Discrete Mathematics 341 (2018) 2387–2397

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Mappings of Butson-type Hadamard matrices[☆]

Patric R.J. Östergård [*], William T. Paavola

Aalto University School of Electrical Engineering, Department of Communications and Networking, P.O. Box 15400, 00076 Aalto, Finland

ARTICLE INFO

Article history:
Received 24 January 2018
Received in revised form 14 May 2018
Accepted 17 May 2018

Keywords:
Butson-type Hadamard matrix
Classification
Complex matrix
Monomial equivalence
Mapping

ABSTRACT

A BH(q, n) Butson-type Hadamard matrix H is an $n \times n$ matrix over the complex qth roots of unity that fulfils $HH^* = nI_n$. It is well known that a BH$(4, n)$ matrix can be used to construct a BH$(2, 2n)$ matrix, that is, a real Hadamard matrix. This method is here generalised to construct a BH(q, pn) matrix from a BH(pq, n) matrix, where q has at most two distinct prime divisors, one of them being p. Moreover, an algorithm for finding the domain of the mapping from its codomain in the case $p = q = 2$ is developed and used to classify the BH$(4, 16)$ matrices from a classification of the BH$(2, 32)$ matrices.

1. Introduction

A BH(q, n) *Butson-type Hadamard matrix* H is an $n \times n$ matrix with entries that are complex qth roots of unity, such that $HH^* = nI_n$ where H^* denotes the conjugate transpose of H and I_n is the $n \times n$ identity matrix [1]. Butson-type Hadamard matrices generalise (real) Hadamard matrices, which are BH$(2, n)$ matrices. For more information about Hadamard matrices in general and Butson-type Hadamard matrices in particular, see, for example, [5,14,17].

An interesting open problem in this area is the *Hadamard Conjecture*, which asserts that BH$(2, n)$ matrices exist whenever n is divisible by 4. With respect to this conjecture, the BH$(4, n)$ matrices have also received attention. The following theorem is [2, Theorem 1]; Turyn [18] gives credit to Williamson [19] for some of the underlying theory.

Theorem 1. *If there is a* BH$(4, n)$ *matrix, then there is a* BH$(2, 2n)$ *matrix.*

If the *Complex Hadamard Conjecture* – saying that BH$(4, n)$ matrices exist whenever n is divisible by 2 – is true, then Theorem 1 implies that the Hadamard Conjecture is also true. (The name of this conjecture comes from the fact that BH$(4, n)$ matrices have been called complex Hadamard matrices and quaternary complex Hadamard matrices in the literature.)

An increasing interest in BH(q, n) matrices with $q \notin \{2, 4\}$ has raised the question whether there are results similar to that in Theorem 1 for other values of q. One such result was obtained by Compton, Craigen, and de Launey [3].

Theorem 2. *If there is a* BH$(6, n)$ *matrix with no entries in* $\{-1, 1\}$, *then there is a* BH$(2, 4n)$ *matrix.*

Theorem 2 can further be seen as a corollary of Theorem 1 and the following result from [12].

Theorem 3. *If there is a* BH$(6, n)$ *matrix with no entries in* $\{-1, 1\}$, *then there is a* BH$(4, 2n)$ *matrix.*

☆ Supported in part by the Academy of Finland, Grant No. 289002.

* Corresponding author.
E-mail addresses: patric.ostergard@aalto.fi (P.R.J. Östergård), william.paavola@aalto.fi (W.T. Paavola).

https://doi.org/10.1016/j.disc.2018.05.012
0012-365X/

Further work on generalising these theorems has been carried out by Egan and Ó Catháin [4].

In this paper, we generalise Theorem 1 and show that a BH(q, pn) matrix can be constructed from a BH(pq, n) matrix, where q is divisible by at most two distinct prime numbers, and p is one of them. This is the topic of Section 2. In Section 3, we discuss equivalence of Butson-type Hadamard matrices, especially in the context of the results of Section 2. In Section 4, we consider the computational problem of finding the domain of the mapping considered in Section 2 when $p = q = 2$. Specifically, we develop an algorithm for classifying the BH(4, n) matrices from a classification of the BH(2, 2n) matrices, and apply this to the classification of the BH(2, 32) matrices carried out by Kharaghani and Tayfeh-Rezaie [8,9]. These results corroborate the computational classification of BH(4, 16), obtained recently in [12] using different techniques.

2. Mappings of matrices

We denote the (i, j)th entry of a matrix M by M_{ij} and the set of qth roots of unity by

$$\Omega_q := \left\{\omega \in \mathbb{C} : \omega^q = 1\right\}.$$

Some types of mappings for Butson-type Hadamard matrices are well known and have been thoroughly studied; perhaps the most basic and natural one is the Kronecker product.

Definition 1. Let A be a $n \times n$ matrix and B a square matrix. The Kronecker product of A and B is defined as

$$A \otimes B = \begin{bmatrix} A_{11}B & \dots & A_{1n}B \\ \vdots & & \vdots \\ A_{n1}B & \dots & A_{nn}B \end{bmatrix}.$$

Lemma 1. *$(A \otimes B)(C \otimes D) = AC \otimes BD$ whenever AC and BD are defined.*

It is easy to show that the Kronecker product of a BH(q, n) matrix and a BH(q, n') matrix is a BH(q, nn') matrix. In this straightforward mapping only the matrix dimensions change. We shall now consider mappings from BH(q, n) matrices to BH(q', n') matrices, where $q' < q$. For this we need some definitions.

Definition 2. The filtering function $f_q : \mathbb{C} \to \Omega_q \cup \{0\}$ is

$$f_q(x) := \begin{cases} x & \text{if } x \in \Omega_q, \\ 0 & \text{otherwise.} \end{cases}$$

When applied to a matrix H, $f_q(H)$ acts elementwise. For a given root of unity ζ, we further define $F_{k,q,\zeta}(H) := f_q(\zeta^k H)$.

Lemma 2. *Let $q = p^a r^b$, $a \geq 1$, $b \geq 0$, where p and r are primes. If H is a BH(pq, n) matrix and $\zeta \in \Omega_{pq} \setminus \Omega_q$, then $H = \sum_{k=0}^{p-1} \zeta^{-k} F_{k,q,\zeta}(H)$.*

Proof. The (multiplicative) cyclic group G over Ω_q is a subgroup of the (multiplicative) cyclic group G' over Ω_{pq}. The result follows if we can show that for an arbitrary element $a \in \Omega_{pq}$, the elements $a\zeta^0, a\zeta^1, \dots, a\zeta^{p-1}$ form a transversal of the cosets of G in G', whereby exactly one of the elements is in Ω_q. Indeed, if $a\zeta^i$ and $a\zeta^j$ with $0 \leq i < j \leq p-1$ would belong to the same coset, then we would have $\zeta^{j-i} \in \Omega_q$, and then $\zeta \in \Omega_{q(j-i)}$. However, since $(j-i)$ and p share no prime divisors, we have $\Omega_{pq} \cap \Omega_{q(j-i)} = \Omega_q$, so this would further imply that $\zeta \in (\Omega_{pq} \setminus \Omega_q) \cap \Omega_{q(j-i)} = \emptyset$, a contradiction. □

Definition 3. Let $R_{m,p,\zeta} := R_{p,\zeta} \otimes I_{m/p}$, where m is divisible by p and $R_{p,\zeta}$ is the $p \times p$ monomial matrix

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & \zeta^{-p} \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ & & \ddots & & \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}.$$

Proving the following properties of the $m \times m$ matrix $R_{m,p,\zeta}$ is a matter of direct calculation. Similar properties hold for $R_{p,\zeta}$.

Lemma 3. *$R_{m,p,\zeta} R^*_{m,p,\zeta} = I_m$ and $R^p_{m,p,\zeta} = \zeta^{-p} I_m$.*

Definition 4. For a BH(pq, n) matrix H, a BH(q, m) matrix C, and $\zeta \in \Omega_{pq} \setminus \Omega_q$, let

$$L(H, C, \zeta) := \sum_{k=0}^{p-1} R^k_{m,p,\zeta} C \otimes F_{k,q,\zeta}(H).$$