Available online at www.sciencedirect.com

ScienceDirect

Discrete Mathematics 308 (2008) 2868–2884

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Power Hadamard matrices

R. Craigen[1], R. Woodford[2]

Department of Mathematics, University of Manitoba, Winnipeg, Canada

Received 28 July 2003; received in revised form 18 February 2005; accepted 21 June 2006
Available online 8 June 2007

Abstract

We introduce *power Hadamard matrices*, in order to study the structure of (group) generalized Hadamard matrices, Butson (generalized) Hadamard matrices and other related orthogonal matrices, with which they share certain common characteristics. The new objects turn out to be as interesting, and perhaps as useful, as the objects that motivated them.

We develop a basic theory of power Hadamard matrices, explore these relationships, and offer some new insights into old results. For example, we show that all 4×4 Butson Hadamard matrices are equivalent to circulant ones, and how to move between equivalence classes.

We provide, among other new things, an infinite family of circulant Butson Hadamard matrices that extends a known class to include one of each positive integer order.

Dedication: In 1974 Jennifer Seberry (Wallis) introduced what was then a totally new structure, orthogonal designs, in order to study the existence and construction of Hadamard matrices. They have proved their worth for this purpose, and have also become an object of interest for their own sake and in applications (e.g., [H.J.V. Tarok, A.R. Calderbank, Space-time block codes from orthogonal designs, IEEE Trans. Inf. Theory 45 (1999) 1456–1467. [26]]). Since then many other generalizations of Hadamard matrices have been introduced, including some discussed herein. In the same spirit we introduce a new object showing this kind of promise.

Seberry's contributions to this field are not limited to her own work, of which orthogonal designs are but one example—she has mentored many young mathematicians who have expanded her legacy by making their own marks in this field. It is fitting, therefore, that our contribution to this volume is a collaboration between one who has worked in this field for over a decade and an undergraduate student who had just completed his third year of study at the time of the work.

Keywords: Hadamard matrix; Generalized Hadamard matrix; Butson Hadamard matrix

1. *GH*'s and *BH*'s

There are many ways to generalize Hadamard matrices. Let us begin by discussing two of them.

1.1. Butson Hadamard matrices

In 1962 Butson [2] introduced what he called "generalized Hadamard matrices", and which we shall call *Butson Hadamard matrices*, namely $n \times n$ matrices H whose entries are complex roots of unity and which satisfy

$$HH^* = nI, \tag{1}$$

[1] Supported by an NSERC grant.
[2] Supported by an NSERC Undergraduate Student Research Award.

E-mail addresses: craigenr@cc.umanitoba.ca (R. Craigen), rogerw@math.ubc.ca (R. Woodford).

0012-365X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2006.06.050

where H^* is the Hermitian adjoint of H. Since H has only finitely many entries, there is some number k such that all of the entries of H are kth roots of unity. For brevity we shall say that H is a $BH(n, k)$, or simply a BH, if n, k are unknown or unimportant in context.

For example, if γ is a primitive cube root of unity, then the following circulant matrix,

$$H = \begin{pmatrix} 1 & \gamma & \gamma \\ \gamma & 1 & \gamma \\ \gamma & \gamma & 1 \end{pmatrix}, \tag{2}$$

is a $BH(3, 3)$, for

$$\begin{aligned} HH^* &= \begin{pmatrix} 1 & \gamma & \gamma \\ \gamma & 1 & \gamma \\ \gamma & \gamma & 1 \end{pmatrix} \begin{pmatrix} 1 & \gamma^2 & \gamma^2 \\ \gamma^2 & 1 & \gamma^2 \\ \gamma^2 & \gamma^2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 1+\gamma+\gamma^2 & 1+\gamma+\gamma^2 \\ 1+\gamma+\gamma^2 & 3 & 1+\gamma+\gamma^2 \\ 1+\gamma+\gamma^2 & 1+\gamma+\gamma^2 & 3 \end{pmatrix} = 3I. \end{aligned}$$

We will encounter many circulants in this paper, so we shall write $\mathrm{circ}(\mathbf{r})$ to denote the circulant matrix determined by first row $\mathbf{r}$. For example, in (2), $H = \mathrm{circ}(1, \gamma, \gamma)$.

If one multiplies all the entries in any row or column of a Butson Hadamard matrix H by a root of unity, permutes the rows or columns, or performs a sequence of such operations, another Butson Hadamard matrix is obtained. We say that matrices thus obtained from H are (*Butson-*)*equivalent to* H, and the set of all matrices equivalent to H is its (*Butson-*)*equivalence class*.

Observe that every $BH(n, k)$ is also a $BH(n, tk)$, for any positive integer t. But there is always a smallest value of h for which it is a $BH(n, h)$: the least common multiple of the multiplicative orders of its entries. Necessarily, $h|k$. Let h_0 be the least possible value of h among all the BH's equivalent to H. We call this number the *characteristic* of the class (or of H).

Every $BH(n, k)$ can be transformed into an equivalent BH with first row and column consisting of 1's, as follows. Permute the rows and columns of the matrix so that the (i, j) entry is moved into the $(1, 1)$ position. Then divide every row by its first entry, and then do the same for every column. We call this procedure *normalizing the matrix relative to the* (i, j) *position*.

Since there are n^2 choices for the pair (i, j), a Butson Hadamard matrix can be normalized in n^2 essentially different ways—"essentially", because we have not specified the final order of rows other than the ith and columns other than the jth. The $(n-1) \times (n-1)$ matrix obtained by stripping off the first row and column of a normalized matrix is called its *core*.

Normalizing a matrix may lead to several different cores. However, there are not necessarily many distinct normal forms—there may be only one: normalizing (2) relative to any position in the matrix always gives (up to permutations of the core) the following matrix.

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \gamma & \gamma^2 \\ 1 & \gamma^2 & \gamma \end{pmatrix}.$$

Lemma 1. *The characteristic*, h_0, *of an equivalence class of BH's is equal to the least common multiple of the multiplicative orders of the entries of any normalized matrix in the class. Further*, *if some matrix in the class is a* $BH(n, k)$, *then* $h_0|k$.

Proof. Given that H is a $BH(n, k)$, the minimum value with which k can be replaced is the least common multiple of the multiplicative orders of the entries of H.

Normalizing H involves permuting the entries and dividing by kth roots of unity, so the normalized matrix H' will remain a $BH(n, k)$, although it might also be a $BH(n, h)$ for some $h < k$, $h|k$. Since normalizing does not increase the