A construction for generalized Hadamard matrices

Jennifer Seberry

*University of Wollongong, jennie@uow.edu.au*
A construction for generalized Hadamard matrices

Abstract
We prove that if $p^v$ 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 $Z_p \times \ldots \times Z_p$. 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 $F(p^{r(p^{r-1})}; p^{r-1})$.

Disciplines
Physical Sciences and Mathematics

Publication Details

This journal article is available at Research Online: http://ro.uow.edu.au/infopapers/1001
A CONSTRUCTION FOR GENERALIZED HADAMARD MATRICES

Jennifer SEBBERRY

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 \( \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p \). This result was motivated by results of Rajkundlia on BIBDs. 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 \( 1 \leq i, j \leq qs \)

and

(ii) \( \sum_{k=1}^{qs} h_{ik} h_{jk}^{-1} = \sum_{g \in G} s_g \)

whenever \( i \neq j \) where the summation is in the group ring \( \mathbb{Z}[G] \).

Several families of generalized Hadamard matrices have been found by Busson (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 \( \lambda_k \) 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 \( \Sigma \) 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 $\Omega = \{b_1, b_2, \ldots, b_k\}$. Then we say $F_2$ and $F_t$ are mutually orthogonal $F$-squares if upon superposition of $F_2$ on $F_t$, $u_i$ appears $\lambda(u_i, b)$ 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 $p'$ and $p' - 1$ are both prime powers. Then there is a GH($p'(p' - 1), C_{p'}$) where $C_{p'}$ is the elementary abelian group $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.

**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 $C_{p'}$ be $e, x_1, \ldots, x_{p'-1}$.

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

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

for $g$ a non-identity element of the group.

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

$$\sum_{k=1}^{p'-1} k_{ik}k_{ik}^{-1} = C_{p'}/\{e\}$$

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 $p' - 1$ normalized as in 3). Write $A^e$ for the matrix representation of $y_{ij}$.

**Step 5.** Form a block matrix $D = (d_{ij})$ whose $ij$ element is: if element of $C$ times $KA^0$, where $C, K$ and $A^0$ are defined in 2), 3) and 4) respectively.

**Step 6.** Take the matrix $Y = \text{GH}(p', C_{p'})$ obtained in 3). Let $s = (1, 1, \ldots, 1)$ be a $1 \times p' - 1$ matrix of ones. Form $G_s$ from $Y$ by removing the first column and
second row and form $G_0$, 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 $(p' - 1) \times (p' - 1)^2$ and $(p' - 1)^2 \times (p' - 1)$ respectively. Let $E$ be the $(p' - 1) \times (p' - 1)$ matrix with every element $e$.

Then we assert

\[
\begin{bmatrix}
E & A \\
B & D
\end{bmatrix}
\]

is the required $\text{GH}(p'(p' - 1), C_{p'})$.

**Proof of Assertion.** As noted any two rows $a, b$ of $C$ have product $p'G_{ab}$, where $G_{ab} \in C_{p'}$ while any two rows of $K$ have product $C_{p'}/(e)$. If we call $D = (X_0)$ a block matrix, with blocks of order $p' - 1$, it is clear any two rows within $X_{1}, \ldots, X_{(p'-1)}$ have product $(p' - 1)C_{p'}/(p' - 1)[e]$. Hence with the border attached we have $(p' - 1)C_{p'}$. Consider the products across from row $l$ to row $m$ in

\[
X_{12} \cdots X_{(p' - 1)} \\
X_{12} \cdots X_{(p' - 1)}.
\]

The effect of the permutation matrix of order $p' - 1$ is to ensure that the $l$th row of $K$ is forced to multiply onto each of the $p' - 1$ rows of $K$ once, giving $G_{a_i}$ $(p' - 1)$ times and $C_{p'}/G_{a_i}$ $(p' - 2)$ times respectively. So we need one extra copy of $C_{p'}/G_{a_i}$ and the border was chosen so $G_{a_i}$ is not a product in $X_1$ and $X_1$ but all the other elements of $C_{p'}$ are.

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

3. **Construction for orthogonal $F$-squares**

Let $A = (a_i)$ be a $\text{GH}(sq, G)$ where $|G| = q$ (or more generally let $A = (a_i)$ be $r \times sq$ rows of a $\text{GH}(sq, G)$. 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 $(b_1, \ldots, b_r)$ 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 \((b_{i}^{k}, b_{i}^{k})\), \(i \neq j\), and show that each \((f_{i}g), f, g \in G\) occurs \(s^2\) times.

The properties of the generalized Hadamard matrix ensures that \(b_{i}^{k}(b_{i}^{k})^{-1}\), \(j = 1, \ldots, qs\) runs through each element of \(G\) \(s\) times. Hence the pairs \((b_{i}^{k}, b_{i}^{k}) = (b_{i}^{k}g, b_{i}^{k}g), g \in G\), obtained by the construction have \(b_{i}^{k}\) take each element of \(G\) \(s\) times, and the product \(b_{i}^{k}g(b_{i}^{k}g)^{-1}\) constant. Hence each pair \((f_{i}g), f, g \in G\), 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 \(\text{GH}(sq, G)\) where \(|G| = q\). Then there exist \(p - 1\) mutually orthogonal F-squares \(F(qs; s)\).

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

**References**


