Journal of Discrete Algorithms 34 (2015) 70–77

Contents lists available at ScienceDirect

Journal of Discrete Algorithms

www.elsevier.com/locate/jda

Uniqueness of Butson Hadamard matrices of small degrees

Mitsugu Hirasaka [a,1], Kyoung-Tark Kim [b,*,2], Yoshihiro Mizoguchi [c]

[a] Department of Mathematics, Pusan National University, Jang-jeon dong, Busan, Republic of Korea
[b] Shanghai Jiao Tong University, 800 Dongchuan Road, Minhang District, Shanghai, China
[c] Institute of Mathematics for Industry, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan

ARTICLE INFO

Article history:
Received 13 January 2014
Received in revised form 30 April 2015
Accepted 27 May 2015
Available online 1 June 2015

Keywords:
Hadamard matrix
Projective plane
Butson Hadamard matrix
Fourier matrix

ABSTRACT

Let $\mathrm{BH}_{n\times n}(m)$ be the set of $n \times n$ Butson Hadamard matrices where all the entries are m-th roots of unity. For $H_1, H_2 \in \mathrm{BH}_{n\times n}(m)$, we say that H_1 is *equivalent* to H_2 if $H_1 = PH_2Q$ for some monomial matrices P and Q whose nonzero entries are m-th roots of unity. In the present paper we show by computer search that all the matrices in $\mathrm{BH}_{17\times 17}(17)$ are equivalent to the Fourier matrix of degree 17. Furthermore we shall prove that, for a prime number p, a matrix in $\mathrm{BH}_{p\times p}(p)$ which is not equivalent to the Fourier matrix of degree p gives rise to a non-Desarguesian projective plane of order p.

1. Introduction

Let m and n be positive integers. We shall denote by $\mathrm{BH}_{n\times n}(m)$ the set of $H \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ such that $HH^* = nI_n$ and each entry of H is an m-th root of unity, where H^* is the conjugate transpose of H and I_n is the $n \times n$ identity matrix. Following [3], we call a matrix in $\mathrm{BH}_{n\times n}(m)$ a *Butson Hadamard matrix*.

We can give an equivalence relation on the set $\mathrm{BH}_{n\times n}(m)$ as follows. Two matrices H_1 and H_2 in $\mathrm{BH}_{n\times n}(m)$ are *equivalent* if H_2 can be obtained from H_1 via a finite sequence of the following operations:

(O1) a permutation of two rows (columns);
(O2) a multiplication of a row (column) by an m-th root of unity.

In fact there are so many works on Butson Hadamard matrices, and it is known that these studies have applications to many areas. (See e.g. [1,4].) However, the fundamental questions for the existence or non-existence of Butson Hadamard matrices with various parameters n and m are normally difficult to answer. One of the most well-known non-existence results is the theorem of Butson:

Theorem 1.1. *(See [3, Theorem 3.1, p. 895].) If p is a prime number, then $\mathrm{BH}_{n\times n}(p) = \emptyset$, unless $n = pt$ where t is a positive integer.*

* Corresponding author.
E-mail addresses: hirasaka@pusan.ac.kr (M. Hirasaka), kyoungtarkkim@gmail.com (K.-T. Kim), ym@imi.kyushu-u.ac.jp (Y. Mizoguchi).
[1] This work was supported by the Financial Supporting Project of Long-term Overseas Dispatch of PNU's Tenure-track Faculty, 2012.
[2] This work was supported by Kyushu University Friendship Scolarship.

http://dx.doi.org/10.1016/j.jda.2015.05.009
1570-8667/

In the present paper we focus on the matrices in $\mathrm{BH}_{p\times p}(p)$ where p is a prime number. Recall that the *Fourier matrix F_p of degree p* is a $p \times p$ complex matrix defined as follows:

$$F_p := \left(\exp \frac{2\pi\sqrt{-1}\,ij}{p}\right)_{0\le i,j\le p-1}.$$

It is well known (or see Remark 2.3 below) that F_p belongs to $\mathrm{BH}_{p\times p}(p)$ for each prime number p. However, it is still open whether or not every matrix in $\mathrm{BH}_{p\times p}(p)$ is equivalent to F_p. On the other hand, it would be an interesting result if we could find a Butson Hadamard matrix in $\mathrm{BH}_{p\times p}(p)$ which is not equivalent to F_p, because such a matrix gives rise to a non-Desarguesian projective plane of order p. (This is a main result of Section 3. See Theorem 3.4 below.)

If one follows the simple method as stated in Proposition 2.4 below (or see Theorem 2.7 below), the uniqueness of the equivalence classes on $\mathrm{BH}_{p\times p}(p)$ is easily shown for $p = 2, 3, 5, 7$ without any use of computer. For $p = 11, 13$, we can also establish the uniqueness equivalence classes on $\mathrm{BH}_{p\times p}(p)$ with a light aid of computer. (The run time over a single 3.0 GHz CPU is less than 10 seconds.) However, for larger prime numbers p, one may notice that a heavy amount of run time is needed for classifying the matrices in $\mathrm{BH}_{p\times p}(p)$. In fact, it was estimated to take about 5000 hours for $\mathrm{BH}_{17\times 17}(17)$ over a single 3.0 GHz CPU. We introduced a parallel algorithm for proving the following result: (The computation was executed on the high performance multi-node server system Fujitsu Primergy CX400 in Kyushu University, Japan [6].)

Theorem 1.2. *Every matrix in* $\mathrm{BH}_{17\times 17}(17)$ *is equivalent to the Fourier matrix of degree* 17.

In Section 2 we explain our algorithm for classifying the matrices in $\mathrm{BH}_{p\times p}(p)$ up to equivalence. In Section 3 we show that if there is a Butson Hadamard matrix in $\mathrm{BH}_{p\times p}(p)$ which is not equivalent to the Fourier matrix F_p, then there exists a non-Desarguesian projective plane of order p.

2. Algorithm for classifying the matrices in $\mathrm{BH}_{p\times p}(p)$

Throughout this paper it is assumed that the entries of an $n \times n$ matrix are indexed by integers from 0 to $n-1$. For instance, the upper leftmost entry of an $n \times n$ matrix is considered to be in $(0,0)$-position rather than in $(1,1)$-position, and the lower rightmost entry is in $(n-1, n-1)$-position rather than in (n,n)-position.

In what follows we assume that p is a prime number and

$$\xi_p = \cos(2\pi/p) + \sqrt{-1}\sin(2\pi/p).$$

We denote by $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ a finite field with p elements, and adopt the natural ordering of $\mathbb{F}_p$, i.e., $0 < 1 < \cdots < p-1$.

Definition 2.1. We say that $D = (D_{i,j}) \in \mathrm{Mat}_{p\times p}(\mathbb{F}_p)$ is a *difference matrix* if $\{D_{i,k} - D_{j,k} \mid k = 0, 1, \dots, p-1\} = \mathbb{F}_p$ for any i and j with $i \ne j$. The set of all difference matrices of degree p is denoted by $\mathcal{D}_{p\times p}$.

Suppose $H = (\xi_p^{E_{i,j}})$ is a matrix in $\mathrm{BH}_{p\times p}(p)$. We always regard an exponent $E_{i,j}$ for $\xi_p^{E_{i,j}}$ as an element of $\mathbb{F}_p$ so that we can define a map

$$\lambda : \mathrm{BH}_{p\times p}(p) \to \mathrm{Mat}_{p\times p}(\mathbb{F}_p) \quad \text{by} \quad \lambda(H) = (E_{i,j}).$$

Lemma 2.2. *The map λ is one to one and $\mathrm{Im}\,\lambda = \mathcal{D}_{p\times p}$. Thus there is a one to one correspondence between $\mathrm{BH}_{p\times p}(p)$ and $\mathcal{D}_{p\times p}$.*

Proof. The injectivity follows from the definition of λ. If $H = (\xi_p^{E_{i,j}})$ is in $\mathrm{BH}_{p\times p}(p)$ then, for all distinct $i, j \in \{0, \dots, p-1\}$,

$$(HH^*)_{i,j} = \sum_{k=0}^{p-1} H_{i,k}\bar{H}_{j,k} = \sum_{k=0}^{p-1} \xi_p^{E_{i,k}-E_{j,k}}.$$

Since $X^{p-1} + \cdots + X + 1 \in \mathbb{C}[X]$ is the minimal polynomial of ξ_p, $(HH^*)_{i,j} = 0$ if and only if $\{E_{i,k} - E_{j,k} \mid k = 0, 1, \dots, p-1\} = \mathbb{F}_p$. Hence $\lambda(H) \in \mathcal{D}_{p\times p}$ and λ is onto $\mathcal{D}_{p\times p}$. $\square$

Remark 2.3. The exponent matrix for the Fourier matrix F_p of degree p is (ij) which is clearly in $\mathcal{D}_{p\times p}$. Thus $F_p \in \mathrm{BH}_{p\times p}(p)$ by Lemma 2.2.

For $D = (D_{i,j}) \in \mathcal{D}_{p\times p}$, we say that D is *fully normalized* if $D_{0,i} = D_{i,0} = 0$ and $D_{1,i} = D_{i,1} = i$ for all $i \in \{0, 1, \dots, p-1\}$. For $H \in \mathrm{BH}_{p\times p}(p)$, we say that H is *fully normalized* if $\lambda(H)$ is. If a matrix $N = (N_{i,j})$ in $\mathcal{D}_{p\times p}$ or $\mathrm{BH}_{p\times p}(p)$ is fully normalized then the $(p-2)\times(p-2)$ submatrix $(N_{i,j})_{i,j=2}^{p-1}$ is referred to as the *core* of N.