ON BALANCED INCOMPLETE BLOCK DESIGNS WITH LARGE NUMBER OF ELEMENTS

HAIM HANANI

1. Introduction. A balanced incomplete block design (BIBD) $B[k, \lambda; v]$ is an arrangement of v distinct elements into blocks each containing exactly k distinct elements such that each pair of elements occurs together in exactly λ blocks.

The following is a well-known theorem [**5**, p. 248].

THEOREM 1. *A necessary condition for the existence of a BIBD* $B[k, \lambda; v]$ *is that*

(1) $\quad \lambda(v-1) \equiv 0 \pmod{k-1}$ *and* $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$.

It is also well known [**5**] that condition (1) is not sufficient for the existence of $B[k, \lambda; v]$.

There is an old conjecture that for any given k and λ condition (1) may be sufficient for the existence of a BIBD $B[k, \lambda; v]$ if v is sufficiently large. It is attempted here to prove this conjecture in some specific cases.

2. Auxiliary lemmas. Let $q = p^\nu$, where p is an odd prime and ν a positive integer. By [**3**, p. 248] there exists a field GF(q) of q elements and an element $x \in \mathrm{GF}(q)$ called a generator of GF(q) such that

$$\{x^s \colon s = 0, 1, \ldots, q-2\} \cup \{0\} = \mathrm{GF}(q).$$

Consider the differences $\{x^\gamma - 1 \colon \gamma = 1, 2, \ldots, q-2\}$. Each of them is some power $\delta(\gamma)$ of x. The number of values of γ such that $\gamma \equiv j \pmod 2$ and $\delta(\gamma) \equiv i \pmod 2$ will be denoted by $M(i, j)$, $i, j = 0, 1$.

LEMMA 1. *Let q be a power of an odd prime. If* $q \equiv 3 \pmod 4$, *then* $M(0, 0) = M(1, 0) = (q-3)/4$; *if* $q \equiv 1 \pmod 4$, *then* $M(0, 0) = (q-5)/4$ *and* $M(1, 0) = (q-1)/4$.

Proof [**11**]. Let x be a generator of GF(q). The differences

$$\{x^\gamma - 1 \colon \gamma = 1, 2, \ldots, q-2\}$$

produce all the powers of x with the exception of $-1 = x^{(q-1)/2}$. Therefore

$$(2) \quad \begin{aligned} &M(0,0) + M(0,1) = (q-1)/2, \quad M(1,0) + M(1,1) = (q-3)/2 \quad \text{for } q \equiv 3 \pmod 4; \\ &M(0,0) + M(0,1) = (q-3)/2, \quad M(1,0) + M(1,1) = (q-1)/2 \quad \text{for } q \equiv 1 \pmod 4. \end{aligned}$$

Received September 10, 1968. Work on this paper was done while the author was at City University of New York.

https://doi.org/10.4153/CJM-1970-008-0 Published online by Cambridge University Press

Let α be an integer $(1 \leqq \alpha \leqq (q-3)/2)$ such that

$$x^{2\alpha} - 1 = x^{2\beta+1} \tag{3}$$

for some β $(0 \leqq \beta \leqq (q-3)/2)$. Multiplying (3) by $x^{-2\beta-1}$ we obtain $x^{2(\alpha-\beta)-1} - 1 = x^{-2\beta-1}$ which shows that $M(1, 1) = M(1, 0)$. From (2) follows $M(1, 0) = (q-3)/4$ for $q \equiv 3 \pmod 4$ and $M(1, 0) = (q-1)/4$ for $q \equiv 1 \pmod 4$. On the other hand, it is clear that $M(0, 0) + M(1, 0) = (q-3)/2$, which proves the lemma.

LEMMA 2. *Let q be a power of an odd prime and let x be a generator of* GF(q). *The differences of the elements* $0, 1, 1, x^2, x^2, x^4, x^4, x^6, x^6, \ldots, x^{q-3}, x^{q-3}$ *are:* $(q-1)/2$ *times the element* 0 *and* $q - 1$ *times each of the elements*

$$1, x, x^2, \ldots, x^{(q-3)/2}. \tag{4}$$

Proof. Clearly, the difference 0 occurs $(q-1)/2$ times. Further, for $q \equiv 3 \pmod 4$, each of the differences

$$|(x^{2\alpha} - 1)x^{2\beta}|, \qquad \alpha = 1, 2, \ldots, (q-3)/4, \quad \beta = 0, 1, \ldots, (q-3)/2, \tag{5}$$

occurs four times and each of the differences

$$|x^{2\beta}|, \qquad \beta = 0, 1, \ldots, (q-3)/2, \tag{6}$$

occurs twice. The differences (5) produce $(q-3)/4$ times each of the elements (4) and the differences (6) produce these elements once each. Accordingly, every element of (4) occurs as difference $4(q-3)/4 + 2 \cdot 1 = q - 1$ times.

Let $q \equiv 1 \pmod 4$. Considering that $|x^{(q-1)/2}| = 1$, each of the differences

$$|(x^{2\gamma} - 1)x^{2\delta}|, \qquad \gamma = 1, 2, \ldots, (q-3)/2, \quad \delta = 0, 1, \ldots, (q-5)/4, \tag{7}$$

occurs four times as well as each of the differences

$$|x^{2\delta}|, \qquad \delta = 0, 1, \ldots, (q-5)/4. \tag{8}$$

By Lemma 1, the differences (7) produce $(q-5)/4$ times the even powers of x and $(q-1)/4$ times the odd powers of x. The differences (8) produce once the even powers of x. Accordingly, each element of (4) occurs as difference $q - 1$ times.

LEMMA 3. *Let $q \equiv 3 \pmod 4$ be a power of a prime and let x be a generator of* GF(q). *The differences of the elements* $0, 0, 1, 1, x^2, x^2, x^4, x^4, x^6, x^6, \ldots, x^{q-3}, x^{q-3}$ are: $(q+1)/2$ *times the element* 0 *and* $q + 1$ *times each of the elements*

$$1, x, x^2, \ldots, x^{(q-3)/2}. \tag{9}$$

Proof. Clearly the difference 0 occurs $(q+1)/2$ times. Further, each of the differences (5) and (6) occurs four times and the proof continues on the same lines as that of Lemma 2.

https://doi.org/10.4153/CJM-1970-008-0 Published online by Cambridge University Press

3. Orthogonal Latin squares. A Latin square of order n ($n \geqq 2$) is an arrangement of n distinct elements in an $n \times n$ matrix in such way that in each row and in each column every element occurs exactly once and in the whole matrix every element occurs exactly n times.

Two Latin squares are said to be orthogonal if for every element a of one square and every element b of the other one there exists exactly one pair of integers i, j such that in the ith row and jth column of the first square is the element a and in the same place in the second square is the element b. r ($r \geqq 2$) Latin squares are said to be mutually orthogonal if any two of them are orthogonal.

Let $N(n)$ denote the maximal number of mutually orthogonal Latin squares of order n. Chowla, Erdős, and Straus proved [**4**] that $N(n)$ tends to infinity with n; in other words we state the following result.

THEOREM 2. *For every positive integer r there exists n_r such that $N(n) \geqq r$ for every $n > n_r$.*

Let n_r be the smallest integer satisfying Theorem 2. The best known estimates for n_r are the following.

THEOREM 3. (i) [**10**]. *For every $r \geqq 2$, $n_r < cr^{42}$, where c is some constant.*
(ii) [**9**; **1**; **2**]. $n_2 = 6$.
(iii) [**8**]. $n_3 \leqq 51$, $n_5 \leqq 62$, $n_{29} \leqq 34{,}115{,}553$.
We may also assume that $n_0 = 0$, $n_1 = 1$.

Let a rectangular $n \times m$ array A of mn elements in n rows and m columns be given. We denote by a group divisible design $\mathrm{GD}[k, \lambda; n \times m]$ an arrangement of the elements of A into blocks each containing exactly k elements such that each pair of elements of distinct columns occurs together in exactly λ blocks, while no pair of elements of the same column occurs together in any block.

By a doubly group divisible design $\mathrm{DGD}[k, \lambda; n \times m]$ we denote an arrangement of the elements of A into blocks of exactly k elements each such that each pair of elements of distinct columns and rows occurs together in exactly λ blocks, while no pair of elements of the same column or the same row occurs together in any block.

The existence of a group divisible design $\mathrm{GD}[k, 1; n \times k]$ is equivalent to the existence of $k - 2$ mutually orthogonal Latin squares of order n. To show this we note that the blocks of $\mathrm{GD}[k, 1; n \times k]$ are of the form

$$\{(a_1; 1), (a_2; 2), \ldots, (a_k; k)\},$$

where $(a_i; i)$, $i = 1, 2, \ldots, k$, is the element of intersection of the a_ith row and ith column in A, and each such block states that on the intersection of the a_{k-1}th row and a_kth column of the jth Latin square comes the element $(a_j; j)$, $j = 1, 2, \ldots, k - 2$.

Let a group divisible design $\mathrm{GD}[k, 1; n \times k]$ be given. Delete the kth column. The blocks which contained any fixed element of the kth column are now dis-

https://doi.org/10.4153/CJM-1970-008-0 Published online by Cambridge University Press

joint and on the other hand they contain all the remaining elements of A. Without loss of generality we may assume that one such family of blocks coincides with the (truncated) rows of A. Delete those blocks (but not their elements). The remaining blocks form a doubly group divisible design $\mathrm{DGD}[k-1; n \times (k-1)]$. By Theorem 2 we have the following result.

THEOREM 4. *If k is a positive integer and $v > n_{k-1}$, then there exists a doubly group divisible design* $\mathrm{DGD}[k, 1; v \times k]$.

4. Balanced incomplete block designs. Let $\mathrm{DGD}[k, 1; v \times k]$ be given. Denote by $(j; i)$, $j = 1, 2, \ldots, v$, $i = 1, 2, \ldots, k$, the element of intersection of the jth row and the ith column in the corresponding array A. The blocks of the $\mathrm{DGD}[k, 1; v \times k]$ have the shape $\{(a_i; i)\colon i = 1, 2, \ldots, k\}$, where $a_i \in \{1, 2, \ldots, v\}$ for $i = 1, 2, \ldots, k$ and $a_i \neq a_h$ for $i \neq h$. We form a configuration C of elements and blocks, taking as elements of C the rows of A, and for every block b of $\mathrm{DGD}[k, 1; v \times k]$ forming a block of C consisting of the rows of A which intersect b. Clearly C is a BIBD $B[k, k(k-1); v]$ and the following result follows from Theorem 4.

THEOREM 5. *If k is a positive integer and $v > n_{k-1}$, then there exists a BIBD,* $B[k, k(k-1); v]$.

Let $\mathrm{DGD}[k, 1; v \times k]$ be given, where k is a power of an odd prime. Consider a set E of $kv + \epsilon$ elements, where $\epsilon = 0$ or 1. Denote the elements of E by (j, g_γ), $j = 1, 2, \ldots, v$, $\gamma = 1, 2, \ldots, k$, where g_γ are distinct elements of $\mathrm{GF}(k)$. In the case that $\epsilon = 1$, denote the additional element by (∞). For every block $\{(a_i; i)\colon i = 1, 2, \ldots, k\}$ of $\mathrm{DGD}[k, 1; v \times k]$ form on the set E the blocks

$$\{(a_1, g_\gamma), (a_i, x^{2([i/2]-1)} + g_\gamma)\colon i = 2, 3, \ldots, k\}, \quad \gamma = 1, 2, \ldots, k,$$

where x is a generator of $\mathrm{GF}(q)$. By Lemma 2, every pair of elements of E, $\{(j, g_\gamma), (h, g_\delta)\}$ with $h \neq j$ occurs together in exactly $k-1$ blocks. Form additional blocks on E as follows: if $\epsilon = 0$, form the blocks

$$\{(j, g_\gamma)\colon \gamma = 1, 2, \ldots, k\}, \qquad j = 1, 2, \ldots, v,$$

$k-1$ times each; if $\epsilon = 1$, form on each of the sets

$$\{(\infty), (j, g_\gamma)\colon \gamma = 1, 2, \ldots, k\}, \qquad j = 1, 2, \ldots, v,$$

all the $k+1$ possible k-tuples. The constructed blocks on E form clearly a BIBD $B[k, k-1; kv + \epsilon]$ and by Theorem 4 we have the following result.

THEOREM 6. *If k is a power of an odd prime and if $v > kn_{k-1} + 1$ satisfies* $v \equiv 0$ or 1 (mod k), *then there exists a BIBD,* $B[k, k-1; v]$.

Let $\mathrm{DGD}[k, 1; v \times k]$ be given, where $k - 1 \equiv 3 \pmod 4$ is a power of a prime. Consider a set E of $(k-1)v + 1$ elements, which we denote by (∞) and (j, g_γ), $j = 1, 2, \ldots, v$, $\gamma = 1, 2, \ldots, k-1$, where g_γ are distinct elements

https://doi.org/10.4153/CJM-1970-008-0 Published online by Cambridge University Press

of GF$(k-1)$. For every block $\{(a_i; i): i = 1, 2, \ldots, k\}$ of DGD$[k, 1; v \times k]$, form on the set E the blocks

$$\{(a_1, g_\gamma), (a_k, g_\gamma), (a_i, x^{2([i/2]-1)} + g_\gamma): i = 2, 3, \ldots, k-1\},$$

$\gamma = 1, 2, \ldots, k-1$, where x is a generator of GF$(k-1)$. By Lemma 3, every pair of elements of E, $\{(j, g_\gamma), (h, g_\delta)\}$ with $h \neq j$, occurs together in exactly k blocks. Form additional blocks on E, namely

$$\{(\infty), (j, g_\gamma): \gamma = 1, 2, \ldots, k-1\},$$

$j = 1, 2, \ldots, v$, k times each. The constructed blocks on E form clearly a BIBD, $B[k, k; (k-1)v+1]$ and by Theorem 4 we have the following result.

THEOREM 7. *If* $k \equiv 0 \pmod 4$ *and* $k-1$ *is a power of a prime and if* $v > (k-1)n_{k-1} + 1$ *satisfies* $v \equiv 1 \pmod{k-1}$, *then there exists a BIBD,* $B[k, k; v]$.

It should be mentioned that for $k \leqq 5$, Theorems 5, 6, and 7 are correct without the restriction that v must be sufficiently large [**6**; **7**].

Putting together Theorems 5, 6, 7 with Theorem 1 we obtain the following result.

THEOREM 8. *Condition* (1) *is necessary and sufficient for the existence of a BIBD,* $B[k, \lambda; v]$, *if* v *is sufficiently large and*

(i) *if* $\lambda = k(k-1)$, *or*

(ii) *if* k *is a power of an odd prime and* $\lambda = k-1$, *or*

(iii) *if* $k - 1 \equiv 3 \pmod 4$ *is a power of a prime and* $\lambda = k$.

REFERENCES

1. R. C. Bose and S. Shrikhande, *On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler*, Trans. Amer. Math. Soc. *95* (1960), 191–209.

2. R. C. Bose, E. T. Parker, and S. Shrikhande, *Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture*, Can. J. Math. *12* (1960), 189–203.

3. R. D. Carmichael, *Introduction to the theory of groups of finite order* (Dover, New York, 1956).

4. S. Chowla, P. Erdős, and E. G. Straus, *On the maximal number of pairwise orthogonal Latin squares of a given order*, Can. J. Math. *12* (1960), 204–208.

5. M. Hall, Jr., *Combinatorial theory* (Blaisdell, Waltham, Massachusetts, 1967).

6. H. Hanani, *The existence and construction of balanced incomplete block designs*, Ann. Math. Statist. *32* (1961), 361–386.

7. ——— *A balanced incomplete block design*, Ann. Math. Statist. *36* (1965), 711.

8. ——— *On the number of orthogonal Latin squares*, J. Combinatorial Theory (to appear).

9. E. Parker, *Construction of some sets of mutually orthogonal Latin squares*, Proc. Amer. Math. Soc. *10* (1959), 946–949.

10. K. Rogers, *A note on orthogonal Latin squares*, Pacific J. Math. *14* (1964), 1395–1397.

11. Th. Storer, *Cyclotomy and difference sets* (Markham, Chicago, 1967).

Technion—Israel Institute of Technology,
Technion City, Haifa

https://doi.org/10.4153/CJM-1970-008-0 Published online by Cambridge University Press