Journal of Statistical Planning and Inference 4 (1980) 365–368.

A CONSTRUCTION FOR GENERALIZED HADAMARD MATRICES

Jennifer SEBERRY

University of Sydney, Sydney, Australia

Received 13 December 1979; revised manuscript received 7 May 1980
Recommended by R.G. Stanton

Abstract: We prove that if p^r and p^r-1 are both prime powers then there is a generalized Hadamard matrix of order $p^r(p^r-1)$ with elements from the elementary abelian group $Z_p \times \cdots \times Z_p$. This result was motivated by results of Rajkundlia on BIBD's. This result is then used to produce p^r-1 mutually orthogonal F-squares $F(p^r(p^r-1); p^r-1)$.

AMS 1970 Subject Classification: Primary 62K10, 62K15; Secondary 05B15.

Key words and Phrases: F-squares.

1. Introduction

A generalized Hadamard matrix GH(qs, G) over the group G of order q is a $qs \times qs$ matrix GH(qs, G) $= (h_{ij})$ such that

(i) $h_{ij} \in G$ for all $1 \leq i, \quad j \leq qs$

and

$$\text{(ii)} \sum_{k=1}^{qs} h_{ik}h_{jk}^{-1} = \sum_{g \in G} sg,$$

whenever $i \neq j$ where the summation is in the group ring $Z[G]$.

Several families of generalized Hadamard matrices have been found by Butson (1962) and Drake (1978). In Section 2 we give another family motivated by the results of Rajkundlia (1978) on BIBDs. Street (1979) gives another family and discusses the various ways of combining known generalized Hadamard matrices.

Let $A = (a_{ij})$ be an $n \times n$ matrix and let $\Sigma = (c_1, c_2, \ldots, c_m)$ be the ordered set of distinct elements of A. In addition, suppose that for each $k = 1, 2, \ldots, m$, c_k appears precisely λ_k times ($\lambda_k \geq 1$) in each row and column of A. Then, A will be called a *frequency square* or, more concisely, an F-square on Σ of order n and frequency vector $(\lambda_1, \lambda_2, \ldots, \lambda_m)$.

We use the notation $F(n; \lambda)$ to denote an F-square of order n with frequency vector $(\lambda, \lambda, \ldots, \lambda)$. An F-square $F(n; 1)$ is just a latin square of order n.

Given an F-square $F_1(n; \lambda_1, \lambda_2, \ldots, \lambda_k)$ on a k-set $\Sigma = \{a_1, a_2, \ldots, a_k\}$ and an

F-square $F_2(n; u_1, u_2, \ldots, u_t)$ on a t-set $\Omega = \{b_1, b_2, \ldots, b_t\}$. Then we say F_2 and F_1 are *mutually orthogonal* F-squares if upon superposition of F_2 on F_1, a_i appears $\lambda_i u_j$ times with b. For more details and constructions see Hedayat and Seiden (1970).

In Section 3 we discuss how to construct mutually orthogonal F-squares from generalized Hadamard matrices.

2. A construction for generalized Hadamard matrices

The following theorem is motivated by an example in Rajkundlia's Ph.D. dissertation.

Theorem 1. *Suppose p^r and $p^r - 1$ are both prime powers. Then there is a* $\mathrm{GH}(p^r(p^r-1), C_{p^r})$ *where C_{p^r} is the elementary abelian group $Z_p \times Z_p \times \cdots \times Z_p$.*

Proof. We first give a construction and then prove it gives the required generalized Hadamard matrix. Proceed as follows:

Step 1. Let the elements of C_{p^r} be $e, x_1, \ldots, x_{p^r-1}$.

Step 2. Write the multiplication table of the group with first row and column $e, x_1, \ldots, x_{p^r-1}$. Write C for the core of this multiplication table (i.e. with the first row and column removed). Then $C = (c_{ij})$ is a matrix of order $p^r - 1$ with the property that

$$\sum_{k=1}^{p^r-1} c_{ik} c_{jk}^{-1} = (p^r - 1)g$$

for g a non-identity element of the group.

Step 3. Write the generalized Hadamard matrix $\mathrm{GH}(p^r, C_{p^r})$ of order p^r with first row and column normalized to be all the identity e and the second row and column rearranged to be $e, x_1, \ldots, x_{p^r-1}$. Remove the first row and column to obtain its core $K = (k_{ij})$. Now

$$\sum_{h=1}^{p^r-1} k_{ih} k_{jh}^{-1} = C_{p^r} - \{e\},$$

where e is the identity element i.e. every element of the group except the identity element exactly once.

Step 4. Let $Y = (y_{ij})$ be the generalized Hadamard matrix of order $p^r - 1$ normalized as in 3). Write A^{ij} for the matrix representation of y_{ij}.

Step 5. Form a block matrix $D = (d_{ij})$ whose ij element is: ij element of C times KA^{ij}, where C, K and A^{ij} are defined in 2), 3) and 4) respectively.

Step 6. Take the matrix $Y = \mathrm{GH}(p^r, C_{p^r})$ obtained in 3). Let $\mathbf{s} = (1, 1, \ldots, 1)$ be a $1 \times p^r - 1$ matrix of ones. Form G_a from Y by removing the first column and

second row and form G_b from Y by removing the first row and second column. Now let $A = G_a \times s$ and $B = G_b \times s^T$ which are of sizes $(p^r-1)\times(p^r-1)^2$ and $(p^r-1)^2\times(p^r-1)$ respectively. Let E be the $(p^r-1)\times(p^r-1)$ matrix with every element e.

Then we assert

$$\begin{bmatrix} E & A \\ B & D \end{bmatrix}$$

is the required GH$(p^r(p^r-1), C_{p^r})$.

Proof of Assertion. As noted any two rows a, b of C have product $p^r g_{ab}$ where $g_{ab} \in C_{p^r}$ while any two rows of K have product $C_{p^r}/\{e\}$. If we call $D = (X_{ij})$ a block matrix, with blocks of order p^r-1, it is clear any two rows within $X_{i2}, \ldots, X_{i(p^r-1)}$ have product $(p^r-1)C_{p^r}/(p^r-1)\{e\}$. Hence with the border attached we have $(p^r-1)C_{p^r}$. Consider the products across from row l to row m in

$$X_{i2}\cdots X_{i(p^r-1)}$$
$$X_{j2}\cdots X_{j(p^r-1)}.$$

The effect of the permutation matrix of order p^r-1 is to ensure that the lth row of K is forced to multiply onto each of the p^r-1 rows of K once, giving g_{ii} (p^r-1) times and $C_{p^r}/\{g_{ii}\}$ (p^r-2) times respectively. So we need one extra copy of $C_{p^r}/\{g_{ij}\}$ and the border was chosen so g_{ij} is not a product in X_{i1} and X_{j1} but all the other elements of C_{p^r} are.

Using a similar argument on the columns of D we see that the necessary border has been chosen. Now considering $X_{12}, \ldots, X_{1p^r-1}$ we see X_{11} must contain only the identity element of C_{p^r}.

3. Construction for orthogonal *F*-squares

Let $A = (a_{ij})$ be a GH(sq, G) where $|G| = q$ (or more generally let $A = (a_{ij})$ be $r \leq sq$ rows of a GH(sq, G)). Then we may construct $sq-1$ (respectively $r-1$) mutually orthogonal F-squares in the following manner.

(i) Normalize A by appropriate column multiplication so the first row of A consists of sq copies of the identity element of G.

(ii) Let $(b^i_{1j}) = (a_{ij})$ be the first row of $sq-1$ (respectively $r-1$) matrices B_i.

(iii) The square is obtained from the first row by multiplying it by s copies of G in some order, each square is obtained using the same sequence of elements.

Proof that we have orthogonal *F*-squares. Since the first row of each B_i contains each element of G s times it is clear that this process gives each element s times in each column of B_i.

For orthogonality we need to compare all the pairs of elements (b^i_{hj}, b^k_{hj}), $i \neq j$, and show that each (f, g), $f, g \in G$ occurs s^2 times.

The properties of the generalized Hadamard matrix ensures that $b^i_{1j}(b^k_{1j})^{-1}$, $j = 1, \ldots, qs$ runs through each element of G s times. Hence the pairs $(b^i_{hj}, b^k_{hj}) = (b^i_{1j}g, b^k_{1j}g)$, $g \in G$, obtained by the construction have b^i_{hj} take each element of G s times, and the product $b^i_{1j}g(b^k_{1j}g)^{-1}$ constant. Hence each pair (f, g), $f, g \in G$, occurs s^2 times as required.

We note that if we had started with a GH $(|G|, G)$ we would have obtained $|G|-1$ mutually orthogonal latin squares (as observed by many authors). Also, if we had started with r rows of a GH $(|G|, G)$ we would have $r-1$ mutually orthogonal latin squares (as used by Johnson, Dulmage, Mendelsohn (1961)).

We summarize these results in the following theorem.

Theorem 2. *Suppose that there exist $p \leq sq$ rows of a generalized Hadamard matrix* GH(sq, G) *where $|G| = q$. Then there exist $p-1$ mutually orthogonal F-squares $F(qs; s)$.*

In particular if p^r and $p^r - 1$ are both prime powers there exists a set of $p^r - 1$ mutually orthogonal F-squares $F(p^r(p^r-1); p^r - 1)$.

References

Butson, A.T. (1962). Generalized Hadamard matrices. *Proc. Amer. Math. Soc.* 13, 894–898.

Butson, A.T. (1963). Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences. *Cahad. J. Math.* 15, 42–48.

Drake, D.A. (1978). Partial λ-geometries and generalized Hadamard matrices over groups. (To appear in *Canad. J. Math.*)

Hedayat, A. and E. Seiden (1970). F-square and orthogonal F-squares design: A generalization of Latin square and orthogonal Latin squares design. *Ann. Math. Statist.* 41, 2035–2044.

Johnson, D.M., A.L. Dulmage and N.S. Medelsohn (1961). Orthomorphisms of groups and orthogonal latin squares I. *Canad. J. Math.* 13, 356–372.

Rajkundlia, D. (1978). Some techniques for constructing new infinite families of balanced incomplete block designs. Ph.D. Dissertation, Queen's University, Kingston, Ontario, Canada.

Seberry, J. (1978). Some remarks on generalized Hadamard matrices and theorems of Rajkundlia on SBIBD's. (To appear in *Combinatorial Mathematics VI*, Springer-Verlag, Berlin-Heidelberg-New York.)

Street, D.J. (1979). Generalized Hadamard matrices, orthogonal arrays and F-squares. Preprint.