数理解析研究所講究録
第 1872 巻 2014 年 39-48

MUTUALLY UNBIASED BASES, GAUSS SUMS AND THE ASYMPTOTIC EXISTENCE OF BUTSON HADAMARD MATRICES

FERENC SZÖLLŐSI

Dedicated to the memory of Alton Thomas Butson (1926 – 1997)

ABSTRACT. In this paper we utilize a recent block construction due to McNulty and Weigert [25] and provide a new and more transparent proof of some of the results of Butson [3], Dawson [7] and de Launey and Dawson [8] on Butson-type complex Hadamard matrices.

2000 Mathematics Subject Classification. Primary 05B20, secondary 46L10.
Keywords and phrases. *Complex Hadamard matrix, Butson-type, Mutually unbiased basis*

1. INTRODUCTION

This paper is based on the talk given at a RIMS Symposium on *Research on finite groups and their representations, vertex operator algebras, and algebraic combinatorics*, RIMS, Kyoto, January 7-10, 2013.

Hadamard matrices, real or generalized, have many applications in mathematics and quantum information theory. A real Hadamard matrix H of order n is an $n\times n$ matrix with $(-1,1)$ entries, such that $HH^T=nI$ holds, where I is the identity matrix. Thus the rows and columns of such a matrix are pairwise orthogonal. A real Hadamard matrix is normalized, if the entries in its first row and column are all 1. Deciding the existence of real Hadamard matrices is a long standing open problem in combinatorics. The Hadamard conjecture asserts that for every doubly even n there exist a real Hadamard matrix. The difficulty of this conjecture lead to the study of various generalizations of real Hadamard matrices, including weighing matrices [20], modular Hadamard matrices [22] and complex Hadamard matrices [30]. Studying these more general problems will hopefully shed some light to this famous unresolved conjecture. Investigating the existence and structural properties of complex Hadamard matrices by the physicists community resulted in a number of exciting new developments in this field very recently [24], [25]. In particular, the concept of mutually unbiased basis [13] turned out to be a valuable tool constructing new weighing and Hadamard matrices [15].

In this paper we study a class of complex Hadamard matrices, which were introduced by Butson in 1951 [3]. A Butson-type complex Hadamard matrix H of order n is an $n\times n$ matrix whose all entries are some complex qth root of unity, satisfying $HH^*=nI$ where $*$ denotes the Hermitian transpose. We denote these matrices by $\mathrm{BH}(n,q)$. A complex Hadamard matrix may be thought of as the limiting case $q\to\infty$ of the $\mathrm{BH}(n,q)$ matrices. We say that the entries of such a matrix are unimodular.

Date: May, 2013.
This work was supported by the Hungarian National Research Fund OTKA K-77748 and by the Grants-in-Aid for Scientific Research program of Japan 24·02807.

It is well known that $\mathrm{BH}(n,4)$ matrices lead to the construction of real Hadamard matrices of order $2n$. This result has substantially been improved in a breakthrough paper by Compton, Craigen and de Launey [4] who pointed out that $\mathrm{BH}(n,6)$ matrices without any $(-1,1)$ entries lead to the construction of real Hadamard matrices of order $4n$. Determining the exact relation between $\mathrm{BH}(n,q)$ and real Hadamard matrices seems to be a challenging, yet extremely rewarding assignment.

It is worthwhile noting that Butson-type complex Hadamard matrices also have current applications in frame theory [2], [29] and coding theory [1], [14], among other things [19].

The goal of this paper is to shed new light onto some classical constructions of Butson-type complex Hadamard matrices. We use a new, non-trivial block construction due to McNulty and Weigert [25] and give a short proof to the existence of $\mathrm{BH}(2p,p)$ matrices for all primes p. Then we show how these ideas can be used to settle the existence of $\mathrm{BH}(4p,p)$ matrices. We believe that our approach is more transparent that of Dawson's [7].

It is known that if p is a prime number and a $\mathrm{BH}(n,p)$ matrix exists then $n = tp$ for some positive integer t [2], [33]. However, determining those values t for which there exists a $\mathrm{BH}(tp,p)$ matrix is already unresolved for $p = 2$. The best asymptotic result in the real case is due to Livinskyi [23], whose methods were influenced by work of Craigen [6], de Launey [10] and Seberry [31]. The analogous asymptotic result in the Butson case is due to de Launey and Dawson [8].

The outline of this paper is as follows. In Section 2 we first recall some number theoretic tools essential to our results and then discuss some properties of mutually unbiased bases. In Section 3 we present a construction of $\mathrm{BH}(4p,p)$ matrices which then will subsequently be generalized in Section 4. To improve the readability of the main text, two rather large matrices were moved to the Appendix.

2. Preliminaries

We begin this section with fixing some notation. Throughout this paper p is a prime number, and we denote by $\left(\frac{\cdot}{p}\right)$ the Legendre symbol. We denote by $\mathbf{i} = \sqrt{-1}$ the complex imaginary unit and introduce a scaling factor σ_p, which depends only on the prime number p as follows:

$$\sigma_p := \frac{1}{\sqrt{p}}(-\mathbf{i})^{1/2-\left(\frac{-1}{p}\right)/2} = \begin{cases} 1/\sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ -\mathbf{i}/\sqrt{p} & \text{if } p \equiv 3 \pmod 4 \end{cases}. \tag{1}$$

Henceforth $\overline{z}$ will refer to the complex conjugate of $z \in \mathbb{C}$. Further, we use the following notation: for a prime number p and for any $z \in \mathbb{C}$ we define the exponential function as $e_p(z) := \mathbf{e}^{\frac{2\pi\mathbf{i}}{p}z}$. With this notation the Fourier matrix can be described as $[F_p]_{i,j} = e_p((i-1)(j-1))$, which is a well-known example of $\mathrm{BH}(p,p)$ matrices.

Next we recall some standard facts from number theory which will be needed later. We refer the reader to the monograph [18] for details.

Gauss proved that if $p \geq 3$ is a prime number, then

$$\sum_{k=1}^{p} e_p(k^2) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ \mathbf{i}\sqrt{p} & \text{if } p \equiv 3 \pmod 4 \end{cases}. \tag{2}$$

From this, it is easy to derive the following.

Lemma 2.1 (Quadratic Gauss sum). *Let $p \geq 3$ be a prime number, $(a,b) \in \mathbb{Z}_p^* \times \mathbb{Z}_p$. Then*

$$\sum_{k=1}^{p} e_p\left(ak^2 + bk\right) = p\overline{\sigma_p}\left(\frac{a}{p}\right) e_p\left(-2^{p-3}a^{p-2}b^2\right).$$

Proof. We use (2) and proceed by completing the square as follows:

$$\begin{aligned}\sum_{k=1}^{p} e_p\left(ak^2 + bk\right) &= e_p\left(-2^{p-3}a^{p-2}b^2\right)\sum_{k=1}^{p} e_p\left(a\left(k + 2^{p-2}a^{p-2}b\right)^2\right)\\ &= p\overline{\sigma_p}\left(\frac{a}{p}\right) e_p\left(-2^{p-3}a^{p-2}b^2\right).\end{aligned}$$

□

The following is a deep result due to André Weil.

Theorem 2.2 (Weil, [32]). *Let $p \geq 3$ be a prime number. For any integer m satisfying $1 \leq m \leq p-1$ and for distinct $a_1, a_2, \ldots, a_m \in \mathbb{Z}_p$, we have*

$$\left|\sum_{k=1}^{p}\prod_{i=1}^{m}\left(\frac{k+a_i}{p}\right)\right| \leq (m-1)\sqrt{p}. \tag{3}$$

The next result is interesting in its own, and will be a key ingredient to our construction.

Proposition 2.3 (cf. Hudson [16]). *Let p be a prime number. There exists a quadratic residue $r \in \mathbb{Z}_p$ such that*

$$\left(\frac{r}{p}\right) = -\left(\frac{r+3}{p}\right) = \left(\frac{r+6}{p}\right) = -\left(\frac{r+8}{p}\right) = -\left(\frac{r+11}{p}\right) = \left(\frac{r+16}{p}\right) = 1,$$

if and only if $p \in \{7, 29, 31, 41, 47, 59, 61\}$ or $p \geq 71$.

The argument is somewhat standard. We follow the one presented in [16].

Proof. It is easy to verify the statement for all primes $p < 71$. Therefore we can assume that $p \geq 71$. Let us define the quantity

$$\begin{aligned}S = \sum_{r=1}^{p-17}&\left(\left(\frac{r}{p}\right)+1\right)\left(\left(\frac{r+3}{p}\right)-1\right)\left(\left(\frac{r+6}{p}\right)+1\right)\\ &\times\left(\left(\frac{r+8}{p}\right)-1\right)\left(\left(\frac{r+11}{p}\right)-1\right)\left(\left(\frac{r+16}{p}\right)+1\right).\end{aligned}$$

Note that each term in the sum is either 0 or -64, therefore if $S < 0$ then clearly exists an integer $1 \leq r \leq p-17$ as claimed. After expanding the brackets we can rearrange the terms by collecting together products of Legendre symbols with the same number of factors. We use the notation $\mathcal{S} := \{0, 3, 6, 8, 11, 16\}$ and we denote a nonempty subset $\mathcal{A} \subseteq \mathcal{S}$ by $\mathcal{A} = \{a_1, a_2, \ldots, a_{|\mathcal{A}|}\}$. We have

$$S = \sum_{r=1}^{p-17}(-1) + \sum_{\substack{\mathcal{A}\subseteq\mathcal{S}\\ |\mathcal{A}|\geq 1}}(-1)^{\xi(\mathcal{A})}\sum_{r=1}^{p-17}\prod_{i=1}^{|\mathcal{A}|}\left(\frac{r+a_i}{p}\right),$$

where $\xi(\mathcal{A})$ denotes either 0 or 1. We complete the sums by adding up the missing 17 terms and, after using the triangle inequality, we apply Weil's estimate (3) to conclude that for each nonempty $\mathcal{A} \subseteq \mathcal{S}$

$$\left|(-1)^{\xi(\mathcal{A})}\sum_{r=1}^{p-17}\prod_{i=1}^{|\mathcal{A}|}\left(\frac{r+a_i}{p}\right)\right| \leq (|\mathcal{A}|-1)\sqrt{p}+17$$

holds. Therefore

$$|S+p-17| \leq \sum_{i=1}^{6}\binom{6}{i}\left((i-1)\sqrt{p}+17\right) = 1071+129\sqrt{p}.$$

If $S < 17-p$ then $S<0$ follows. Otherwise, if $S \geq 17-p$ then for $p \geq 18757$ we find that

$$S \leq 1088+129\sqrt{p}-p<0.$$

It remains to be seen that all primes in the range $71 \leq p < 18757$ satisfy the claim. This can be easily verified by computers. □

After these number theoretic preliminaries we now turn to the discussion of mutually unbiased bases. Two orthonormal bases of $\mathbb{C}^d$, $\mathcal{B}_1$ and $\mathcal{B}_2$, are called mutually unbiased, if for every $e \in \mathcal{B}_1$ and $f \in \mathcal{B}_2$ we have $|\langle e, f\rangle| = 1/\sqrt{d}$. A collection of orthonormal bases $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_k$ are called (pairwise) mutually unbiased, if any two of them are unbiased. Mutually unbiased bases form a fundamental concept in quantum tomography [13]. We note that it is a major open problem to decide the maximum number of pairwise mutually unbiased bases of non prime power orders [13], [24].

Throughout this paper we identify these bases with matrices of size d whose column vectors are the respective basis vectors. In this terminology, two unitary matrices K and L of size d are unbiased if and only if $\sqrt{d}K^*L$ is a complex Hadamard matrix.

Next we recall a construction of a complete set of mutually unbiased bases in prime orders. We denote by D the following diagonal matrix once and for all:

$$D := \operatorname{diag}\left[e_p\left(0^2\right), e_p\left(1^2\right), \dots, e_p\left((p-1)^2\right)\right]. \tag{4}$$

Lemma 2.4 (See e. g. [17]). *Let p be a prime number and D as in* (4). *Then the set* $\{I_p, \frac{1}{\sqrt{p}}F_p, \frac{1}{\sqrt{p}}DF_p, \dots, \frac{1}{\sqrt{p}}D^{p-1}F_p\}$ *forms a collection of $p+1$ mutually unbiased bases in* $\mathbb{C}^p$.

Proof. It is clear that each of the matrices are unitary and hence, the identity matrix I_p is unbiased to all further matrices. It remains to be seen that for all $a \in \mathbb{Z}_p^*$ the product $\frac{1}{\sqrt{p}}F_p^*D^aF_p$ describes a complex Hadamard matrix, i. e. its entries are unimodular. We use Lemma 2.1 to compute the (i,j)th entry of the matrix $F_p^*D^aF_p$. In particular, we get

$$\left[F_p^*D^aF_p\right]_{i,j} = \sum_{k=1}^{p} e_p\left(a(k-1)^2+(j-i)(k-1)\right) = p\overline{\sigma_p}\left(\frac{a}{p}\right)e_p\left(-2^{p-3}a^{p-2}(j-i)^2\right). \tag{5}$$

□

Remark 2.5. From (5) it follows that the entries of the matrix $\sigma_pF_p^*D^aF_p$ are either pth roots of unity, or their negative, depending on the number $a \in \mathbb{Z}_p^*$.

The generalized Kronecker product (also called as Diţă's construction [12]) is a fundamental method obtaining parametric families of complex Hadamard matrices of composite orders.

Lemma 2.6. *Let $H = [h_{ij}]_{i,j=1}^n$ be a complex Hadamard matrix of order n and $L_1, L_2, \dots, L_n$ be complex Hadamard matrices of order m. Then the following block matrix*

$$M = H \otimes \begin{bmatrix} L_1 & L_2 & \dots & L_n \end{bmatrix} := \begin{bmatrix} h_{11}L_1 & h_{12}L_2 & \dots & h_{1n}L_n \\ h_{21}L_1 & h_{22}L_2 & & h_{2n}L_n \\ \vdots & & \ddots & \vdots \\ h_{n1}L_1 & h_{n2}L_2 & \dots & h_{nn}L_n \end{bmatrix}$$

is a complex Hadamard matrix of order mn.

Proof. It is clear that all entries of M are unimodular. The identity $MM^* = mnI_{mn}$ follows immediately upon block-multiplication. □

We conclude this section with our final ingredient, which is a remarkable generalization of Lemma 2.6.

Proposition 2.7 (McNulty–Weigert, [25]). *Let $H = [h_{ij}]_{i,j=1}^n$ be a complex Hadamard matrix of order n, $K_1, K_2, \dots, K_n$ and $L_1, L_2, \dots, L_n$ be unitary matrices of order m, such that K_i is unbiased to L_j for all $i, j = 1, 2, \dots, n$. Then the matrix*

$$M = \sqrt{m} \begin{bmatrix} h_{11}K_1^*L_1 & h_{12}K_1^*L_2 & \dots & h_{1n}K_1^*L_n \\ h_{21}K_2^*L_1 & h_{22}K_2^*L_2 & & h_{2n}K_2^*L_n \\ \vdots & & \ddots & \vdots \\ h_{n1}K_n^*L_1 & h_{n2}K_n^*L_2 & \dots & h_{nn}K_n^*L_n \end{bmatrix}$$

is a complex Hadamard matrix of order mn.

Proof. On the one hand the unbiasedness condition ensures that all entries are unimodular. On the other hand the identity $MM^* = mnI_{mn}$ follows immediately upon block-multiplication. Thus the array describes a complex Hadamard matrix. □

3. The existence of $\mathrm{BH}(4p, p)$ matrices

McNulty and Weigert have successfully constructed various new and interesting examples of $\mathrm{BH}(n, q)$ matrices of small orders [25]. Among other things they have essentially rediscovered the following classical theorem of Butson. We include this here as a trivial warm-up result.

Theorem 3.1 (Butson, [2]). *Let $p \geq 3$ be a prime number, and let $1 < s < p$ be a quadratic nonresidue modulo p. Then the matrix*

$$M = \begin{bmatrix} I_p & 0 \\ 0 & \sigma_p F_p^* D \end{bmatrix} \begin{bmatrix} F_p & D^{s-1}F_p \\ F_p & -D^{s-1}F_p \end{bmatrix} = \begin{bmatrix} F_p & D^{s-1}F_p \\ \sigma_p F_p^* D F_p & -\sigma_p F_p^* D^s F_p \end{bmatrix},$$

is a $\mathrm{BH}(2p, p)$ matrix, where σ_p and D are described by (1) and (4), respectively.

Proof. Follows immediately from Lemma 2.4, Remark 2.5 and Proposition 2.7. □

Now we proceed further, and consider a 4×4 real Hadamard matrix H, and apply the McNulty–Weigert construction to obtain the following result.

Proposition 3.2. *Let $p \geq 3$ be a prime number, and assume that there exists $(\alpha, \beta, \gamma) \in \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ such that*

$$\left(\frac{\alpha+1}{p}\right) = \left(\frac{\beta+4}{p}\right) = \left(\frac{\gamma+9}{p}\right) = 1, \qquad \text{and}$$

$$\left(\frac{\alpha+4}{p}\right) = \left(\frac{\alpha+9}{p}\right) = \left(\frac{\beta+1}{p}\right) = \left(\frac{\beta+9}{p}\right) = \left(\frac{\gamma+1}{p}\right) = \left(\frac{\gamma+4}{p}\right) = -1$$

holds. Then

$$M_p(\alpha,\beta,\gamma) = \begin{bmatrix} F_p & D^{\alpha}F_p & D^{\beta}F_p & D^{\gamma}F_p \\ \sigma_pF_p^*DF_p & \sigma_pF_p^*D^{\alpha+1}F_p & -\sigma_pF_p^*D^{\beta+1}F_p & -\sigma_pF_p^*D^{\gamma+1}F_p \\ \sigma_pF_p^*D^4F_p & -\sigma_pF_p^*D^{\alpha+4}F_p & \sigma_pF_p^*D^{\beta+4}F_p & -\sigma_pF_p^*D^{\gamma+4}F_p \\ \sigma_pF_p^*D^9F_p & -\sigma_pF_p^*D^{\alpha+9}F_p & -\sigma_pF_p^*D^{\beta+9}F_p & \sigma_pF_p^*D^{\gamma+9}F_p \end{bmatrix} \tag{6}$$

is a $\mathrm{BH}(4p,p)$ *matrix, where σ_p and D are described by* (1) *and* (4), *respectively.*

Proof. Follows immediately from Lemma 2.4, Remark 2.5 and Proposition 2.7. □

In Table 1 we have exhibited several triplets (α, β, γ) satisfying the conditions of Proposition 3.2 thus yielding examples of $\mathrm{BH}(4p,p)$ matrices.

TABLE 1. Triplets, yielding $\mathrm{BH}(4p,p)$ matrices via (6) for several values of p.

p	(α,β,γ)	p	(α,β,γ)	p	(α,β,γ)
11	(4,1,6)	19	(4,1,11)	43	(3,11,1)
13	(2,6,1)	23	(1,21,16)	53	(10,11,1)
17	(1,5,6)	37	(9,5,1)	67	(3,2,1)

The following is a special case of a result of Dawson.

Theorem 3.3 (Dawson, [7]). *There exists a* $\mathrm{BH}(4p,p)$ *matrix for every prime number* p.

Proof. The case $p = 2$ is trivial, while the sporadic cases, corresponding to $p = 3$ and $p = 5$ are contained in the Appendix. Table 1 displays further 9 values of p for which the existence of $\mathrm{BH}(4p,p)$ matrices follow via the array described in (6).

Hence we can assume that p is a prime number for which Proposition 2.3 applies, and therefore there exist a quadratic residue $r \in \mathbb{Z}_p$ such that the matrix $M_p(r-1, r+2, r+7)$, described by formula (6) in Proposition 3.2 is a $\mathrm{BH}(4p,p)$ matrix, as required. □

4. The doubly even case

The aim of this section is to generalize the methods presented in Section 3 and provide an asymptotic result for the existence of $\mathrm{BH}(np,p)$ matrices for doubly even n (see Theorem 4.1). The idea is to blow up a real Hadamard matrix H via the McNulty–Weigert construction with similar ingredients what we used in the construction of (6). Let H be a normalized real Hadamard matrix of order $n \geq 4$, and let us consider the following matrix:

$$\begin{aligned} M(r) :=& \mathrm{diag}\left[I_p, \sigma_pF_p^*D, \sigma_pF_p^*D^4, \dots, \sigma_pF_p^*D^{(n-1)^2}\right] \\ &\times \left(H \otimes \left[F_p, D^rF_p, D^{r+(n-1)^2}F_p, \dots, D^{r+(n-2)(n-1)^2}F_p\right]\right). \end{aligned} \tag{7}$$

This new array $M(r)$ has the property that (upon multiplying together its defining factors) the exponents of D are different, so that we can prescribe them to be either quadratic residues or nonresidues depending on the underlying plus or minus sign inherited from H. To conclude that such a prescribed choice of exponents indeed exist for large p we use Hudson's idea combined with Weil's estimate in exactly the same way as in the $\mathrm{BH}(4p,p)$ case.

Theorem 4.1 (cf. [8]). *Let n be the order of a real Hadamard matrix, and $p > 2^{2n^2+1}$ be a prime number. Then there exist a $\mathrm{BH}(np,p)$ matrix.*

We remark here that the obtained bound on p is considerably larger than the one given in [8]. The presented proof here serves illustrative purposes only.

Proof. We assume that $n \geq 4$, $p > 2^{2n^2+1}$ and take any normalized real Hadamard matrix H. Our aim is to prove that there exist an $r \in \mathbb{Z}_p$ such that the array $M(r)$, described by (7), is composed of pth roots of unity. We introduce the following sets $\mathcal{B} := \{1, 4, 9, \dots, (n-1)^2\}$, $\mathcal{C} := \{0, (n-1)^2, 2(n-1)^2, \dots, (n-2)(n-1)^2\}$, and further $\mathcal{S} := \{b + c \colon b \in \mathcal{B}, c \in \mathcal{C}\}$ with distinct entries $s_1, s_2, \dots, s_{(n-1)^2}$. Next we define, similarly as before, the quantity

$$S = \sum_{r=1}^{p-(n-1)^3-1} \prod_{s_i \in \mathcal{S}} \left(\left(\frac{r+s_i}{p} \right) \pm 1 \right), \tag{8}$$

where the plus or minus sign in a factor $\left(\frac{r+s_i}{p}\right) \pm 1$ is uniquely determined by the sign pattern of the underlying real Hadamard matrix H as follows: there are unique indices $j, k \in \{1, 2, \dots, n-1\}$ such that $s_i = b_j + c_k$, $b_j \in \mathcal{B}$ and $c_k \in \mathcal{C}$. We choose the plus sign in this factor if and only if the $\left(1 + \sqrt{b_j}, 2 + c_k/(n-1)^2\right)$th entry of H is 1. Otherwise we choose the minus sign. Therefore, as H is a normalized, $n \geq 4$ doubly even, each term within S is either 0 or $2^{(n-1)^2}$. Hence, if we could argue that $S > 0$ then clearly exists a suitable integer r for which $M(r)$ is a $\mathrm{BH}(np,p)$ matrix.

We expand and then rearrange (8) by collecting together products of Legendre symbols with the same number of factors to obtain

$$S = \sum_{r=1}^{p-(n-1)^3-1} (-1)^{n(n-1)/2} + \sum_{\substack{\mathcal{A} \subseteq \mathcal{S} \\ |\mathcal{A}| \geq 1}} (-1)^{\xi(\mathcal{A})} \sum_{r=1}^{p-(n-1)^3-1} \prod_{i=1}^{|\mathcal{A}|} \left(\frac{r+a_i}{p} \right),$$

where $\xi(\mathcal{A})$ denotes either 0 or 1. We complete the sums by adding up the missing $(n-1)^3+1$ terms and, after using the triangle inequality, we apply Weil's estimate (3) to conclude that for each nonempty $\mathcal{A} \subseteq \mathcal{S}$

$$\left| (-1)^{\xi(\mathcal{A})} \sum_{r=1}^{p-(n-1)^3-1} \prod_{i=1}^{|\mathcal{A}|} \left(\frac{r+a_i}{p} \right) \right| \leq (|\mathcal{A}| - 1)\sqrt{p} + (n-1)^3 + 1$$

holds. Therefore

$$\begin{aligned} \left| S - \left(p - (n-1)^3 - 1\right) \right| &\leq \sum_{i=1}^{(n-1)^2} \binom{(n-1)^2}{i} \left((i-1)\sqrt{p} + (n-1)^3 + 1 \right) \\ &= \left(2^{(n-1)^2} - 1 \right) \left((n-1)^3 + 1 - \sqrt{p} \right) + 2^{(n-1)^2-1}(n-1)^2\sqrt{p} \end{aligned}$$

If $S - \left(p - (n-1)^3 - 1\right) \geq 0$ then, as $p \geq (n-1)^3 + 2$, $S \geq 1$ follows and we are done. Otherwise, if $S - \left(p - (n-1)^3 - 1\right) < 0$ we find that

$$\begin{aligned} S &\geq p - \left(2^{n^2-2n}(n^2-2n-1)+1\right)\sqrt{p} - 2^{(n-1)^2}\left(n^3-3n^2+3n\right) \\ &> p - 2^{n^2}\sqrt{p} - 2^{n^2} > 0, \end{aligned}$$

where the last inequality follows for $p > 2^{2n^2+1}$ via elementary calculus. $\square$

The bounds exhibited in Theorem 4.1 are admittedly enormous, however, when n is fixed one can improve upon these considerably by evaluating (8) with computers. Moreover, one can use several free parameters as exponents in the array (7) similarly to (6) to exhibit further $\mathrm{BH}(np,p)$ matrices with this structure. This approach, however, completely fails when $p \leq 2n-1$, as in this case we simply do not have enough quadratic residues to build up arrays of this type. Constructing these relatively small dimensional examples seems to be a non-trivial task in general. See [21], [26] and [27].

Despite all these difficulties, we hope that the methods used in this paper combined with more sophisticated number theoretic tools and non-trivial computer programming are strong enough to conclude the existence of $\mathrm{BH}(np,p)$ matrices for further (relatively small) values of doubly even numbers n. The first open case $n=8$ is particularly promising, as here the existence of $\mathrm{BH}(8p,p)$ matrices has been confirmed for $p > 19$ in [9]. However, dealing with the single even case, and in particular determining the existence of $\mathrm{BH}(6p,p)$ matrices seems to require some fundamentally new ideas in the future. Addressing the odd case, where several non existence results are already known [5], [11], [33] looks even more elusive.

References

[1] K. Akiyama, M. Ogawa, C. Suetake: *On $STD_6[18;3]s$ and $STD_7[21;3]s$ admitting a semiregular automorphism group of order* 9, Electron. J. Combin., **16**, #R148, 21 pp. (2009).

[2] B. G. Bodmann, H. J. Elwood: *Complex Equiangular Parseval Frames and Seidel Matrices containing pth roots of unity*, Proceedings of the American Mathematical Society, **138**, 4387–4404 (2010).

[3] A. T. Butson: *Generalized Hadamard matrices*, Proc. Am. Math. Soc., **13**, 894–898 (1962).

[4] B. Compton, R. Craigen, W. de Launey: *Unreal $BH(n,6)$'s and Hadamard matrices*, Preprint, (2008).

[5] C. H. Cooke, I. Heng: *On the non-existence of some generalized Hadamard matrices*, Australasian J. Combin. **19**, 137–148 (1999).

[6] R. Craigen: *Signed groups, sequences and the asymptotic existence of Hadamard matrices*, J. Combin. Theory A, **71**, 241–254 (1995).

[7] J. E. Dawson: *A construction for generalized Hadamard matrices* $\mathrm{GH}(4q,\mathrm{EA}(q))$, J. Stat. Plann. and Inference **11**, 103–110 (1985).

[8] J. E. Dawson, W. de Launey: *An Asymptotic Result on the Existence of Generalised Hadamard matrices*, J. Combin. Th. Ser. A **65**, 158–163 (1994).

[9] J. E. Dawson, W. de Launey: *A note on the construction of* $\mathrm{GH}(4tq;EA(q))$ *for* $t=1,2$, Australas. J. Combin. **6**, 177–186 (1992).

[10] W. de Launey: *On the asymptotic existence of Hadamard matrices*, J. Combin. Theory A **116**, 1002–1008 (2009).

[11] W. de Launey: *On the non-existence of generalized Hadamard matrices*, J. Stat. Plann. and Inference **10**, 385–396 (1984).

[12] P. Diţă: *Some results on the parametrization of complex Hadamard matrices*, J. Phys. A: Math. Gen., **37**, 5355–5374 (2004).

[13] T. Durt, B.-G. Englert, I. Bengtsson, K. Życzkowski: *On mutually unbiased bases*, Int. J. Quantum Information, **8**, 535–640 (2010).

[14] M. Harada, C. Lam, A. Munemasa, V. D. Tonchev: *Classification of generalized Hadamard matrices $H(6,3)$ and quaternary Hermitian self-dual codes of length* 18, Elec. J. Combin., **17**, #R171, 14 pp. (2010).
[15] W. Holzmann, H. Kharaghani, W. Orrick: *On the real unbiased Hadamard matrices*, Contemp. Maths., Combinatorics and Graphs, **531**, 243–250 (2010).
[16] R. H. Hudson: *On the first occurrence of certain patterns of quadratic residues and non-residues*, Israel Journal of Mathematics, **44**, 23–32 (1983).
[17] I. D. Ivanovic: *Geometrical description of quantal state determination*, J. Phys. A: Math. Gen., **14**, 3241 (1981).
[18] H. Iwaniec, E. Kowalski: Analytic Number Theory, Colloqium publications (2004).
[19] M. Kolountzakis, M. Matolcsi: *Complex Hadamard matrices and the spectral set conjecture*, Collect. Math., Vol. Extra, 281–291 (2006).
[20] I. Kotsireas, C. Koukouvinos, J. Seberry: *Weighing matrices and string sorting*, Ann. Comb. **13**, 305–313 (2009).
[21] P. H. J. Lampio, P. Östergård: *Classification of difference matrices over cyclic groups*, J. Statistical Inference and Planning, **141**, 1194–1207 (2011).
[22] M. H. Lee, F. Szöllősi: *Hadamard matrices modulo* 5, J. Combin. Designs, to appear (2013).
[23] I. Livinskyi: *Asymptotic existence of Hadamard matrices*, Master's thesis, University of Manitoba, 2012.
[24] M. Matolcsi, I. Z. Ruzsa, M. Weiner: *Systems of mutually unbiased Hadamard matrices containing real and complex Matrices*, The Australasian J. Combin. **55**, p. 35 (2013).
[25] D. McNulty, S. Weigert: *Isolated Hadamard matrices from mutually unbiased product bases*, J. Math. Phys. **53**, 122202 (2012).
[26] G. E. Moorhouse: *The 2-Transitive Complex Hadamard Matrices*, Preprint, `http://www.uwyo.edu/moorhouse/pub/complex.pdf` (2001).
[27] J. Seberry: *A construction for generalized Hadamard matrices*, J. Statistical Planning and Inference, **4**, 365–368 (1980).
[28] E. Seiden: *On the problem of construction of orthogonal arrays*, Ann. Math. Statist. **25**:1, 151–156 (1954).
[29] F. Szöllősi: *Complex Hadamard matrices and equiangular tight frames*, Linear Algebra and its Applications **438**, 1962–1967 (2013).
[30] F. Szöllősi: *Construction, classification and parametrization of complex Hadamard matrices*, PhD thesis, Central European University, Budapest, Hungary (2011).
[31] J. S. Wallis: *On the existence of Hadamard matrices*, J. Combin. Theory **21**, 188–195 (1976).
[32] A. Weil: *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind. 1041, Publ. Inst. Math. Univ. Strasbourg 7 (1945), Hermann et Cie., Paris (1948).
[33] A. Winterhof: *On the non-existence of generalised Hadamard matrices*, J. Statist. Plann. Inference, **84**, 337–342 (2000).

Appendix: A BH(12, 3) and a BH(20, 5) matrix

In this section we exhibit two sporadic examples of $\mathrm{BH}(4p, p)$ matrices. For typographic reasons we display these matrices in "log-form", i.e. the entries $e_p(z)$ of the Butson-type complex Hadamard matrices are replaced by a number $z \in \mathbb{Z}_p$. The first $\mathrm{BH}(12, 3)$ matrix was found by Seiden [28]. Actually, it is a sporadic example of difference matrices (see [21]):

$$S_{12} = \begin{bmatrix} 0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&1&1&1&1&2&2&2&2\\ 0&0&1&2&2&2&0&1&1&1&2&0\\ 1&0&0&2&2&1&0&2&2&0&1&1\\ 1&2&0&0&0&2&2&1&1&0&2&1\\ 0&0&2&1&0&1&2&2&0&1&2&1\\ 0&2&1&0&1&2&0&2&0&2&1&1\\ 1&0&2&0&1&2&2&0&2&1&1&0\\ 0&2&0&1&2&2&1&0&2&1&0&1\\ 2&0&0&1&0&2&1&2&1&2&1&0\\ 2&0&1&0&2&1&2&0&1&2&0&1\\ 0&1&0&0&2&0&2&2&1&1&1&2 \end{bmatrix}.$$

The following BH(20, 5) matrix is a particular example of an infinite family of generalized Hadamard matrices, discovered by Seberry [27]:

$$S_{20} = \left[\begin{array}{cccc|cccc|cccc|cccc|cccc} 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&2&2&2&2&4&4&4&4&1&1&1&1&3&3&3&3\\ 0&0&0&0&3&3&3&3&1&1&1&1&4&4&4&4&2&2&2&2\\ 0&0&0&0&4&4&4&4&3&3&3&3&2&2&2&2&1&1&1&1\\ \hline 0&2&3&4&3&4&0&1&4&0&1&2&0&1&2&3&1&2&3&4\\ 0&2&3&4&4&1&3&0&0&2&4&1&1&3&0&2&2&4&1&3\\ 0&2&3&4&0&3&1&4&1&4&2&0&2&0&3&1&3&1&4&2\\ 0&2&3&4&1&0&4&3&2&1&0&4&3&2&1&0&4&3&2&1\\ \hline 0&4&1&3&4&0&1&2&1&3&0&2&3&1&4&2&0&4&3&2\\ 0&4&1&3&0&2&4&1&0&1&2&3&4&3&2&1&4&2&0&3\\ 0&4&1&3&1&4&2&0&3&2&1&0&1&2&3&4&3&0&2&4\\ 0&4&1&3&2&1&0&4&2&0&3&1&2&4&1&3&2&3&4&0\\ \hline 0&1&4&2&0&1&2&3&3&1&4&2&0&4&3&2&4&1&3&0\\ 0&1&4&2&1&3&0&2&4&3&2&1&4&2&0&3&3&4&0&1\\ 0&1&4&2&2&0&3&1&1&2&3&4&3&0&2&4&1&0&4&3\\ 0&1&4&2&3&2&1&0&2&4&1&3&2&3&4&0&0&3&1&4\\ \hline 0&3&2&1&1&2&3&4&0&4&3&2&4&1&3&0&1&4&2&0\\ 0&3&2&1&2&4&1&3&4&2&0&3&3&4&0&1&2&1&0&4\\ 0&3&2&1&3&1&4&2&3&0&2&4&1&0&4&3&4&0&1&2\\ 0&3&2&1&4&3&2&1&2&3&4&0&0&3&1&4&0&2&4&1 \end{array}\right].$$

FERENC SZÖLLŐSI: RESEARCH CENTER FOR PURE AND APPLIED MATHEMATICS, GRADUATE SCHOOL OF INFORMATION SCIENCES, TOHOKU UNIVERSITY, SENDAI 980-8579, JAPAN

E-mail address: szoferi@gmail.com