GENERALIZED HADAMARD MATRICES AND ORTHOGONAL ARRAYS OF STRENGTH TWO

S. S. SHRIKHANDE

1. The purpose of this note is to point out some connexions between generalized Hadamard matrices **(4, 5)** and various tactical configurations such as group divisible designs **(3)**, affine resolvable balanced incomplete block designs **(1)**, and orthogonal arrays of strength two **(2)**. Some constructions for these arrays are also indicated.

2. Preliminary results. A balanced incomplete block design (BIBD) with parameters v, b, r, k, λ is an arrangement of v symbols called treatments into b subsets called blocks of $k < v$ distinct treatments such that each treatment occurs in r blocks and any pair of treatments occurs in λ blocks. A symmetrical BIBD (SBIBD) is a BIBD with $v = b$ and hence $r = k$. A BIBD is called resolvable if the blocks can be separated into r sets each forming a complete replication of all the treatments. A resolvable BIBD is called affine resolvable BIBD (ARBIBD) if any two blocks of different sets have the same number of treatments in common. As shown by Bose **(1)**, the parameters of such a design are given in terms of two integers $s \geqslant 2, t \geqslant 0$ by

$$v = sk = s^2[(s-1)t + 1], \qquad b = sr = s(s^2t + s + 1), \qquad \lambda = st + 1.$$

We shall denote this design by $A(s, t)$.

A group divisible design (GDD) is an arrangement of $v = mn$ treatments, partitioned into m sets of n each, in blocks of $k < v$ treatments such that each treatment is replicated in r blocks and any two treatments of the same set (different sets) occur together in λ_1 blocks (λ_2 blocks).

Let G be a module of order mn and N a subgroup of G of order n. Let W be the set of elements of G not in N. A difference set of G relative to N is a set $R = \{r_1, r_2, \ldots, r_k\}$ of distinct elements of G such that for $i \neq j$, the differences $r_i - r_j$ contain only the elements of W, each exactly δ times. It is then obvious that the $b = mn$ blocks obtained by adding each of the elements of G to R generate a symmetrical GDD with

$$v = b = mn, \qquad r = k, \qquad \lambda_1 = 0, \qquad \lambda_2 = \delta,$$

with m sets of n treatments each. We shall call R a difference set for this GDD.

An orthogonal array $[\lambda s^2, t, s, 2]$ of strength 2, t constraints, index λ in s symbols is a matrix of order $(t, \lambda s^2)$ in s distinct symbols with the property that any two of its rows contain all the s^2 ordered pairs exactly λ times. Bose

Received August 16, 1963.

and Bush **(2)** give an upper bound for t in terms of s and λ from which it follows that for $[2s^n, t, s, 2]$

$$t \leqslant 1 + 2(s + s^2 + \ldots + s^{n-1}). \tag{1}$$

We shall denote the orthogonal array $[s^2\{(s-1)t+1\}, s^2t + s + 1, s, 2]$ by the symbol $\mathrm{OA}(s, t)$.

A square matrix H of order h with elements the pth roots of unity is called a generalized Hadamard matrix $(H(p, h))$ if $HH^{cT} = hI_h$. It is easily seen that when p is a prime, $H(p, h)$ can exist only if $h = pt$ where t is a positive integer. Such matrices have been considered by Butson **(4, 5)**. In **(4)** he proves the following theorem.

THEOREM A. *$H(p, 2p^n)$ exists where p is any prime and n is any positive integer.*

3. Hadamard matrices and certain configurations. Denote by $G(s, t)$ the GDD with

$$v = b = (s-1)(s^2t + s + 1), \qquad r = k = s[(s-1)t + 1],$$
$$\lambda_1 = 0, \qquad \lambda_2 = (s-1)t + 1$$

with $m = s^2t + s + 1$ sets of $n = s - 1$ treatments each. We then have the following theorem.

THEOREM 1. (i) *The existence of any one of $A(s, t)$, $G(s, t)$, and $\mathrm{OA}(s, t)$ implies the existence of the other two. If further there exists a difference set R which generates $G(s, t)$, then the* SBIBD *with*

$$v = s(s^2t + s + 1), \qquad r = s^2t + s + 1, \qquad \lambda = st + 1$$

exists.

(ii) *If p is a prime, the existence of $\mathrm{OA}(p, t)$ implies the existence of $H(p, p^2[(p-1)t + 1])$.*

Proof. The equivalence of $A(s, t)$ and $\mathrm{OA}(s, t)$ has been shown by Plackett and Burman **(7)**. We now show the equivalence of $A(s, t)$ and $G(s, t)$. Suppose $A(s, t)$ exists. Then omitting the blocks containing a particular treatment we get an arrangement with $v = b = (s-1)(s^2t + s + 1)$. The omitted blocks contain all the $(s-1)(s^2t + s + 1)$ treatments $st + 1$ times. Hence, for the arrangement so obtained $r = k = s[(s-1)t + 1]$. Further, the blocks of the arrangement can be divided into $s^2t + s + 1$ sets of $s - 1$ each such that any two blocks of the same set are disjoint whereas any two blocks of different sets have exactly $(s-1)t + 1$ treatments in common. It is now obvious that the dual **(9)** of this arrangement is exactly $G(s, t)$. Conversely, given $G(s, t)$, consider its dual which has the same values of v, b, r, k as $G(s, t)$ and in which the blocks are divided into $s^2t + s + 1$ sets S_i of $s - 1$ each such that any two blocks of the same set are disjoint whereas any two blocks from different sets

have exactly $(s-1)t+1$ treatments in common. To each S_i add an additional block of size k containing a new treatment, say ∞, and $k-1$ other treatments so that the new set S_i' of s blocks forms a complete replication of $s^2[(s-1)t+1]$ treatments. Utilizing the fact that any two blocks coming from different S_i's have exactly $(s-1)t+1$ treatments in common, it is easy to see that the same is true for S_i''s. Further, the design given by S_i''s has $b = v + r - 1$. Hence, from the results of Plackett and Burman **(7)** it follows that the blocks of S_i', $i = 1, 2, \ldots, s^2t + s + 1$, give an ARBIBD. This completes the proof of the first part of (i).

To prove the latter part of (i) we note that we can modify the proof given by Butson **(5)** to show that we get a difference set for the factor group G/N which generates the SBIBD with

$$v = s^2t + s + 1, \qquad r = s[(s-1)t+1], \qquad \lambda = (s-1)[(s-1)t+1].$$

The complementary design is then a SBIBD with

$$v = s^2t + s + 1, \qquad r = st + 1, \qquad \lambda = t.$$

The existence of this design together with that of $A(s, t)$ already proved above implies the existence of SBIBD of the theorem as shown by Shrikhande **(8)**.

To prove (ii) consider the array $\mathrm{OA}(p, t)$ where the symbols can be taken as elements of $\mathrm{GF}(p)$. Replacing $x \in \mathrm{GF}(p)$ by ρ^x where ρ is a primitive root of $x^p = 1$, we get a matrix A_1. From A_1 obtain A_i by replacing ρ by ρ^i, $i = 1, 2, \ldots, p-1$; and consider the matrix

$$A = \begin{bmatrix} A_1 \\ A_2 \\ \cdot \\ \cdot \\ \cdot \\ A_{p-1} \\ J' \end{bmatrix}$$

where J' is a row with all elements 1. We show that A is the required Hadamard matrix of the theorem. Obviously any two rows of any A_i are orthogonal. Also J' is orthogonal to all the other rows of A, since each of these rows contains all the pth roots of unity the same number of times. Now consider two rows of A coming one from A_i and the other from A_j, $i \neq j$. If these rows correspond to the same row of A_1, then it is obvious that the ordered pairs

$$\begin{pmatrix} \rho^{xi} \\ \rho^{xj} \end{pmatrix}, \qquad x \in \mathrm{GF}(p),$$

occur in these rows the same number of times and hence these rows are orthogonal. If, however, the rows of A_i and A_j correspond to different rows of A_1, then under each set of ρ^{xi} in the row from A_i the row from A_j contains all the

distinct powers of ρ exactly $(p-1)t+1$ times and hence again the rows are orthogonal.

4. Construction of orthogonal arrays. Let M denote a module of order s and let D be a matrix of t rows and μs columns with elements from M. Then D is called a difference set $D(\mu s, t, s, 2)$ if the ordered differences arising from any two rows of D contain all the elements of M exactly μ times. As shown in **(2)** such a difference set leads to $(\mu s^2, t, s, 2)$ by replacing each element of D by the corresponding row of the addition table of M.

Let p denote a fixed prime and $H=(h_{ij})$ denote an $H(p, pt)$. Each element of h_{ij} is of the form ρ^x where ρ is a primitive pth root of unity and $x \in \mathrm{GF}(p)$. Define $\theta(\rho^x)=x$ and put $E=\theta(H)=(\theta(h_{ij}))$. It then follows that E is a difference set $D(pt, pt, p, 2)$ in the residues (mod p). Utilizing Theorem A, we have

LEMMA 1. *If p is a prime, then for any positive integer n, $D(\mu p, 2p^n, p, 2)$ exists with $\mu = 2p^{n-1}$.*

THEOREM 2. $[2p^{n+1}, 1+2(p+p^2+\ldots+p^n), p, 2]$ *exists for any prime p and any positive integer n.*

Proof. For $n=1$, $D(2p, 2p, p, 2)$ of the above lemma gives $[2p^2, 2p, p, 2]$, which is resolvable, i.e. the $2p^2$ columns can be divided into $2p$ sets of p each such that in any row of the array each set contains all the p symbols exactly once. We can add one more row by putting the symbol x in any two sets, $x \in \mathrm{GF}(p)$. Obviously then we have $[2p^2, 2p+1, p, 2]$. Now suppose that $A(n)=[2p^{n+1}, 1+2(p+\ldots+p^n), p, 2]$ exists for any given n. From the above lemma $D(2p^{n+1}, 2p^{n+1}, p, 2)$ exists and gives rise to $B(n+1)=[2p^{n+2}, 2p^{n+1}, p, 2]$, which is resolvable with $2p^{n+1}$ sets of p columns each. Under the columns of the ith set of $B(n+1)$, write down the ith column of $A(n)$ repeated p times, $i=1, 2, \ldots, 2p^{n+1}$. It is then obvious that we get $A(n+1)$. The proof is thus complete.

For given p and n we note from (1) that the orthogonal array of the above theorem has the maximum possible number of rows. Kempthorne and Addelman **(6)** have given a method not depending upon difference sets for the construction of the above array with p replaced by s, which is a prime power.

We now obtain two composition theorems for orthogonal arrays.

Let $D_i = D(\mu_i s, t_i, s, 2)$, $i=1, 2$, be two difference sets with elements in M. Define the Kronecker sum $D_1 \dot{+} D_2$ to be the matrix of order $(t_1 t_2, \mu_1 \mu_2 s^2)$ obtained by replacing each element $d_1(ij)$ of D_1 by the matrix obtained from D_2 by adding $d_1(ij)$ to all the elements of D_2. We then have

THEOREM 3. *If $D_i = D(\mu_i s, t_i, s, 2)$, $i=1, 2$, are two difference sets with elements in M, then $D = D_1 \dot{+} D_2$ is also a difference set $D(\mu s, t_1 t_2, s, 2)$ where $\mu = \mu_1 \mu_2 s$.*

Proof. Consider any two rows of D which arise from the elements in a given row of D_1. Noting that D_2 is a difference set it is obvious that all the elements of M will occur μs times in the differences arising from these rows. Now consider any two rows of D which arise from the same row of D_2 but different rows of D_1. The result again follows from the fact that D_1 is a difference set. A similar result follows for two rows of D which arise from different rows of both D_1 and D_2, from the fact that both D_1 and D_2 are difference sets.

For any $[\mu s^2, t, s, 2]$ we can choose the s symbols as residues (mod s) and define the Kronecker sum of two arrays in the same manner as indicated above. In a similar manner it is then easy to verify

THEOREM 4. *The existence of* $[\mu_i s^2, t_i, s, 2]$, $i = 1, 2$ *implies the existence of* $[\mu_1 \mu_2 s^4, t_1 t_2, s, 2]$.

REFERENCES

1. R. C. Bose, *A note on the resolvability of balanced incomplete block designs*, Sankhyā, *6* (1942), 105–110.
2. R. C. Bose and K. A. Bush, *Orthogonal arrays of strength two and three*, Ann. Math. Stat., *23* (1952), 508–524.
3. R. C. Bose and T. Shimamoto, *Classification and analysis of partially balanced incomplete block designs with two associate classes*, J. Amer. Stat. Ass., *47* (1952), 151–184.
4. A. T. Butson, *Generalized Hadamard matrices*, Proc. Amer. Math. Soc., *13* (1962), 894–898.
5. ——— *Relations among generalized Hadamard matrices*, Can. J. Math., *15* (1963), 42–48.
6. O. Kempthorne and S. Addelman, *Some main effect plans and orthogonal arrays of strength two*, Ann. Math. Stat., *32* (1961), 1167–1178.
7. R. L. Plackett and J. P. Burman, *Designs of optimum multifactorial experiments*, Biometrika, *33* (1946), 305–325.
8. S. S. Shrikhande, *On the nonexistence of affine resolvable balanced incomplete block designs*, Sankhyā, *11* (1951), 185–186.
9. ——— *On the dual of some balanced incomplete block designs*, Biometrics, *8* (1952), 66–72.

University of Bombay