# UNIQUENESS OF BUTSON HADAMARD MATRICES OF SMALL DEGREES 

MITSUGU HIRASAKA ${ }^{1}$, KYOUNG-TARK KIM ${ }^{2}$, AND YOSHIHIRO MIZOGUCHI


#### Abstract

For positive integers $m$ and $n$, we denote by $\mathrm{BH}(m, n)$ the set of all $H \in M_{n \times n}(\mathbb{C})$ such that $H H^{*}=n I_{n}$ and each entry of $H$ is an $m$-th root of unity where $H^{*}$ is the adjoint matrix of $H$ and $I_{n}$ is the identity matrix. For $H_{1}, H_{2} \in \mathrm{BH}(m, n)$ we say that $H_{1}$ is equivalent to $H_{2}$ if $H_{1}=\mathrm{PH}_{2} Q$ for some monomial matrices $P, Q$ whose nonzero entries are $m$-th roots of unity. In this paper we classify $\mathrm{BH}(17,17)$ up to equivalence by computer search.


## 1. Introduction

Following [1], we call an $n \times n$ complex matrix $H$ a Butson-Hadamard matrix of type $(m, n)$ if each entry of $H$ is an $m$-th root of unity and $H H^{*}=n I_{n}$ where $H^{*}$ is the conjugate transpose of $H$ and $I_{n}$ is the $n \times n$ identity matrix. We denote by $\mathrm{BH}(m, n)$ the set of all ButsonHadamard matrices of type $(m, n)$. We give an equivalence relation on $\mathrm{BH}(m, n): H_{1}, H_{2} \in \mathrm{BH}(m, n)$ are equivalent if $H_{2}$ can be obtained from $H_{1}$ via a finite sequence of the following operations:
(O1) a permutation of the rows (columns);
(O2) a multiplication of a row (column) by an $m$-th root of unity.
In this paper we focus on $\operatorname{BH}(p, p)$ where $p$ is a prime. It is wellknown that the Fourier matrix $F_{p}=\left(\exp \frac{2 \pi \sqrt{-1} i j}{p}\right)_{0 \leq i, j \leq p-1}$ of degree $p$ is in $\mathrm{BH}(p, p)$ for each prime $p$, but it is still open whether or not every matrix in $\mathrm{BH}(p, p)$ is equivalent to $F_{p}$. On the other hand it would be a quite exciting result if we could find a matrix in $\mathrm{BH}(p, p)$ which is not equivalent to $F_{p}$. Because, such a matrix gives rise to a non-Desarguesian projective plane of order $p$ (see Proposition 3.4).

One may get a positive answer for the uniqueness of the equivalence classes on $\operatorname{BH}(p, p)$ for $p=2,3,5,7$ without any use of computer, and also for $p=11,13$ with a light support of computer. (The complexity over 3.0 GHz CPU is about less than 10 seconds.) But, for larger prime numbers $p$, one may notice that a heavy amount of complexity is needed in order to classify matrices in $\mathrm{BH}(p, p)$. In fact it was estimated to take about 5000 hours in order to do it for $\mathrm{BH}(17,17)$ over a single 3.0

[^0]GHz CPU. We introduced a parallel algorithm to solve the following result. The computation is executed on the high performance multinode server system Fujitsu Primergy CX400 in Kyushu University.

Theorem 1.1. For a prime $p \leq 17$, every matrix in $\operatorname{BH}(p, p)$ is equivalent to the Fourier matrix of degree $p$.
In section 2 we explain our algorithm to find up to equivalence all the matrices in $\mathrm{BH}(p, p)$. In section 3 we will prove that if there is a matrix in $\mathrm{BH}(p, p)$ which is not equivalent to the Fourier matrix $F_{p}$ then there exists a non-Desarguesian projective plane of order $p$.

## 2. Algorithm to classify $\operatorname{BH}(p, p)$

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

In the sequel we assume that $p$ is prime and

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

We denote by $\mathbb{F}_{p}=\{0,1, \ldots, p-1\}$ 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 $D=\left(D_{i, j}\right) \in M_{p \times p}\left(\mathbb{F}_{p}\right)$ is a difference matrix if $\mathbb{F}_{p}=\left\{D_{i, k}-D_{j, k} \mid k=0,1, \ldots, p-1\right\}$ for any $i$ and $j$ with $i \neq j$. The set of all difference matrices of degree $p$ is denoted by $\mathcal{D}(p)$.

We define a map $\lambda: \mathrm{BH}(p, p) \rightarrow M_{p \times p}\left(\mathbb{F}_{p}\right)$ by $\lambda(H)=\left(E_{i, j}\right)$ for $H=\left(\xi_{p}^{E_{i, j}}\right) \in \mathrm{BH}(p, p)$. (Since $\left(\xi_{p}\right)^{p}=1$ we can regard an exponent $E_{i, j}$ as an element of $\mathbb{F}_{p}$.)

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

Proof. The injectivity follows from the definition of $\lambda$. Let $H=\left(\xi_{p}^{E_{i, j}}\right) \in$ $\mathrm{BH}(p, p)$. Then, for all distinct $i, j$ with $0 \leq i, j \leq p-1$,

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

Since $x^{p-1}+\cdots+x+1$ is the minimal polynomial of $\xi_{p},\left(H H^{*}\right)_{i, j}=0$ if and only if $\left\{E_{i, k}-E_{j, k} \mid k=0,1, \ldots, p-1\right\}=\mathbb{F}_{p}$. Hence $\lambda(H) \in \mathcal{D}(p)$ and $\lambda$ is onto $\mathcal{D}(p)$.

For $D=\left(D_{i, j}\right) \in \mathcal{D}(p)$ 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 $i=0,1, \ldots, p-1$. For $H \in \operatorname{BH}(p, p)$, $H$ is called fully normalized if so is $\lambda(H)$. If $N=\left(N_{i, j}\right)$ in $\mathcal{D}(p)$ (in $\mathrm{BH}(p, p)$, respectively) is fully normalized then the $(p-2) \times(p-2)$ submatrix $\left(N_{i, j}\right)_{2 \leq i, j \leq p-1}$ is called the core of $N$.

Classifying $\mathrm{BH}(p, p)$ is equivalent to finding all possible cores of fully normalized matrices in $\mathrm{BH}(p, p)$. For convenience we can move our workspace to $\mathcal{D}(p)$ due to Lemma [2.2, The next proposition shows that there is a systematic way to find a difference matrix:

Proposition 2.3. Let $L=\left(L_{i, j}\right) \in M_{p \times p}\left(\mathbb{F}_{p}\right)$. Then, $L \in \mathcal{D}(p)$ if and only if $L_{i, j} \neq L_{i, b}+L_{a, j}-L_{a, b}$ for all $0 \leq a<i \leq p-1$ and $0 \leq b<j \leq p-1$.

Proof. $(\Rightarrow)$ By the definition of a difference matrix we have $L_{i, j}-L_{a, j} \neq$ $L_{i, b}-L_{a, b} .(\Leftarrow)$ Fix $i$ and $a$. Then $\left\{L_{i, k}-L_{a, k} \mid k=0, \ldots, p-1\right\}=\mathbb{F}_{p}$ by the condition.

Fix $i$ and $j$ with $0<i, j \leq p-1$. Then Proposition 2.3 tells us that if we hope to determine the ( $i, j$ )-entry of a difference matrix then we have to check the condition $L_{i, j} \neq L_{i, b}+L_{a, j}-L_{a, b}$ for all $a$ and $b$ with $0 \leq a<i$ and $0 \leq b<j$. This leads the following algorithm:

Algorithm, $C(i, j)$ :
Input: $i, j \in\{1, \ldots, p-1\}$ and a $p \times p$ matrix $L=\left(L_{i, j}\right)$
Output: $r(i, j)$ (a subset of $\mathbb{F}_{p}$ )

```
\(r(i, j) \leftarrow \mathbb{F}_{p} ; a \leftarrow 0 ; b \leftarrow 0\)
WHILE \(0 \leq a<i\) DO
    WHILE \(0 \leq b<j\) DO
        \(r(i, j) \leftarrow r(i, j) \backslash\left\{L_{i, b}+L_{a, j}-L_{a, b}\right\}\)
        \(b \leftarrow b+1\)
    \(a \leftarrow a+1\)
RETURN \(r(i, j)\)
```

The algorithm $C(i, j)$ returns a set $r(i, j)$ of candidates for the entry $L_{i, j}$ if the upper left entries $L_{a, b}(0 \leq a<i$ and $0 \leq b<j)$ are already determined.
Now suppose that we hope to construct a fully normalized matrix in $\mathcal{D}(p)$. Let $L$ be a matrix in $M_{p \times p}\left(\mathbb{F}_{p} \cup\{\perp\}\right)$ such that

$$
\begin{equation*}
L_{0, i}=L_{i, 0}=0, L_{1, i}=L_{i, 1}=i \text { and } L_{j, k}=\perp \tag{1}
\end{equation*}
$$

for all $i \in\{0, \ldots, p-1\}$ and $2 \leq j, k \leq p-1$ where $\mathbb{F}_{p} \cap\{\perp\}=\emptyset$. (The letter ' $\perp$ ' stands for the 'empty' entry.) In the sequel we should fill the core of $L$ by using the algorithm $C(i, j)$ so that $L \in \mathcal{D}(p)$. First of all we need an appropriate order of computation which is compatible to the algorithm $C(i, j)$ :
Definition 2.4. Let $\mathcal{I}=\{(i, j) \mid 2 \leq i, j \leq p-1\}$ be the set of indices of the core of $L$. A total order $\preceq$ on $\mathcal{I}$ is called admissible if the following conditions hold.
(i) For all $(i, j) \in \mathcal{I}$ we have $(2,2) \preceq(i, j)$;


Figure 1. The main algorithm, $M(a, b, c, d)$.
(ii) For any $(i, j) \in \mathcal{I}$, if $2 \leq k \leq i, 2 \leq l \leq j$ then $(k, l) \preceq(i, j)$.

Example 2.4.1. The following are admissible total orders on $\mathcal{I}$.
(i) Diagonal order $1, \preceq_{D}:(2,2) \prec(2,3) \prec(3,2) \prec(3,3) \prec$ $(2,4) \prec(3,4) \prec(4,2) \prec(4,3) \prec(4,4) \prec \cdots$.
(ii) Diagonal order $2, \preceq_{D^{\prime}}:(2,2) \prec(2,3) \prec(3,2) \prec(2,4) \prec$ $(3,3) \prec(4,2) \prec(2,5) \prec(3,4) \prec(4,3) \prec(5,2) \prec \cdots$.
(iii) Horizontal order, $\preceq_{H}:(2,2) \prec(2,3) \prec \cdots \prec(2, p-1) \prec$ $(3,2) \prec \cdots \prec(3, p-1) \prec(4,2) \prec \cdots$.

With an admissible total order $\preceq$ on $\mathcal{I}$ we now introduce the main algorithm $M(a, b, c, d)$. See Figure 1. Notice that the parameter $(a, b)$ (respectively, $(c, d)$ ) indicates the starting (resp. finishing) index of the algorithm. For example, by calling $M(2,2, p-1, p-1)$, we can obtain all possible cores of fully normalized matrices in $\mathcal{D}(p)$.

There is a redundancy in our algorithm. Notice that if there exists a matrix $A$ in $\mathcal{D}(p)$ then the transpose $A^{\mathrm{T}}$ is also in $\mathcal{D}(p)$, because the initial part (cf. the equation (1)) of the construction for $L$ is symmetric. Although $A$ and $A^{\mathrm{T}}$ may not be equivalent it is sufficient to find only one of $A$ and $A^{\mathrm{T}}$ in the searching algorithm, and we just add each transpose to the result in the final step. Therefore we may assume

$$
\begin{equation*}
L_{2,3} \leq L_{3,2} \tag{2}
\end{equation*}
$$

For primes $p \leq 13$ the main algorithm $M(2,2, p-1, p-1)$ works well. Over 3.0 GHz CPU within less than 10 seconds, we obtain the following result: For a prime $p \leq 13$, there is a unique fully normalized matrix in $\mathrm{BH}(p, p)$, namely, the Fourier matrix of degree $p$.


Figure 2. The case $p=7$.


Figure 3. The case $p=11$.

The next case $p=17$ needs a heavy computer calculation. So we use a parallel algorithm to use a supercomputer. Our strategy is given as follows: Let $(r, s)$ be a fixed index among a total order $\preceq$. The master thread carries out $M(2,2, r, s)$. If there is a partial solution from $(2,2)$ to $(r, s)$ then the master process passes this partial information of the matrix $L$ to one of many slave threads. For given data from the master thread, a slave thread decides whether or not there are fully normalized matrices in $\mathcal{D}(p)$ by calling $M(m, n, p-1, p-1)$ where $(m, n)$ is the successor of $(r, s)$. Of course, in our parallel program, the master thread also has the role of jobs scheduler, i.e., the management of slave threads.
A choice of the dividing index $(r, s)$ (i.e., the finishing index of the master thread) depends on the specific total order $\preceq$. We checked the three types of total orders, that is, $\preceq_{D}, \preceq_{D^{\prime}}$ and $\preceq_{H}$. (See Example [2.4.1.) The figure 2 and 3 show respectively the cases of $p=7$ and $p=11$. The X -axis of the figures stands for choices of the dividing

| $(r, s)$ | $M(2,2, r, s)$ | \#Partial results |
| :---: | ---: | ---: |
| $(2,2)$ | $\varepsilon$ seconds | 14 |
| $(2,3)$ | $\varepsilon$ seconds | 157 |
| $(2,4)$ | $\varepsilon$ seconds | 1507 |
| $(2,5)$ | $\varepsilon$ seconds | 12327 |
| $(2,6)$ | $\varepsilon$ seconds | 84573 |
| $(2,7)$ | $\varepsilon$ seconds | 478501 |
| $(2,8)$ | 1 seconds | 2186161 |
| $(2,9)$ | 1 seconds | 7865605 |
| $(2,10)$ | 5 seconds | 21644469 |
| $(2,11)$ | 12 seconds | 43828409 |
| $(2,12)$ | 29 seconds | 61675825 |


| $(r, s)$ | $M(2,2, r, s)$ | \#Partial results |
| :---: | ---: | ---: |
| $(2,13)$ | 50 seconds | 55494757 |
| $(2,14)$ | 69 seconds | 28008069 |
| $(2,15)$ | 81 seconds | 6275119 |
| $(2,16)$ | 81 seconds | 6275119 |
| $(3,2)$ | 85 seconds | 37464544 |
| $(3,3)$ | 112 seconds | 376242051 |
| $(3,4)$ | 335 seconds | 2737088388 |
| $(3,5)$ | 1852 seconds | 15753030361 |
| $(3,6)$ | 9878 seconds | 71394611311 |
| $\vdots$ | $\vdots$ | $\vdots$ |

Figure 4. The computation data in the case $p=17$.
indices $(r, s)$ among total orders, and the Y -axis means the corresponding counts of possibility for the partial results which is carried out by $M(2,2, r, s)$. We see that the horizontal order is most efficient in the three types. Therefore we adopt the horizontal order in the case of $p=17$ too, and in this case we choose the dividing index as $(2,16)$ as Figure 4 suggested.

The specification of parallel computation for $p=17$ is the following:
Fujitsu PRIMERGY CX400 2;
CPU: Intel Xeon E5-2680 ( $2.7 \mathrm{GHz}, 8$ core $) \times 2 /$ node;
Memory: 128GB / node
Interconnection network: InfiniBand FDR1 6.78GB/sec
Server system total peak performance: 811.86TFLOPS (1476 nodes) OS: Red Hat Enterprise Linux;
Programming language: C with MPI (message passing interface);
Total number of processes: 1 (master) +63 (slaves) $=64$;
Total required time: 246093 seconds ( $\doteqdot 68$ hours);
As mentioned in introduction, we obtain Theorem 1.1 as a result.

## 3. Desarguesian projective plane yields the Fourier matrix.

Let $\mathcal{A}$ be a nonempty finite set and $\mathcal{B}$ a family of subsets of $\mathcal{A}$. We say that $\rho \in \operatorname{Sym}(\mathcal{A} \cup \mathcal{B})$ is an automorphism of $(\mathcal{A}, \mathcal{B})$ if, for all $(a, B) \in \mathcal{A} \times \mathcal{B}, a \in B$ if and only if $\rho(a) \in \rho(B)$. We denote by Aut $(\mathcal{A}, \mathcal{B})$ the group of automorphisms of $(\mathcal{A}, \mathcal{B})$.

For a positive integer $k \geq 2$ a pair $\mathcal{D}=(\mathcal{P}, \mathcal{L})$ is called a projective plane of order $k$ if $|\mathcal{P}|=|\mathcal{L}|=k^{2}+k+1,|\{x \in \mathcal{P} \mid x \in L\}|=k+1$ for each $L \in \mathcal{L}$ and $\left|\left\{x \in \mathcal{P} \mid x \in L \cap L^{\prime}\right\}\right|=1$ for all distinct $L, L^{\prime} \in \mathcal{L}$. A pair $(x, L) \in \mathcal{P} \times \mathcal{L}$ is called a flag of $\mathcal{D}$ if $x \in L$. For a flag $(x, L)$ of $\mathcal{D}$ we say that $\sigma \in \operatorname{Aut}(\mathcal{P}, \mathcal{L})$ is an elation with respect to $(x, L)$ if $\sigma$ fixes each point in $L$ and each line through $x$.

Let $\mathcal{D}=(\mathcal{P}, \mathcal{L})$ be a projective plane of order $p$ containing an elation $\sigma$ of order $p$ with respect to a flag $(x, L)$. Let $y, z \in \mathcal{P} \backslash L$ be such that
$x, y$ and $z$ are not on a common line. For $i \in\{0,1, \ldots, p-1\}$ we define $N_{i} \in \mathcal{L}$ to be the line through $y$ and $\sigma^{i}(z)$, and $y_{i} \in \mathcal{P}$ to be the point incident to $N_{0}$ and $\sigma^{-i}\left(N_{1}\right)$.
Lemma 3.1. For all $i, j \in\{0, \ldots, p-1\}$ there is a unique $E_{i, j} \in \mathbb{F}_{p}$ such that $\sigma^{E_{i, j}}\left(y_{i}\right) \in N_{j}$. Moreover $\left(E_{i, j}\right)$ is fully normalized in $\mathcal{D}(p)$.
Proof. Since $y_{i} \in \mathcal{P} \backslash L$ and $x \notin N_{j}$, the line $M$ through $x$ and $y_{i}$ intersects $N_{j}$ at exactly one point. Since $\sigma$ acts regularly on $M \backslash\{x\}$, the first assertion follows. Since $y_{i} \in N_{0}$ and $y=y_{0} \in N_{i}$ we have $E_{i, 0}=E_{0, i}=0$ for each $i \in\{0,1, \ldots, p-1\}$. Since $y_{i} \in \sigma^{-i}\left(N_{1}\right)$ and $\sigma^{i}\left(y_{1}\right)=\sigma^{i}(z) \in N_{i}$ we have $\sigma^{i}\left(y_{i}\right) \in N_{1}$ and $\sigma^{i}\left(y_{1}\right) \in N_{i}$ whence $E_{i, 1}=$ $E_{1, i}=i$ for each $i \in\{0,1, \ldots, p-1\}$. Suppose that $E_{i, k}-E_{j, k}(k=$ $0,1, \ldots, p-1)$ are not distinct for some $i \neq j$, i.e., $E_{i, k}-E_{j, k}=E_{i, l}-E_{j, l}$ for some $k \neq l$. Since $\sigma^{E_{i, k}}\left(y_{i}\right), \sigma^{E_{j, k}}\left(y_{j}\right) \in N_{k}$ and $\sigma^{E_{i, l}}\left(y_{i}\right), \sigma^{E_{j, l}}\left(y_{j}\right) \in$ $N_{l}$ it follows that

$$
\sigma^{E_{i, k}-E_{j, k}}\left(y_{i}\right), y_{j} \in \sigma^{-E_{j, k}}\left(N_{k}\right) \cap \sigma^{-E_{j, l}}\left(N_{l}\right)
$$

Since $y_{j} \notin\langle\sigma\rangle y_{i}$ and $N_{k} \notin\langle\sigma\rangle N_{l}$ we have a contradiction. This completes the proof of the second assertion.

We fix the point set $\mathcal{P}$ of size $p^{2}+p+1$. Let $\Delta$ be the set of all quadruples ( $\mathcal{D}, \sigma, y, z$ ) satisfying the following conditions:
(i) $\mathcal{D}=(\mathcal{P}, \mathcal{L})$ is a projective plane of order $p$;
(ii) $\sigma$ is an elation of $\mathcal{D}$ with respect to a flag $(x, L)$;
(iii) $y, z \in \mathcal{P} \backslash L$ such that $x, y, z$ are not on a common line.

By Lemma 3.1 we define a function $\Psi$ from $\Delta$ to the set of all fully normalized Butson-Hadmard matrices of type $(p, p)$ by $\Psi(\mathcal{D}, \sigma, x, y)=$ $\left(\xi_{p}^{E_{i, j}}\right)$ where $\sigma^{E_{i, j}}\left(y_{i}\right) \in N_{j}$.
Lemma 3.2. The function $\Psi$ is surjective.
Proof. Let $H \in \mathrm{BH}(p, p)$ be fully normalized. Then $H=\left(\xi_{p}^{E_{i, j}}\right)$ where $\left(E_{i, j}\right) \in \mathcal{D}(p)$ is also fully normalized. Let $C$ denote the $p \times p$ permutation matrix corresponding to the map from $\mathbb{F}_{p}$ to itself defined by $\alpha \mapsto \alpha+1$. We denote the $p^{2} \times p^{2}$ matrix $\left(C^{E_{i, j}}\right)$ by $P(H)$. We denote the $m \times n$ all one and zero matrix by $J_{m, n}$ and $O_{m, n}$ respectively, and we define $Q(H)$ to be a $\left(p^{2}+p+1\right) \times\left(p^{2}+p+1\right)$ matrix such that

$$
Q(H)=\left(\begin{array}{c|c|c}
1 & J_{1, p} & O_{1, p^{2}} \\
\hline J_{p, 1} & O_{p, p} & D \\
\hline O_{p^{2}, 1} & D^{T} & P(H)
\end{array}\right)
$$

where $D$ is a $p \times p^{2}$ matrix and

$$
D=\left(\begin{array}{c|c|c|c}
J_{1, p} & O_{1, p} & \cdots & O_{1, p} \\
\hline O_{1, p} & J_{1, p} & \ddots & \vdots \\
\hline \vdots & \ddots & \ddots & O_{1, p} \\
\hline O_{1, p} & \cdots & O_{1, p} & J_{1, p}
\end{array}\right) .
$$

Note that $Q(H)$ forms an incidence matrix of a projective plane of order $p$ and

$$
R Q(H) R^{t}=Q(H) \quad \text { where } \quad R=\left(\begin{array}{c|c}
I_{p+1} & O_{p+1, p^{2}} \\
\hline O_{p^{2}, p+1} & I_{p} \otimes C
\end{array}\right)
$$

This implies that the projective plane $\mathcal{D}$ having its incidence matrix $Q(H)$ has an elation $\sigma$ with respect to the flag corresponding to the $(0,0)$-entry of $Q(H)$. Let $y, z$ be the points corresponding to the $(p+1)$ th row and $(2 p+1)$-th row of $Q(H)$, respectively. Then the quadruple $(\mathcal{D}, \sigma, y, z)$ is mapped to $H$ by $\Psi$. Therefore $\Psi$ is surjective.

Lemma 3.3. If $\mathcal{D}$ is a Desarguesian projective plane of order $p$ then $\Psi(\mathcal{D}, \sigma, y, z)$ is $\left(\xi_{p}^{i j}\right)$, namely, the Fourier matrix of degree $p$.

Proof. Suppose $\mathcal{D}=(\mathcal{P}, \mathcal{L})$ is Desarguesian. Then the automorphism group of $\mathcal{D}$ is isomorphic to $\operatorname{PGL}(3, p)$. Let $\sigma$ be an elation of order $p$ with respect to a flag $(x, L)$ and let $y, z \in \mathcal{L}$ be such that $x, y, z$ are not in a common line. We denote by $G$ the normalizer of $\langle\sigma\rangle$ in $\operatorname{Aut}(\mathcal{P}, \mathcal{L})$. It is known that $G$ acts doubly transitively on $\mathcal{P} \backslash L$ and $G \simeq \operatorname{AGL}(2, p)$, and hence $G_{y, z} \simeq \operatorname{AGL}(1, p)$ where we denote by $G_{y, z}$ the stabilizer subgroup fixing $y$ and $z$. Note that $G_{y, z}$ contains $\tau$ which acts regularly on $\left\{y_{i} \mid i=1,2, \ldots, p-1\right\}$ and regularly on $\left\{N_{i} \mid i=1,2, \ldots, p-1\right\}$.

Suppose $\tau\left(N_{1}\right)=N_{j}$ for some $j$. Since $\sigma\left(y_{1}\right) \in N_{1}$ by the assumption and $y_{1}=z$,

$$
\left(\tau \sigma \tau^{-1}\right)\left(y_{1}\right) \in \tau\left(N_{1}\right)=N_{j}
$$

Since $\sigma^{j}\left(y_{1}\right) \in N_{j}$ by the assumption and $\tau \sigma \tau^{-1}\left(y_{1}\right) \in N_{j}$ it follows that $\tau \sigma \tau^{-1}=\sigma^{j}$. Since $\tau\left(y_{i}\right)=y_{i}$ and $\sigma^{i}\left(y_{i}\right) \in N_{1}$ we have

$$
\tau \sigma^{i} \tau^{-1}\left(y_{i}\right) \in \tau\left(N_{1}\right)=N_{j}
$$

On the other hand, since $\tau \sigma \tau^{-1}=\sigma^{j}$ we have $\tau \sigma^{i} \tau^{-1}=\sigma^{i j}$. Thus we have

$$
\sigma^{i j}\left(y_{i}\right)=\tau \sigma^{i} \tau^{-1}\left(y_{i}\right) \in N_{j}
$$

This implies that we have $E_{i, j}=i j$ for all $i$ and $j$. This completes the proof.
Proposition 3.4. If there is a fully normalized matrix in $\mathrm{BH}(p, p)$ which is not the Fourier matrix then it induces a non-Desarguesian projective plane of order $p$.

Proof. This is due to the contrapositive of Lemma 3.3.
From Theorem [1.1] we have the following result:
Corollary 3.5. For a prime $p \leq 17$, there is no non-Desarguesian projective plane of order $p$.

## Acknowledgements

1. The computation was mainly carried out using the computer facilities at Research Institute for Information Technology, Kyushu University [2].
2. We would like to thank Dong-been Kim, a student of the R\&E (research and education) lecture given by the first author for his basic algorithm to search Butson Hadamard matrices.

## References

[1] A.T. Butson, Generalized Hadamard matrices, Proc. Amer. Math. Soc. 131962 894-898.
[2] http://www.cc.kyushu-u.ac.jp/scp/
Department of mathematics, Pusan National University, Jang-Jeon dong, Busan, Republic of Korea

E-mail address: hirasaka@pusan.ac.kr
Department of mathematics, Pusan National University, jang-jeon dong, Busan, Republic of Korea

E-mail address: poisonn00@hanmail.net
Institute of Mathematics for Industry, Kyushu University, 744 Motooka, Nishi-ku Fukuoka 819-0395, Japan

E-mail address: ym@imi.kyushu-u.ac.jp


[^0]:    ${ }^{1}$ 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.

