bmatrix}$$

are mutually orthogonal in the sense that each of the 4^3 messages from a quaternary alphabet occur in the (i,j)th positions of A_1 ,B_1, C_1. For example, the message 1,3,3 occurs in the (2,6) position.

This process of adding more mutually orthogonal faces to a higher dimensional array allows:

(a) a key to be used to choose any subset of the faces of the array;
(b) the rows and columns of the faces to be permuted;
(c) the elements of the faces to be permuted;
(d) compression of the message;
(e) the key to be used to choose inequivalent higher dimensional arrays at any stage of the encryption process.

3. Encryption methods using Room squares.

Room squares can also be used to send messages in a fashion similar to that described for Latin squares. As currently defined not all messages are available. For example consider the Room square

$$\begin{bmatrix} 01 & 45 & 27 & - & 36 & - & - \\ - & 02 & 56 & 31 & - & 47 & - \\ - & - & 03 & 67 & 42 & - & 52 \\ 62 & - & - & 04 & 71 & 53 & - \\ - & 73 & - & - & 05 & 12 & 64 \\ 75 & - & 14 & - & - & 06 & 23 \\ 34 & 16 & - & 25 & - & - & 07 \end{bmatrix} .$$

The situation becomes a little better for encryption if we note this example is of a skew Room square and so if the i,j entry is empty the j,i entry, $i \neq j$ is not.Thus we can send any message.

Example . Use the modified Room square

$$\begin{bmatrix} 11 & 45 & 27 & - & 36 & - & - \\ - & 22 & 56 & 31 & - & 47 & - \\ - & - & 33 & 67 & 42 & - & 51 \\ 62 & - & - & 44 & 71 & 53 & - \\ - & 73 & - & - & 55 & 12 & 64 \\ 75 & - & 14 & - & - & 66 & 23 \\ 34 & 16 & - & 25 & - & - & 77 \end{bmatrix} .$$

Then to encode the message 76 we observe 67 in the 3,4th position and send 43.

All the permutations that were previously used for the Latin squares can still be used.

We note further that the Room square of the example is constructed using the starter-adder technique and each element can be found from the first row

so that if the 1,j element is x,y the i,j+i-1 element is x+i-1,y+i-1 where j+i-1, x+i-1 and y+i-1 are reduced mod n, the size of the Room square. We use {1, 2, ... , n} as class of representatives.

The differences between the elements of the first row are all different so to encipher 76 we first note that 6-7=-1 and 45 has difference 1, hence 76 can also be encrypted by -1, 2 meaning

(a) start with the pair distance 1 apart,
(b) add two to both,
(c) reverse the order.

Thus to decode -2,4 we note 7 and 2 are -2 apart and so decode as 64.

To encrypt longer messages the higher dimensional anlogues of skew Room squares are most useful.

4. Designs with two way elimination of heterogeneity.

These designs were first studied in connection with estimating tobacco mosaic virus by Youden[1937] and have subsequently been studied by a number of authors including Agrawal [1966i,ii], Agrawal and Mishra[1971] Preece[1966i,ii], Seberry[1979i], Street[1981], Sterling and Wormald[1976]. A number of infinite families as well as one-off examples are known.

These designs comprise two designs with parameters $(v_1, b, r_1, k, \lambda_1)$ and $(r_1, b, v_1, k, \lambda_2)$, such that the incidence matrices N_1 and N_2 of the designs satisfy the additional property

$$N_1 N_2^T = kJ.$$

Example. Let the designs have the parameters

$$v_1 = r_2 = 9,\ r_1 = v_2 = 4,\ b = 12,\ k = 3$$

and treatments A,B,C,D,E,F,G,H,I and a,b,c,d respectively.

The two way design is

N_{12} =

A	b	a	d	c
B	c	a	d	b
C	d	a	b	c
D	c	d	a	b
E	d	c	a	b
F	b	d	a	c
G	b	c	d	a
H	c	d	b	a
I	d	c	b	a

Note that the blocks of N_2 are the columns of the following array:

b, c, b, a, a, a, d, d, b, c, b, c
c d c d c d a a a b c b
d b d c d c b b d a a a

The blocks of N_1 are the columns of the following array:

A, D, G, A, B, C, A, B, C, A, B, C
B E H D E F F D E E F D
C F I G H I H I G I G H

The two-way design is

Ab Dc Gb Aa Ba Ca Ad Bd Cb Ac Bb Cc
Bc Ed Hc Dd Ec Fd Fa Da Ea Eb Fc Db
Cd Fb Id Gc Hd Ic Hb Ib Gd Ia Ga Ha

There is a number of encryption methods possible using these designs.

(1) The treatment of N_1 is sent to indicate the message given by the r_1-tuple of treatments of N_2 associated with that treatment.

In the above example sending F would actually send the message (b,d,a,c).

(2) The block of N_1 is sent to indicate the message given by the k_2-tuple of treatments of N_2 associated with that block.

In the example sending 5 would actually send the message (a,c,d).

(3) A pair of treatments of N_1 is sent. Since N_1 is a block design any pair of treatments occurs in λ_1 blocks and the message is those pairs (in the order given by the treatments of N_1).

In the example, sending AG actually sends the message ac, where GA sends ca.

Now a secret key can be used to

(a) permute the rows of the two-way designs,
(b) permute the columns of the two-way design,
(c) permute the treatments of the second design,
(d) permute the blocks of the second design.

The advantages of using such designs are

(a) message compression,
(b) ease of decoding/encoding,
(c) if used in reverse it is asymmetric,
(d) the reverse procedure can combine encryption with error correction,
(e) these designs are hard to find even before permutations are used on them.

5. Crypto and coloured designs.

Some designs exist which may be more useful for encryption method 3 of the previous section. For example in the following design on five symbols every pair of elements (x,y), x, y ϵ {a,b,c,d,e} occurs as an intersection of some pair of rows.

A	a	b	c	
B	a		d	e
C	b			e e
D		b	b	a
E		c	a	e
F			c	d c
G			d d	b

So to send say (a,e) we send DC, but to send (e,a) we send CD. The structure of the design ensures that all the permutations that can be effected and selected by the secret key are available.

Similar designs where pairs (or t-tuples) occur exactly once in a row or column have not been widely studied and offer a fruitful area of research.

Cryptodesigns with the less restrictive condition that every element occurs once in a row (so every row is an r-tuple) but each element in column is different are called *coloured designs* and have proved extremely useful, in constructing new BIBDs and SBIBDs(see Seberry(1985ii), Sarvate and Seberry(1985) and de Launey and Seberry(1985).).

6. Encryption method using ordered designs.

The method described in this section is for encrypting a k-ary message by using combinatorial designs with blocks,whose elements are ordered. We encrypt a message of length t into a message of length 2, in other words we compress the message.

Examples of such designs are modified directed balanced incomplete block designs i.e. DBIBDs (see Seberry and Skillicorn [1980] , Street and Wilson[1980], Colbourn and Colbourn[1984]), cyclic BIBDs (see Colbourn and Colbourn[1984]) and directed packings (see Skillicorn and R.G.Stanton[1982], Dawson, Seberry, and Skillicorn [1984]) over v treatments , $v \geq k$. The method can be easily extended to unordered designs.

Label $n_1, n_2, \ldots, n_s$, the $s = \binom{v}{t}$ ways of selecting a t-tuple from a given block of a DD(t,k,v), with NDD(t,k,v) = N, the number of blocks. Now the DD(t,k,v) uses a k-ary alphabet with blocks of size v such that each ordered t-tuple occurs at least once. Thus a t-digit message can be sent by transmitting two symbols, the first giving the block number (an integer between 1 and N) and the other the number, n_a which indicates the position of the required t-tuple in the block.

The sender needs a large dictionary but the receiver needs only a list of the blocks and the way of choosing the n_i^{th} t-tuple from each block.

This method has the advantages of:

(1) message compression of a high order;
(2) small storage and time needed for decryption.

These properties are needed for example, in transmission to space-shuttles, undersea activities or other remote receivers.

Example: Let the message be aab dcc adc. Suppose we use the following design, DD(3,4,4) together with 14 extra blocks to cover all the possible triples.

DD(3,4,4) : B_1 = a b c d B_2= b a d c B_3= c a d b
B_4= d a c b B_5=d b c a B_6=c b d a

Extra blocks : B_7=a b a b B_8=a c a c B_9=a d a d
B_{10} =b c b c B_{11} =b d b d B_{12} =c d c d
B_{13} =a b a a B_{14} =b c b b B_{15} =c d c c
B_{16} =d d a d B_{17} =d b b a B_{18} =c d a a
B_{19} =c c a b B_{20}=d d b c

Suppose n_1 indicates we should choose positions 123 of the block, and n_2,n_3,n_4 indicate choosing positions 124, 134, 234 respectively of the block. Then since aab is found in B_7, aab is encoded as 7,n_3. dcc is encoded 15,n_4 and adc is encoded 2,n_4.

This design is not optimal in the sense that many pairs and triples occur 2 and 3 times. Optimal solutions where each possible t-tuple occurs and the fewest number of blocks possible is used, would be of great interest.

7. A practical Method.

An interesting application of the Rubik cube, in games or teaching, occurs when the message is of length less than or equal to 54 units. The sender and the receiver know how to read the message on the cube. The sender applies operations P_1,P_2, ..., P_n and sends the cube via a messenger. The receiver applies P_n^{-1}, ..., P_1^{-1} and recovers the message.

References:

Agrawal, H.L.(1966i), *Some Methods of construction of designs for two way elimination of heterogeneity* I. J. Amer. Statist. Assoc.,61,1153-1171.

Agrawal, H.L.(1966ii), *Some systematic methods of construction of designs for two-way elimination of heterogeneity* Calcutta Statist. Assoc. Bull., 15, 93-108.

Agrawal, H.L. and Mishra, R.I.(1971), *Some methods of construction of 4 DIB designs* Calcutta Statist. Assoc. Bull., 20, 89-92.

Ayoub, F.(1981), *Encryption with keyed random permutations* Electronics Letters, 17, 583-585.

Bose, R.C.(1942), *A Note on the resolvability of balanced incomplete block designs* Sankhya, 6,105-110.

Colbourn, C.J. and Colbourn, M. J.(1984), *Every two-fold triple system can be directed* J. Combinatorial Theory, A, 34, 375-378.

Colbourn,M.J. and Colbourn,C.J.(1984), *Recursive constructions for cyclic designs* J.Stat.Plan.and Inf.,10, 97-103.

Dawson, J.E. ,Seberry, J. and Skillicorn, D.B.(1984), *The directed packing numbers DD(t,v,v), t·4* Combinatorica, 4, (2-3) 121-130.

de Launey, W. and Seberry J. (1985), New group divisible designs obtained via matrices associated with generalized Hadamard matrices, (preprint).

Hall, M. Jr.(1967), *Combinatorial Theory,* Ginn (Blaisdell), Bostan.

Hess, P. and Wirl, K.(1983), *A voice scrambling system for testing and demonstration,* Cryptography, Lecture notes in Computer Science , Springer-Verlag(Berlin), Edited T.Beth,149, *147-156.*.

Preece, D.A.(1966i), *Some row and column designs for two sets of treatments*, Biometrics,22,1-25.

Preece, D.A.(1966ii), *Some balanced incomplete block designs for two sets of treatments* Biometrika, 53,497-506.

Raghavrao, D.(1971), *Construction and combinatorial Problems in Design of Experiments* John Wiley, New York.

Sarvate D.G. and Seberry J.(1985) Colourable designs and new group divisible designs, (preprint).

Seberry, J.(1979i), *A note on orthogonal graeco-latin designs*, Ars Combinatoria, 8, 85-94.

Seberry, J.(1985ii) Generalized Hadamard matrices in the construction of regular GDDs with two and three associate classes (preprint).

Seberry, J. and Skillicorn, D.B.(1980), *All directed BIBDs with k=3 exist*, J. Combinatorial Theory, A, 29, 244-248.

Skillicorn, D.B. and Stanton, R.G.(1982), *The directed packing numbers DD(t,v,v)* Proceedings of the Eleventh Manitoba Conference on Numerical Mathematics and Computing, Winnipeg, Manitoba,1981, Congressus Numerantium, 34, 247- 252.

Sloane, N.J.A.(1983), *Encrypting by random rotations*, Cryptography, Lecture notes in Computer Science , Springer-Verlag(Berlin), Edited by T.Beth,149, 71-127.

Sterling, L.S. and Wormald, N.(1976), *A remark on the construction of designs for two-way elimination of heterogeneity*, Bull. Austral. Math. Soc.,14, 383-388.

Street, D. and Seberry, J.(1980), *All DBIBDs with block size four exist*, Utilitas Mathematica, 18, 27-34.

Street, D.(1981), *Graeco latin and nested row and column designs.* Combinatorial Mathematics VIII, edited by K.L.McAvaney, Vol. 884, Lecture Notes in Mathematics, Springer-Verlag, Berlin- Heidelberg- New York, 304-313.

Street, D. and Wilson, W.(1980), *On directed balanced incomplete block designs with block size five*, Utilitas Mathematica,18, 161-174.

Wallis, W. D. , Street, A. P. and Seberry Wallis, J.(1972), *Combinatorics*, Lecture Notes in Mathematics, vol 292, Springer - Verlag, Berlin-Heidelberg-New York.

Youden, W.J.(1937), *Use of incomplete block replications in estimating tobocco mosaic virus*, Contributions from Boyce Thompson Institute, 9, 41-48.

8.2 Encryption using Hungarian rings

The Hungarian Rings puzzle (called Hungarian rings) consists of two interlocked rings of 20 balls such that either ring can rotate as a cycle. The intersections of the two rings are 5 balls apart in each ring as shown in Fig. 1.

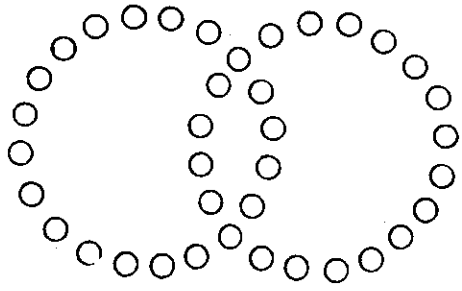


Fig. 1

We know that encryption is closely related to substitution and permutation of the message symbols. We wish to give a systematic method to permute the message block while scrambling in the message a number of arbitrary message symbols. If any secure substitution, which also compresses the message, is used with the method given in the attached paper

"Encryption using Hungarian rings", Discrete Applied Mathematics, 16, 1987, 151-155,

then we may have a very secure encryption. A method which uses ordered designs and which has a message compression of a very high order, is given in section 8.1 (Sarvate and Seberry (1986)). The version of the Hungarian rings which is used in the attached paper consists of two interlocked rings of a and b balls respectively. At any instance the two interlocked rings have only two balls common. We do not restrict the intersections of the two rings to be a fixed number of balls apart. The method can be easily modified for any integer a, b and any integer t of common balls.

Encryption using Hungarian rings

Joseph Hammer and Dinesh G. sarvate

Introduction

Encryption is closly related to substitution and permutation of message symbols. In this note we use the Hungarian rings structure for that purpose. It breaks up a message into segments of different lengths. For each segment we apply a different permutation. We are going to present a systematic method to permute the segments while scrambling a number of arbitrary message symbols. Note that the Hungarian rings present a physical model for the abstract concept of scrambling and permutation. For us the Hungarian rings HR(a, b) consists of two inter-locked rings, R_1 and R_2, of a and b balls respectively with four operations, called HR operations R_1^+, R_1^-, R_2^+ and R_2^-, where R_i^+ is to rotate the balls of the ring R_i in the anticlockwise direction and R_i^- is to rotate the balls of R_i in the clockwise direction. We notice that R_i^+ and R_i^- are inverse operations. For proper definition and illustration the reader is referred to Singmaster [4]. Encryption methods based on combinatorial designs were studied recently by Sarvate and Seberry [2]. The technique depends mainly on the random permutations and the large number of equivalent designs with same parameters. In the present note we have used the structure of Hungarian rings and its movement (i.e. HR operations) together with the random permutations to encrypt a message of length m into a message of length Lm, the key being a 6-coordinate number with s HR operations $P_1, P_2, \ldots, P_S$.

The message is encrypted in such a way that each (a+b-2) bits of encoded message will have only 'a' bits of information scrambled by a random permutation and s HR operations.

When we talk about labelling the ring by message block, we understand that the balls on each ring have an inner labelling as 1, ..., a and 1, ..., b and also an inner labelling of 1, ..., a+b-2 when we consider both rings together.

When we talk about generating random permutations or random numbers, we assume that a common procedure is known to both sender and the receiver. We also assume that both sender and receiver have a collection of sets of two methods for random number generation and three methods for random permutation generation. The sixth coordinate will indicate the set which will be used at the next message. Of course, for the first time both sender and receiver have fixed a set to be used for encryption. An excellent survey of random permutations can be found in Sloane [3].

Algorithm

Step 1. Generate random integer sequences $\{x_i\}_{i=1}^{t}$ and $\{N_i\}_{i=1}^{t}$, using the first and second coordinate of the key, such that

$$\sum_{i=1}^{t-1} y_i N_i \le m \le \sum_{i=1}^{t} y_i N_i$$

where $y_i = a$ or b depending on x_i being odd or even.

Step 2. Break the message into submessages of length $y_i N_i$, $i = 1, \ldots, t$.

Step 3. Produce sequences of random permutations $\{B_i\}_{i=1}^{t}$, $\{A_i\}_{i=1}^{t}$ and $\{S_i\}_{i=1}^{t}$ using the third, fourth and fifth coordinate of the key respectively, where B_i is a permutation over $\{1, \ldots, b\}$, A_i is a permutation over $\{1, \ldots, a\}$ and S_i is a permutation over $\{1, 2, \ldots, a+b-2\}$.

Step 4. For $i = 1$ to t, encode the submessage block of length $y_i N_i$.

Step (i). Call the ring with y_i balls R_1 and the other ring R_2.

Step (ii). Break the submessage block into blocks of length y_i.

Step (iii). For $j = 1$ to N_i do the following:

(a) Label R_1 by the message block.

(b) Label R_2 by arbitrary message symbols.

(c) If R_1 is of 'a' balls, then apply A_i on R_1, else apply B_i on R_1.

(d) If R_2 is of 'b' balls, then apply B_i on R_1, else apply A_i on R_2.

(e) Apply S_i on R_1 and R_2 together.

(f) Apply HR operations $P_1, \ldots, P_s$.

(g) Send the message.

To decode, the receiver applies Steps 1 and 3, except that he breaks the message into subsequences of length $(a+b-2) \cdot N_i$. In Step 4 he uses the inverse permutations and HR operations, while applying substeps in reverse order.

Remarks. (1) Note that the arbitrary symbols of the second ring will not change the position in the encrypted message, thereby making them vulnerable for breaking. This problem can be solved by using successive relabelling in the sense that from $j = 1$ to N_i, for $j = l+1$, consider the positions in the step $j = l$ in R_1 and R_2 as the original positions (as inner labelling). This can conveniently be done in a computer program.

(2) Instead of six-coordinate key we can send only one number to be used to produce six random numbers, which can be used as seeds for the algorithm.

Complexity. Suppose m is the length of the message and it is encrypted into a message of length $n = Lm$. The intruder first has to factorize $n = Lm$ in $a + b - 2$ and $\sum N_i$ to be able to determine the size of the rings and the sequence of integers N_i. Next the intruder has to determine all subsets S of $\{1, 2, \ldots, \sum N_i\}$ such that $\sum_{j \in S} j = \sum_{i=1}^{t} N_i$ (where S is independent of t). Now this problem contains the following NP-complete problem in Garey and Johnson [1, p. 223].

Given a set A, size $s(a) \in Z^+$ for each $a \in A$, and a positive integer B. Is there a subset A' of A s.t. the sum of the sizes of the elements in A' is B?

Example. For simplicity we assume that our rings are of four and three balls respectively and the balls are named as b_1, b_2, b_3, b_4 and b_5. Two balls are common to both the rings, and each ball is represented by a triple (x, y, z) where x represents the inner labelling as a ball from an individual ring, y is the inner labelling when we consider the balls together and z is the message symbol attached to the ball while encrypting a certain submessage block.

Let

$$b_1 = (1, 1, -), \qquad b_2 = (2, 3, -), \qquad b_3 = (3_1, 4, -),$$

$$b_4 = (4_1, 5, -) \quad \text{and} \quad b_5 = (3_2, 2, -)$$

where b_1, b_2, b_3 and b_4 are the balls of first ring and b_1, b_2 and b_5 are the balls of the second ring. The subscripts for the first coordinate are same for two balls from the same ring. The first coordinate without subscript means that ball is common to both rings.

Let the HR operations in the key be R_1+ and R_2-.

Let the secret message be 0 1 1 1 0 1 1 1 0 1.

Step 1. Let $x_1 = 2$, $x_2 = 5$, $N_1 = 2$ and $N_2 = 1$.

Step 2. The message is broken into two parts of lengths $b \cdot N_1 = 3 \cdot 2$ and $a \cdot N_2 = 4 \cdot 1$, viz.

0 1 1 1 0 1 and 1 1 0 1.

Step 3. For the sake of simplicity, let A_1, B_1 and S_1 be the identity permutations and let A_2, B_2 and S_2 be the shift permutations by 1 (i.e., $A_2(x) = x + 1, x = 1, \ldots, a - 1$ and $A_2(a) =$ 1. Similarly for B_2 and S_2).

Step 4. We encode first 0 1 1 1 0 1 with the following steps.

Step (i). Let the ring with balls b_1, b_2 and b_5 be R_1 and the other ring be R_2.

Step (ii). Let the submessage blocks be 0 1 1 and 1 0 1.

Step (iii). (a) Label R_1 by the message block 0 1 1.

(b) Assign the arbitrary message symbols 0, 1 to the balls b_3 and b_4, i.e., we have $b_1 = (1, 1, 0)$, $b_2 = (2, 3, 1)$, $b_3 = (3_1, 4, 0)$, $b_4 = (4_1, 5, 1)$, $b_5 = (3_2, 2, 1)$.

(c) Apply identity permutation B_1 on R_1.

(d) Apply identity permutation A_1 on R_2.

(e) Apply identity permutation S_1 on R_1 and R_2 together, so in these steps there is no change in the coordinates of the b_i's.

(f) Apply R_1+, to get

$$b_1=(2,3,1), \quad b_2=(3_2,2,1), \quad b_3=(3_1,4,0),$$

$$b_4=(4_1,5,1), \quad b_5=(1,1,0).$$

(i.e., $b_1\to b_5$, $b_5\to b_2$, $b_2\to b_1$; $b_3\to b_3$, $b_4\to b_4$. {read b_5 becomes b_1 etc.}.)

Apply R_2-, to obtain

$$b_1=(4_1,5,1), \quad b_2=(2,3,1), \quad b_3=(3_2,2,1),$$

$$b_4=(3_1,4,0), \quad b_5=(1,1,0)$$

(i.e., $b_1\to b_2$, $b_2\to b_3$, $b_3\to b_4$, $b_4\to b_1$; $b_5\to b_5$)

(g) Hence the encrypted message for 0 1 1 is

1 1 1 0 0.

(i.e., the last coordinates of the b_i's). Similarly 1 0 1 is encrypted into

1 0 1 0 1.

Now to encrypt 1 1 0 1, we proceed as before:

Step (i). Let the ring with balls b_1, b_2, b_3 and b_4 be R_1 and the ring with balls b_1, b_2, b_5 be R_2.

Step (ii). Here the submessage block is only one, viz. 1 1 0 1.

Step (iii). (a) Label R_1 by the message 1 1 0 1.

(b) Let the ball b_5 be labeled by the symbol 1, i.e., we have

$$b_1=(1,1,1), \quad b_2=(2,3,1), \quad b_3=(3_1,4,0),$$

$$b_4=(4_1,5,1), \quad b_5=(3_2,2,1).$$

(c) Apply the shift permutation, A_2 on R_1, to get

$$b_1=(2,3,1), \quad b_2=(3_1,4,0), \quad b_3=(4_1,5,1),$$

$$b_4=(1,1,1), \quad b_5=(3_2,2,1)$$

(i.e., $b_2\to b_1$, $b_3\to b_2$, $b_4\to b_3$, $b_1\to b_4$).

(d) Apply the shift permutation, B_2 on R_2, to get

$$b_1=(3_1,4,0), \quad b_2=(3_2,2,1), \quad b_3=(4_1,5,1),$$

$$b_4=(1,1,1), \quad b_5=(2,3,1)$$

(i.e., $b_2\to b_1$, $b_5\to b_2$, $b_1\to b_5$; $b_3\to b_3$, $b_4\to b_4$).

(e) Apply the shift permutation S_2 on R_1 and R_2 together to get

$$b_1=(3_2,2,1), \quad b_2=(4_1,5,1), \quad b_3=(1,1,1),$$

$$b_4=(2,3,1), \quad b_5=(3_1,4,0)$$

(i.e., $b_2 \to b_1$, $b_3 \to b_2$, $b_4 \to b_3$, $b_5 \to b_4$, $b_1 \to b_5$).

(f) Apply R_1+ to get:

$$b_1 = (4_1, 5, 1), \quad b_2 = (1, 1, 1), \quad b_3 = (2, 3, 1),$$

$$b_4 = (3_2, 2, 1), \quad b_5 = (3_1, 4, 0)$$

(i.e., $b_1 \to b_4$, $b_4 \to b_3$, $b_3 \to b_2$, $b_2 \to b_1$; $b_5 \to b_5$).

Apply R_2-, to get

$$b_1 = (3_1, 4, 0), \quad b_2 = (4_1, 5, 1), \quad b_3 = (2, 3, 1),$$

$$b_4 = (3_2, 2, 1), \quad b_5 = (1, 1, 1)$$

(i.e., $b_1 \to b_2$, $b_5 \to b_1$, $b_2 \to b_5$; $b_3 \to b_3$, $b_4 \to b_4$).

(g) Hence the encrypted message for 1 1 0 1 is

0 1 1 1 1

So the message 0 1 1 1 0 1 1 1 0 1 is encrypted into

1 1 1 0 0 1 0 1 0 1 0 1 1 1 1.

Acknowledgement

We wish to thank Dr. J.R. Seberry for helpful discussions.

References

[1] M.R. Garey and D.S. Johnson, Computers and Intractability, A Guide to the Theory of NP-Completeness (W.H. Freedman, San Francisco, 1979).

[2] D.G. Sarvate and J.R. Seberry, Encryption methods based on combinatorial designs, Ars Combinatoria, 21 A (1986) 237-246.

[3] J. Sloane, Encryption by random permutations, in: T. Beth, ed., Cryptography, Lecture Notes in Computer Science 149 (Springer, Berlin, 1983) 71-128.

[4] D. Singmaster, Hungarian rings groups, Bull. Institute of Mathematics and its Applications 20 (1984) 137-139.

CONCLUSION

In the light of the results presented, some unanswered problems are posed for further research.

In Chapters 1 and 6, the technique used to give constructions for BIBDs and PBIBDs has been explored to construct t-designs (Kramer and Messner (1976), Alltop (1971)). Can we use similar techniques to construct cyclic and directed t-designs?. Algorithms to order BIBDs of block size 3 to get directed designs have been studied by Colbourn and Harms (1983). Can we get similar algorithms and results for directed designs with block size greater than 3 and for cyclic and equi-neighboured designs with block size greater than or equal to 3?

In Chapter 2, Harms and Colbourn's conjecture has been discussed. Can we give non-trivial families which satisfy the conjecture? Can we apply Hanani's theory to the conjecture with block size greater than 3?

The existence problem for colourable designs is settled, but that for crypto designs is still untouched. Colourable designs have been used to construct orthogonal designs. How can they be used to construct other designs? Now, as colourable designs are edge-coloured graphs and colourable designs are used to construct GDDs, can we use some other edge-coloured graphs to construct BIBDs and GDDs? Can they be used in encryptions?

The generalized Bhaskar Rao designs over abelian (but not elementary abelian) groups are mostly untouched except for the result on block size 3 over Z_4. In general, we need to identify systematically the unknown GBRDs and look for them, e.g. GBRD(7, 3, 2^t; Z_2t) is not known. We know that an SBIBD(5,4,3) and a GBRD(4, 3, 2^t; Z_2t) exist and hence a GBRD(5, 3, 3.2^t; Z_2t) exists. A GBRD(3, 3, 12; Z_{12}) cannot exist because of Drake's theorem (Drake (1979), Theorem 1.10) but we can get GBRD(3, 3, 24; Z_{12}). Dr Jennifer Seberry has recently found a few more new GBRDs (v, 4, 4) over $Z_2 \times Z_2$, to complete the work on block size 4. The work is still not over. The method

used in constructing orthogonal designs is simple and must be exploited more. Sarvate and Seberry (198?) have recently given a new construction for a known family of weighing matrices viz. $W(p^2(p-1), p^2)$, using the 2-adjugate method of Patwardhan and Vartak(1980). Can we modify the method to get new weighing matrices. How the construction for orthogonal designs be generalised?. In the end, as Constance Reid has written in "Hilbert", "The world of mathematics is inexhaustible."

BIBLIOGRAPHY

Agrawal, H. L., (1966a), Some methods of construction of designs for two way elimination of heterogeneity; *J. Amer. Statist. Assoc*, **61**, 1153-1171.

Agrawal, H. L., (1966b), Some systematic methods of construction of designs for two way elimination of heterogeneities, *Calcutta Staitst. Assoc. Bull*, **15**, 93-108.

Agrawal, H. L., (1966c), Some generalizations of distinct representatives with applications to statistical designs, *Ann. Math. Stat.*, **37**, 525-526.

Agrawal, H. L. and Mishra, R. I., (1971), Some methods of construction of 4DIB designs, *Calcutta Statist. Assoc. Bull.*, **20**, 89-92.

Alltop, W. O., (1966), On the construction of block designs, *J. Combinatorial Th.*, **1**, 501-502.

Alltop, W. O., (1971), Some 3-designs and a 4-design, *J. Combinatorial Th.*, **11**, 190-195.

Ayoub, F., (1981), Encryption with keyed random permutations, *Electronics Letters*, **17**, 583-585.

Bermond, J. C., Huang, C. and Sotteau, D., (1978), Balanced cycle and circuit designs: even cases, *Ars Combinatoria*, **5**, 293-318.

Bhaskar Rao, M., (1966), Group divisible family of PBIB designs, *J. Indian Stat. Assoc.*, **4**, 14-28.

Bhaskar Rao, M., (1970), Balanced orthogonal designs and their application in the construction of some BIB and group divisible designs, *Sankhya*, **32 A**, 439-448.

Bhat, V. N. and Shrikhande, S. S., (1970), Nonisomorphic solutions of some balanced incomplete block designs I, *J. Combinatorial Th.*, **5**, 174-191.

Biggs, N. L. and White, A. T., (1979), *Permutation Groups and Combinatorial Structures*, London Mathematical Society Lecture Note Ser. **33**, Cambridge University Press.

Bose, R. C., (1939), On the construction of balanced incomplete block designs, *Ann. Eugenics*, **9**, 353 -399.

Bose, R. C., (1942), A note on the resolvability of balanced incomplete block designs, *Sankhya*, **6**, 105-110.

Brouwer, A. E., Schrijven, A. and Hanani, H., (1977), Group divisible designs with block size four, *Discrete Math.*, **20**, 1-10.

Brunk, M. E. and Federer, W. T., (1953), Experimental designs and probability sampling in marketing research, *J. Amer. Statist. Assoc.*, **48**, 440-452.

Cameron, P. J., (1978), Strongly regular graphs, *Selected Topics in Graph Theory*, (edited by L. W. Beineke and R. J. Wilson), Academic Press, 337-360.

Cameron, P. J. and van Lint, J. H. (1980), *Graphs, Codes and Designs*, London Math. Soc. Lecture Note Series, **43**, Cambridge University Press.

Cheng, C. S., (1983), Construction of optimal balanced incomplete block designs for correlated observations, *Ann. Statist.*, **11**, 240-246.

Clatworthy, W. H., (1973), *Tables of Two-Associate-Class Partially Balanced Designs*, National Bureau of Standards Applied Mathematics Ser. **63**, U. S. Government Printing Office, Washington.

Colbourn, C. J. and Colbourn, M. J., (1983), Every twofold triple system can be directed, *J. Combinatorial Th.* Ser. A, **34**, 375-378.

Colbourn, C. J. and Harms, J. J., (1983), Directing triple systems, *Ars Combinatoria*, **15**, 261-266.

Colbourn, M. J. and Colbourn, C. J., (1984), Recursive constructions for cyclic designs, *J. Statist. Plan. and Inf.*, **10**, 97-103.

Dawson, J. E., (1985), Equineighbour designs of block size four, *Ars Combinatoria*, **19A**, 295-301.

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

de Launey, W., (1984), Non-existence of generalised weighing matrices, *Ars Combinatoria*, **17A**, 117-132.

de Launey, W. and Sarvate D.G., (1984), Non-existence of certain GBRDs, *Ars Combinatoria*, **18**, 5-20

de Launey, W., Sarvate, D. G. and Seberry, J., (1985), Generalised Bhaskar Rao designs with block size 3 over Z_4, *Ars Combinatoria*, **19A**, 273-286.

de Launey, W. and Seberry, J., (1984), Generalized Bhaskar Rao designs of block size four, *Congressus Numerantium*, **41**, 229-294.

de Launey, W. and Seberry, J. (198?), Bhaskar Rao designs of block size 4, *Proceedings of the Calcutta Conference, 1982*, (to appear)

Denes, J. and Keedwell, A. D., (1974), *Latin Squares and Their Applications*, Univ. Press, London.

Doyen, J. and Rosa, A., (1973), A bibliography and survey of Steiner systems, *Bollettino V. M. J.*, **4**, 392-419.

Drake, D. A., (1979), Partial geometries and generalized matrices over groups, *Canad. J. Math.*, **31**, 617-627.

Durbin, J., (1951), Incomplete blocks in ranking experiments, *Brit. J. Psychology*, **4**, 85-90.

Erdos, P., (1982), Problems and Results on block designs and set systems *Congressus Numerantium*, **35**, 3-6.

Fiorini, S. and Wilson, R. J., (1977), *Edge-colouring of Graphs*, Reserch Notes in Mathematics, **16** , Pitman, London-San Francisco-Melbourne.

Geramita, A. V. and Seberry, J., (1979), *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York-Basel.

Gibbons, P., (1975), *Computing Techniques for the construction and Analysis of Block Designs*, Ph. D. Dissertation, University of Toronto.

Gibbons, P. and Mathon, R., (1986), Construction methods for Bhasker Rao and related designs, *J. Austral. Math. Soc.* , Ser. A, (to appear).

Glynn, D. G., (11978), *Finite Projective Planes and Related Combinatorial Systems*, Ph. D. Thesis, University of Adelaide.

Hall, Jr., M. (1986), *Combinatorial Theory*, Wiley Interscience Series in Discrete Mathematics, John Wiley and Sons, NY.

Hammer, J. and Sarvate, D. G., (1987), Encryption using Hungarian rings, *Discrete Applied Math.*, **16** , 151-155.

Hammer, J. and Sarvate, D. G., (198?), On the introduction of block designs by graphs, *Mathematics Magazine*, (submitted).

Hammer, J., Sarvate, D. G., and Seberry, J., (198?) A note on orthogonal designs, *Ars Combinatoria*, (to appear).

Hanani, H., (1975), Balanced incomplete block designs and related designs, *Discrete Math*, **11** , 255-369.

Harms, J. J., (1985), Directing cyclic triple systems, Algorithms in Combinatorial Design Theory, *Annals of Discrete Mathematics*, **26**, (edited by C. J. Colbourn and M. J. Colbourn) 221-226.

Harms, J. J. and Colbourn, C. J., (1983), Partitions into directed triple systems, *Ars Combinatoria*, **16**, 21-25.

Hess, P. and Wirl, K., (1983), A voice scrambling system for testing and demonstration, *Cryptography*, (edited by T. Beth), Lecture Notes in Computer Science, **149**, Springer-Verlag, Berlin, 147-156.

Hughes, D. R., (1965), On t-designs and groups, *Am. J. Math.*, **87**, 761-778.

Hussain, Q. M., (1945), On the totality of the solutions for the symmetrical incomplete block designs $\lambda=2$, $K=5$ or 6, *Sankhya*, **7**, Part 2, 204-208.

Hwang, F. K. and Lin, S., (1973), Directed triple systems, *J. Combinatorial Th.*, Ser.A, **14**, 310-318.

Jimbo, M. and Kuriki, S., (1983), On a composition of cyclic 2-designs, *Discrete Math.*, 46, 3, 249-255.

Keifer, J. and Wynn, H. P., (1981), Optimum balanced incomplete block designs for correlated observations, *Ann. Statist.*, **9**, 737-757.

Kharaghani, H., (1985), New class of weighing matrices, *Ars Combinatoria*, **19**, 69-73.

Kohler, E., (1981), k difference-cycles and the construction of cyclic t-designs, *Geometrics and Groups*, Lecture Notes in Mathematics, **893**, Springer-Verlag, Berlin-Heidelberg-New York, 195-203.

Kramer, E. S. and Messner, D., (1976), t-designs on hypergraphs, *Discrete Math.*, **15**, 263-296.

Lam, C. and Seberry, J., (1984), Generalized Bhasker Rao designs, *J. Statist. Plan. and Inf.*, **10**, 83-95.

Lindner, C. C. and Rosa, A., (1975b), Steiner triple systems having a prescribed number of triples in common, *Can. J. Math.*, **27**, 5, 1166-1175.

Lu, J. X., (1984), On large sets of disjoint Steiner triple systems, VI, *J. Combinatorial Th.*, Ser. A, **37**, 189-192.

Mathon, R. and Rosa, A., (1985), Tables of parameters of BIBDs with $r \leq 41$, *Annals of Discrete Mathematics*, **26**, (edited by C. J. Colbourn and M. J. Colbourn), 275-308.

Mendelsohn, N. S., (1971), A natural generalization of Steiner triple systems, *Computers in Number Theory*, (edited by A. O. L. Atkin and B. J. Birch), Academic Press, New York, 323-329.

Mullin, R. C., (1975), A note on balanced weighing matrices, *Combinatorial Mathematics III*, Proceedings of the Third Australian Conference, in Lecture Notes in Mathematics, **452**, Springer-Verlag, Berlin-Heidelberg-New York.

Patwardhan G. A. and Vartak M. N., (1980), On the adjugate of a symmetrical balanced incomplete block design with $\lambda = 1$, *Combinatorics and Graph Theory*, Lecture Notes in Mathematics, **885**, Springer-Verlag Berlin, 133-155.

Peltesohn, R., (1939), Eine Losung der beiden Hefterschen Differenzenprobleme. *Compositio Math.*, **6**, 251-257.

Preece, D. A., (1966a), Some row and column designs for two sets of treatments, *Biometrics*, **22**, 1-25.

Preece, D. A., (1966b), Some balanced incomplete designs for two sets of trements, *Biometrics*, **53**, 497-506.

Preece, D. A., (1976), Non-orthogonal Graeco-Latin designs, *Combinatorial Mathematics iv*, Proceedings of the Fourth Australian Conference on Combinatorial Mathematics, in Lecture Notes in Mathematics, **560**, Springer-Verlag, Berlin-Heidelberg-New York, 7-26.

Raghavarao, D., (1971), *Construction and Combinatorial Problems in Design of Experiments*, Wiley, New York.

Roberts F. S., (1984), *Applied Combinatorics*, Prentice-Hall.

Rodger, C. A., (1986), Triple systems with a fixed number of repeated triples, *J. Australia Math. Soc.*, ser A, **41**, 180-187.

Rodger, C. A., Sarvate, D. G. and Seberry, J., (1987), Colourable designs, new group divisible designs and pairwise balanced designs, *J. Statist. Plan. and Inf.*, **15**, 379-389.

Rosa, A., (1975), A theorem on the maximum number of disjoint Steiner triple systems, *J. Combinatorial Th.* Ser.A, **18**, 305-312.

Rosa, A., (1980), Intersection properties of Steiner systems, *Annals of Discrete Mathematics*, **7**, 115-128.

Saha, G. M., (1973), On construction of T_m -type PBIB designs, *Ann. Inst. Statist. Math.*, **25** (3), 605-616.

Sarvate, D. G., (1984), All directed GDDs with block size three, $\lambda_1=0$, exist, *Utilitas Mathematica*, **26**, 311-317.

Sarvate, D. G., (1985a), Some results on directed and cyclic designs, *Ars Combinatoria*, **19A**, 179-190.

Sarvate, D. G., (1985b), A note on equi-neighboured block designs, *Utilitas Mathematica*, **28**, 91-98.

Sarvate, D. G., (1986a), Block designs without repeated blocks, *Ars Combinatoria*, **21**, 71-87.

Sarvate, D. G., (1986b), All simple BIBDs with block size 3 exist, *Ars Combinatoria*, **21A** , 257-270.

Sarvate, D. G., (1986c), On a BIBD construction, *Ars Combinatoria*, **22**, 165-169.

Sarvate, D. G. and Seberry, J., (1986), Encryption methods based on combinatorial designs, *Ars Combinatoria*, **21A**, 237-246.

Schellenberg, P. J., (1975), A computer construction for balanced orthogonal matrices, *Congressus Numerantium*, Proceedings of Sixth South-eastern Conference on Combinatorics, Graph Theory and Computing, **14** , 513-522.

Schreiber, S., (1974), Some balanced complete block designs, *Israel J. Math.*, **18** , 31-37.

Seberry, J., (1979), A note on orthogonal Graeco-Latin designs, *Ars Combinatoria*, **8**, 85-94.

Seberry, J., (1981), Some families of partially balanced incomplete block designs, *Combinatorial Mathematics IX* (edited by E. J. Billington, S. Oates-Williams and A. P. Street), Lecture Notes in Mathematics, **952**, Springer-Verlag, Berlin-Heidelberg-New York, 378-386.

Seberry, J., (1984), Regular group divisible designs and Bhaskar Rao designs with block size 3, *J. Statist. Plan. and Inf.*, **10** , 69-82.

Seberry, J., (1986), A construction for Williamson-type matrices, *Graphs and Combinatorics*, **2**, 81-87.

Seberry, J., (1987), Generalized Hadamard matrices and colourable designs in the construction of regular GDDs with two associate classes, *J. Statist. Plan. and Inf.*, **15** , 237-246.

Seberry, J., and Skillicorn, D. B., (1980), All directed designs with k=3 exist, *J. Combinatorial Th.* , Ser. A , **29**, 244-248.

Seberry, J. and Whiteman, A. L., (1972), Some class of Hadamard matrices with constant diagonal, *Bull. Austral. Math. Soc*, **7**, 233-249.

Seberry Wallis, J., (1972), Hadamard matrices, part IV, *Combinatorics: Room squares, Sum Free Sets, Hadamard Matrices*, Lecture Notes in Mathematics, **292**, Springer-Verlag, Berlin-Heidelberg-New York.

Seidel, J. J., (1969), Strongly regular graphs, *Recent Progress in Combinatorics*, (edited by W. Tutte), Academic Press, New York, 185-198.

Shrikhande, S. S., (1962), On a two-parameter family of balanced incomplete block designs, *Sankhya*, **24**, Ser A, 33-40.

Simmons, G. J., (1979), Cryptology: The mathematics of secure communication, *The Mathematical Intelligencer*, **1(4)**, 233-246.

Singh, S. J., (1982), Some Bhasker Rao designs and application for k=3, $\lambda = 2$, *University of Indore Research J. Science*, **7**, 8-15.

Singmaster, D., (1984), Hungarian rings groups, *The bulletin of the Institute of Mathematics and its applications*, **20**, 137-139.

Sinha, K., (1978), Partially balanced incomplete block designs and partially balanced weighing designs, *Ars Combinatoria*, **6**, 91-96.

Sinha, K.,(1979), A series of BIB designs, *J. Australian Math. Soc.*, Ser. A, **27**, 88-90.

Sinha, K., (1984), A BIBD arising from a construction for PBIBDs, *Ars Combinatoria*, **18**, 217-219.

Skillicorn, D. B., (1981), *Directed Packings and Covering with Computer Applications*, Ph. D. Thesis, University of Manitoba, Winnipeg.

Skillicorn, D. B., (1983), Complete directed designs, *Congressus Numerantium*, **38**, 247-252.

Skillicorn, D. B. and Stanton, R. G., (1982), The directed packing numbers DD(t, v, v), *Congressus Numerantium*, Proceedings of the Eleventh Manitoba Conference on Numerical Mathematics and Computing, Winnipeg, Manitoba, 1981, **34**, 247-252.

Sloane, N. J. A, (1983), Encrypting by random rotations, *Cryptography*, (edited by T. Beth), Lecture Notes in Computer Science, **149**, Springer-Verlag, Berlin.

Stanton, R. G., (1983), The appropriatness of standard BIBD presentation, *Ars Combinatoria*, **16 A**, 289-296.

Stanton, R. G. and Collens, R. J., (1976), A computer system for research on the family classification of BIBDs, *Colloquio Internazionale Sulle Teoric Combinatorie*, (Roma 1973) Tomo I, Attidei Conmvegni Lincei, **17**, Accad. Naz. Lincei, Rome, 133-169.

Stanton, R. G. and Goulden, I. P., (1981), Graph factorization, general triple systems and cyclic triple systems, *Aequationes Math.*, **22**, 1-28.

Steiner, J., (1853), Combinatorische Aufgabe, *J. reine angew. Math.*, **45**, 181-182.

Sterling, L. S. and Wormald, N., (1976), A remark on the construction of designs for two-way elimination of heterogeneity, *Bull. Austral. Math. Soc.*, **14**, 383-388.

Street, A. P., (1980), Some designs with block size three, *Combinatorial Mathematics VII*, (edited by R. W. Robinson, G. W. Southern and W. D. Wallis), Lecture Notes in Mathematics, **829**, Springer-Verlag, Berlin-Heidelberg-New York, 224-237.

Street A. P. and Wallis W. D., (1984), Combinatorial Theory: An Introduction, Winnipeg, Canada.

Street, D. J., (1981), *Cyclotomy and Designs*, Ph. D. Thesis, University of Sydney.

Street, D. J., (1981a), Bhaskar Rao design from cyclotomy, *J. Austral. Math. Soc.*, Ser. A, **29**, 425-430.

Street, D. J., (1981b), Graeco-Latin and nested row and column designs, *Combinatorial Mathematics VIII*, (edited by K. L. McAvaney), Lecture Notes in Mathematics, **884**, Springer-Verlag, Berlin-Heidelberg-New York, 304-313.

Street, D. J. and Rodger, C. A., (1980), Some results on Bhaskar Rao designs, *Combinatorial Mathematics VII*, (edited by R. W. Robinson, G. W. Southern and W. D. Wallis), Lecture Notes in Mathematics, **829**, Springer-Verlag, Berlin-Heidelberg-New York, 238-245.

Street, D. J. and Seberry, J., (1980), All DBIBDs with block size four exist, *Utilitas Mathematica*, **18**, 383-388.

Street, D. J. and Wilson, W., (1980), On directed balanced incomplete block designs with block size five, *Utilitas Mathematica*, **18**, 161-174.

Teirlinck, L., (1975), On the maximum number of disjoint triple systems, *J. Geometry*, **6(2)**, 93-96.

Tillson, T. W., (1980), A Hamiltonian decomposition of K^*_{2m}, $2m \geq 8$, *J. Combinatorial Th.* Ser.A, **29**, 68-74.

Van Buggenhaut, J., (1974a), On the existence of 2-designs $S_2(2, 3, v)$ without repeated blocks, *Discrete Mathematics*, **8**, 105-109.

Van Buggenhaut, J., (1974b), On the existence of 2-designs $S_3(2, 3, v)$ without repeated blocks, *J. Geometry*, **4**, 1-10.

Vyas, R., (1982), Some Bhaskar Rao designs and applications for $k = 3$, $\lambda = 4$, *University of Indore Research J. Science*, **7**, 16-25.

Wallis, J., (1971), Some results on configurations, *J. Austral. Math. Soc.*, **12**, 378-384.

Wallis, J. and Whiteman, A. L., (1972), Some classes of Hadamard matrices with constant diagonal, *Bull. Austral. Math. Soc.*, **7**, 233-249.

Wallis, W. D., Street, A. P. and Seberry Wallis, J. (1972), *Combinatorics: Room Squares, Sum Free Sets, Hadamard Matrices*, Lecture Notes in Mathematics, **292**, Springer-Verlag, Berlin-Heidelberg-New York.

Wellhausen, E. J., (1943), The accuracy of incomplete block designs on varietal trials in West Virginia, *J. Amer. Soc. of Agronomics*, **35**, 66-76.

Wilson, R. M., (1975), Construction and uses of pairwise balanced designs, *Combinatorics*, (edited by M. Hall, Jr. and J. H. van Lint), Mathematisch Centrum, Amsterdam, 18-45.

Wilson, R. J., (1985), *Introduction to Graph Theory*, Third edition, Longman.

Woolhouse, W.S.B., (1844), Prize question 1733, *Lady's and Gentleman's Diary.*

Yates, F., (1936), Incomplete randomized blocks, *Ann. Eugen.*, **7**, 121-140.

Youden, W. J., (1937), Use of incomplete block replications in estimating Tobacco-Mosaic virus, *Contr. Boyce Thompson Inst.*, **9**, 41-48. 8

SUMMARY

Theory of combinatorial designs with applications
to
encryption and the design of experiments

By

D. G. Sarvate

The main aim of this thesis is to prove that the necessary conditions are sufficient for the existence of various block designs with small block sizes and to explore the use of block designs in encryption and the design of experiments. Some general constructions and results are obtained.

The various designs studied are as follows.

In Chapter 1 block designs are introduced, using graphs, and a construction of PBIBDs, using n-partite graphs, is given.

Chapter 2 deals with directed and cyclic designs of block size 3 and 4. By generalizing results of Hanani, it is proved that the necessary conditions are sufficient for the existence of directed group divisible designs(GDDs) of block sizes 3, 4 and cyclic GDDs of block size 3 except $v = 6$ and group size = 1. Some general results are given. The existence of cyclic BIBD(v, b, r, 4, (4t+2)*) for $v \equiv 0, 1 \pmod 4$ and cyclic BIBD(v, b, r, 4, 4t*) for all $v \geq 4$ is established.

Chapter 3 is on equi-neighboured designs. One of the results proved is that every GDD of block size three, with $\lambda = 3t$, underlies an equi-neighboured GDD.

Chapter 4 is on simple designs. A theorem of R. G. Stanton and R. J. Collens is used to show that the necessary conditions are sufficient for the existence of simple balanced incomplete block designs (simple BIBDs) with block size three. Embedding theorems for simple BIBDs, based on a method of graph factorization, are given.

Coloured designs are in Chapter 5. Many new families of GDDs and BIBDs can be obtained by using construction based on coloured designs. One such construction and an existence theorem for coloured designs are given.

In Chapter 6 some general constructions, based on directed graphs and t-designs, for families of PBIBDs and BIBDs are given.

Generalized Bhaskar Rao designs and orthogonal designs are studied in Chapter 7. It is shown that neither BRD(10,4,2) nor GBRD(7, 4, 4; $Z_2 \times Z_2$) exists. It is shown that the necessary conditions are sufficient for the existence of a GBRD(v, 3, 4t; Z_4) except possibly when (v, t) = (27, 1) or (39, 1). Some new constructions for weighing matrices and orthogonal designs are obtained by extending a method of Kharaghani.

Chapter 8 gives some ideas about applications of designs in encryption. A systematic method to permute the message block, while scrambling, in the message, a number of arbitrary message symbols, is given.

X