MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

ORDERLY GENERATION OF BUTSON HADAMARD MATRICES

PEKKA H.J. LAMPIO, PATRIC R.J. ÖSTERGÅRD, AND FERENC SZÖLLŐSI

Abstract. In this paper Butson-type complex Hadamard matrices $\mathrm{BH}(n, q)$ of order n over the complex qth roots of unity are classified for small parameters by computer-aided methods. The results include a classification of $\mathrm{BH}(21, 3)$, $\mathrm{BH}(16, 4)$, and $\mathrm{BH}(14, 6)$ matrices. There are exactly 72, 1786763, and 167776 such matrices, respectively, up to monomial equivalence. Additionally, an example of a $\mathrm{BH}(14, 10)$ matrix is shown for the first time, and the nonexistence of $\mathrm{BH}(8, 15)$, $\mathrm{BH}(11, q)$ for $q \in \{10, 14, 15\}$, and $\mathrm{BH}(13, 15)$ matrices is proved.

1. Introduction

Let n and q be positive integers, and let $\zeta_q := \exp(2\pi\mathbf{i}/q)$ be the canonical complex qth root of unity. A Butson-type complex Hadamard matrix of order n over the complex qth roots of unity is an $n \times n$ matrix H with elements ζ_q^i, $i \in \{0, \ldots, q-1\}$, such that $HH^* = nI_n$, where I_n denotes the identity matrix of order n, and H^* denotes the conjugate transpose of H. The rows (and columns) of H are therefore pairwise orthogonal in $\mathbb{C}^n$. For a fixed n and q we denote the set of all Butson-type complex Hadamard matrices by $\mathrm{BH}(n, q)$, and we simply refer to them as "Butson matrices" for brevity [22]. The simplest examples of Butson matrices are the Fourier matrices $F_n := [\zeta_n^{ij}]_{i,j=1}^n \in \mathrm{BH}(n, n)$, frequently appearing in various branches of mathematics [51].

A major unsolved problem in design theory is the "Hadamard Conjecture" which predicts the existence of $\mathrm{BH}(n, 2)$ matrices (real Hadamard matrices) for all orders divisible by 4. The concept of Butson matrices was introduced to shed some light onto this question from a more general perspective [7]. Complex Hadamard matrices play an important role in the theory of operator algebras [16], [38], and they have also applications in harmonic analysis [29]. Currently there is a renewed interest in complex Hadamard matrices due to their connection to various concepts of quantum information theory, e.g., to quantum teleportation schemes and to mutually unbiased bases [3], [11], [23], [51], [53].

This paper is concerned with the computer-aided generation and classification of Butson matrices. Let X and Y be $n \times n$ monomial matrices, that is, they have exactly one nonzero entry in each of their rows and columns which is a complex qth root of unity. The group G of pairs of monomial matrices acts on the Butson matrices H by $H^{(X,Y)} \mapsto XHY^*$. Two Butson matrices H_1 and H_2 are called (monomial) equivalent, if they are in the same G-orbit. The automorphism group

Received by the editor April 4, 2019.
2010 *Mathematics Subject Classification.* Primary 05B20.
This research was supported in part by the Academy of Finland, Grant #289002.

of H, denoted by $\mathrm{Aut}(H)$ is the stabilizer subgroup of G with respect to H. Note that if $H \in \mathrm{BH}(n,q)$ then naturally $H \in \mathrm{BH}(n,r)$ for any r being a multiple of q. Therefore the group $\mathrm{Aut}(H)$ depends on the choice of q.

Earlier work predominantly considered the classification of the real case in a series of papers [25], [27], [46], see also [19, Section 7.5] for a historical overview. The quaternary case also received some attention in [36] and [49]. Other papers in the literature deal with settling the simpler existence problem through combinatorial constructions [3], [45], [47], [48] or focus on the generation of matrices with some special structure [2], [4], [8], [9], [12], [13], [21], [37].

The outline of this paper is as follows. In Section 2 we give a short overview of computer representation of Butson matrices and recall the concept of vanishing sums of roots of unity. In Section 3 we briefly describe the method of orderly generation which serves as the framework used for equivalence-free exhaustive generation. In Section 4 we present three case studies: the classification of $\mathrm{BH}(16,4)$ matrices; the classification of $\mathrm{BH}(21,3)$ matrices; and the nonexistence of $\mathrm{BH}(n,q)$ matrices for several values n and q. An additional contribution of this section is Theorem 4.7, which establishes a connection between unreal $\mathrm{BH}(n,6)$ matrices and $\mathrm{BH}(2n,4)$ matrices. In Section 5 we discuss our efforts in verifying the computational results. We conclude the paper in Section 6 with several open problems.

The results of this paper extend [3, Theorem 7.10], where the (non)existence of Butson matrices is settled for $n \leq 10$ and $q \leq 14$. The reader might wish to jump ahead to Table 2 to get a quick overview of the known number of $\mathrm{BH}(n,q)$ matrices for $n \leq 21$ and $q \leq 17$, including the new results established in this paper. The generated matrices are available as an electronic supplement on the web [35]. The interested reader is also referred to [6] where various parametric families of complex Hadamard matrices [11] can be found, based on the catalog in [51].

2. Computer representation of Butson Hadamard matrices

A Butson matrix $H \in \mathrm{BH}(n,q)$ is conveniently represented in logarithmic form, that is, the matrix $H = [\zeta_q^{\psi_{i,j}}]_{i,j=1}^n$ is represented by the matrix $L(H) := [\psi_{i,j} \bmod q]_{i,j=1}^n$ with the convention that $L_{i,j} \in \mathbb{Z}_q$ for all $i,j \in \{1,\ldots,n\}$. Throughout this paper we denote by $\mathbb{Z}_q$ the additive group of integers modulo q, where the underlying set is $\{0,\ldots,q-1\}$. With this convention $(\mathbb{Z}_q^n, \preceq)$ is a linearly ordered set, where for $a,b \in \mathbb{Z}_q^n$ we write $a \preceq b$ if and only if $a = b$ or a lexicographically precedes b.

Example 2.1. The following is a $\mathrm{BH}(14,10)$ matrix H, displayed in logarithmic form.

$$L(H) = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&5&5&5&5&5&5&5\\
0&0&2&4&5&6&8&0&0&2&4&5&6&8\\
0&1&5&9&7&5&3&7&9&5&1&2&7&3\\
0&2&6&8&4&2&7&9&4&7&5&1&3&9\\
0&2&8&6&0&4&5&3&7&3&9&5&1&8\\
0&4&2&6&8&0&5&9&5&0&1&7&5&3\\
0&4&6&2&6&8&1&5&7&1&3&9&2&7\\
0&5&0&4&6&2&8&4&2&6&0&1&8&6\\
0&6&4&0&2&8&5&5&3&1&8&3&7&9\\
0&6&4&5&2&8&0&0&8&6&8&3&2&4\\
0&6&9&8&4&4&2&8&2&2&6&7&0&4\\
0&8&4&2&8&3&6&4&0&8&6&7&2&2\\
0&8&8&4&2&6&3&2&5&7&3&9&7&1
\end{bmatrix}, \quad |\mathrm{Aut}(H)| = 20.$$

Observe that the matrix shown in Example 2.1 is in dephased form [51], that is, its first row and column are all 0 (representing the logarithmic form of 1). Every

matrix can be dephased by using equivalence-preserving operations. Throughout this paper all matrices are assumed to be dephased.

Let $H \in \mathrm{BH}(n,q)$, and let $r_1, r_2 \in \mathbb{Z}_q^n$ be row vectors of $L(H)$. Then, by complex orthogonality, the difference row $d := r_1 - r_2 \in \mathbb{Z}_q^n$ satisfies $\mathcal{E}_{n,q}(d) = 0$, where

$$\mathcal{E}_{n,q} \colon \mathbb{Z}_q^n \to \mathbb{C}, \qquad \mathcal{E}_{n,q}(x) := \sum_{i=1}^{n} \zeta_q^{x_i}$$

is the evaluation function. In other words, d represents an n-term vanishing sum of qth roots of unity [32]. We note that the number $\mathcal{E}_{n,q}(x)$ is algebraic, and its value is invariant up to permutation of the coordinates of $x \in \mathbb{Z}_q^n$. In particular, $\mathcal{E}_{n,q}(x) = \mathcal{E}_{n,q}(\mathrm{Sort}(x))$, where $\mathrm{Sort}(x) = \min\{\sigma(x) \colon \sigma \text{ is a permutation on } n \text{ elements}\}$ (with respect to the ordering $\preceq$).

We introduce the orthogonality set, which contains the representations of the normalized, sorted, n-term vanishing sums of qth roots of unity:

$$\mathcal{O}(n,q) := \{x \in \mathbb{Z}_q^n \colon x_1 = 0;\ x = \mathrm{Sort}(x);\ \mathcal{E}_{n,q}(x) = 0\}.$$

Once precomputed, the set $\mathcal{O}(n,q)$ allows us to determine if two rows of length n of a dephased matrix with elements in $\mathbb{Z}_q$ are complex orthogonal in a combinatorial way, i.e., without relying on the analytic function $\mathcal{E}_{n,q}$. Indeed, for any vector $x \in \mathbb{Z}_q^n$ having at least one 0 coordinate, $\mathcal{E}_{n,q}(x) = 0$ if and only if $\mathrm{Sort}(x) \in \mathcal{O}(n,q)$.

One can observe that for certain values of n and q the set $\mathcal{O}(n,q)$ is empty, that is, it is impossible to find a pair of orthogonal rows in $\mathbb{Z}_q^n$ and consequently $\mathrm{BH}(n,q)$ matrices do not exist. For example, it is easy to see that $|\mathcal{O}(n,2)| = 0$ for odd $n > 1$. The following result characterizes the case when the set $\mathcal{O}(n,q)$ is nonempty and should be viewed as one of the fundamental necessary conditions on the existence of Butson matrices.

Theorem 2.2 ([32, Theorem 5.2])**.** *Let n, r, and a_i, $i \in \{1,\dots,r\}$ be positive integers, and let $q = \prod_{i=1}^{r} p_i^{a_i}$ with distinct primes p_i, $i \in \{1,\dots,r\}$. Then, we have $|\mathcal{O}(n,q)| \geq 1$ if and only if there exist nonnegative integers w_i, $i \in \{1,\dots,r\}$ such that $n = \sum_{i=1}^{r} w_i p_i$.*

In order to classify all $\mathrm{BH}(n,q)$ matrices for given parameters, three tasks have to be completed: (i) the set $\mathcal{O}(n,q)$ has to be determined; (ii) vectors $x \in \mathbb{Z}_q^n$ orthogonal to a prescribed set of vectors should be generated; and (iii) equivalent matrices should be rejected. In the next section we discuss these three tasks in detail.

3. Generating Butson Hadamard matrices

3.1. **Generating the vanishing sums of roots of unity.** For a given n and q, our first task is to determine the set $\mathcal{O}(n,q)$ which in essence encodes complex orthogonality of a pair of rows. It turns out that when q is a product of at most two prime powers, then a compact description of the elements of $\mathcal{O}(n,q)$ is possible. The following two results are immediate consequences of [32, Corollary 3.4].

Lemma 3.1. *Let a, n be positive integers, and let $q = p^a$ be a prime power. Let $e = [1,1,\dots,1] \in \mathbb{Z}_q^p$. Let $u = [0, q/p, 2q/p, \dots, (p-1)q/p] \in \mathbb{Z}_q^p$, and let $x \in \mathbb{Z}_q^n$. Then $x \in \mathcal{O}(n,q)$ if and only if there exist a positive integer s such that $ps = n$, and $r_i \in \{0,\dots,q/p-1\}$, $i \in \{1,\dots,s-1\}$, such that $x = \mathrm{Sort}([u, r_1 e+u, \dots, r_{s-1} e+u])$.*

Lemma 3.2. *Let a, b and n be positive integers, and let $q = p_1^a p_2^b$ be the product of two distinct prime powers. Let $e_f = [1, 1, \ldots, 1] \in \mathbb{Z}_q^f$ for $f \in \{p_1, p_2\}$. Let $u = [0, q/p_1, 2q/p_1, \ldots, (p_1-1)q/p_1] \in \mathbb{Z}_q^{p_1}$, $v = [0, q/p_2, 2q/p_2, \ldots, (p_2-1)q/p_2] \in \mathbb{Z}_q^{p_2}$, and let $x \in \mathbb{Z}_q^n$. Then $x \in \mathcal{O}(n, q)$ if and only if there exist nonnegative integers s, t such that $p_1 s + p_2 t = n$, and $r_i \in \{0, \ldots, q/p_1 - 1\}$, $i \in \{1, \ldots, s\}$, $R_j \in \{0, \ldots, q/p_2 - 1\}$, $j \in \{1, \ldots, t\}$ such that $x = \mathrm{Sort}([r_1 e_{p_1} + u, r_2 e_{p_1} + u, \ldots, r_s e_{p_1} + u, R_1 e_{p_2} + v, R_2 e_{p_2} + v, \ldots, R_t e_{p_2} + v])$, and $0 \in \{r_1, R_1\}$.*

The main point of the rather technical Lemma 3.1 and Lemma 3.2 is the following: as long as q is the product of at most two prime powers, the constituents of any n-term vanishing sum of qth roots of unity are precisely p-term vanishing sums, where p is some prime divisor of q. These p-term vanishing sums are in turn the (scalar multiplied, or, "rotated") sums of every pth root of unity.

The significance of these structural results is that based on them one can generate the set $\mathcal{O}(n, q)$ for $q < 30 = 2 \cdot 3 \cdot 5$ in a combinatorial way, that is, without the need of the analytic function $\mathcal{E}_{n,q}$. Indeed, by Lemma 3.1 the generation of $\mathcal{O}(n, q)$ for $q = p^a$ and $n = ps$ relies only on the generation of the set of possible rotations $0 \le r_1 \le \cdots \le r_{s-1} \le q/p - 1$. In particular, this task can be done by using exact integer arithmetic.

In certain simple cases it is possible to enumerate (as well as to generate) the set $\mathcal{O}(n, q)$ by hand. We offer the following counting formulae for means of checking consistency.

Lemma 3.3. *Let a and n be positive integers, and let $q = p^a$ be a prime power. Assume that p divides n. Then $|\mathcal{O}(n, q)| = \binom{(n+q)/p-2}{n/p-1}$.*

Proof. Let $e = [1, 1, \ldots, 1] \in \mathbb{Z}_q^p$. By Lemma 3.1 elements of the set $\mathcal{O}(n, q)$ can be partitioned into n/p parts of the form $r_i e + [0, q/p, 2q/p, \ldots, (p-1)q/p]$, each part being identified by the rotation $r_i \in \{0, \ldots, q/p - 1\}$, $i \in \{0, \ldots, n/p - 1\}$ with $r_0 = 0$. The number of ways to assign q/p values to a set of $n/p - 1$ variables (up to relabelling) is exactly $\binom{(n+q)/p-2}{n/p-1}$; each of these choices lead to different elements of $\mathcal{O}(n, q)$. □

A slightly more complicated variant is the following result.

Lemma 3.4. *Let $n \ge 2$ be an integer, let p be an odd prime, and let $q = 2p$. Then*

$$|\mathcal{O}(n, q)| = \delta + \frac{1 + (-1)^n}{2} \binom{p + \lfloor n/2 \rfloor - 2}{\lfloor n/2 \rfloor - 1} + \sum_{\substack{2s+pt=n \\ s \ge 1, t \ge 1}} \frac{p + 2s - 1}{s} \binom{p + s - 2}{s - 1},$$

where $\delta = 1$ if p divides n, and $\delta = 0$ otherwise.

Proof. This can be inferred by using Lemma 3.2. We count the elements $x \in \mathcal{O}(n, q)$ based on how many pairs of coordinates $[x_i, x_i + p] \in \mathbb{Z}_q^2$ they have. Let us denote the number of such pairs by s.

If $s = 0$, then clearly p divides n and x can be partitioned into $t = n/p$ parts, each being either of the form $[0, 2, 4, \ldots, 2p - 2]$ or $[1, 3, 5, \ldots, 2p - 1]$. However, since $s = 0$, only one of these two forms could appear, and since x must have a coordinate 0, this leaves us with only $\delta = 1$ case.

If $s = n/2 \ge 1$ then n is necessarily even, and x can be partitioned into $n/2$ parts, each being of the form $[x_i, x_i + p]$ for some $x_i \in \{0, \ldots, p - 1\}$, $i \in \{1, \ldots, n/2\}$.

Since x must contain 0, one of these parts must be $[0,p]$, while the other $n/2-1$ parts can take p different forms. There are a total of $\binom{p+n/2-2}{n/2-1}$ cases.

Finally, if $0<s<n/2$, then there are either $t=(n-2s)/p\geq 1$ parts of the form $[0,2,4,\ldots,2p-2]$ or t parts of the form $[1,3,5,\ldots,2p-1]$. In the first case there are $\binom{p+s-1}{s}$ ways to assign values to the remaining s parts; in the second case, since x must have a 0 coordinate, there are $\binom{p+s-2}{s-1}$ ways to assign values to the remaining s parts. The sum of these two numbers is shown in the statement. □

The statements of Lemma 3.3 and Lemma 3.4 are strong enough to cover all cases $q\leq 17$ except for $q\in\{12,15\}$. We have applied these results to verify that the computer-generated sets $\mathcal{O}(n,q)$ are of the correct cardinality. In the next subsection we will see a further application of the set $\mathcal{O}(n,q)$.

Remark 3.5. There is no analogous result to Lemma 3.1 and Lemma 3.2 when q has more than two prime factors. For example, $[0,1,7,13,19,20]\in\mathcal{O}(6,30)$ but does not have any m-term vanishing subsums with $m\in\{2,3,5\}$. See [32, Example 6.7] for examples of similar flavor.

An alternative, algebraic way to generate the set $\mathcal{O}(n,q)$ is to compute for all $x\in\mathbb{Z}_q^n$ with $x_1=0$ and $\mathrm{Sort}(x)=x$ the minimal polynomial $p(t)$ of the algebraic number $\mathcal{E}_{n,q}(x)$. With this terminology, $x\in\mathcal{O}(n,q)$ if and only if $p(t)=t$. The efficiency of this approach can be greatly improved by testing first by fast numerical means whether the Euclidean norm of $\mathcal{E}_{n,q}(x)$ is small, say if $\|\mathcal{E}_{n,q}(x)\|^2=\mathcal{E}_{n,q}(x)\mathcal{E}_{n,q}(-x)<0.01$ holds.

A further approach, based on cyclotomic polynomials, was followed in [30, Section 3.1].

3.2. **Orderly generation of rectangular matrices.** In this section we briefly recall the method of orderly generation, which is a technique for generating matrices exhaustively in a way that no equivalence tests between different matrices are required [14], [24, Section 4.2.2], [43]. Such a search can be efficiently executed in parallel. The main idea is to select from each equivalence class of Butson matrices a canonical representative, and organize the search in a way to directly aim for this particular matrix. Variations of this basic approach were employed for the classification of $\mathrm{BH}(n,2)$ matrices for $n\leq 32$, see [25], [46].

Let $n,r\geq 1$. We associate to each $r\times n$ matrix R whose elements are complex qth roots of unity its vectorization $v(R):=[L(R)_{1,1},\ldots,L(R)_{1,n},L(R)_{2,1},\ldots,L(R)_{r,n}]\in\mathbb{Z}_q^{rn}$ formed by concatenating the rows of its logarithmic form $L(R)$. We say that R is in canonical form, if $v(R)=\min\{v(XRY^*)\colon X \text{ and } Y \text{ are } q\text{th root monomial matrices}\}$, where comparison is done with respect to the ordering $\preceq$. Canonical matrices defined in this way have a number of remarkable properties. For example, if R is canonical, and r_1 and r_2 are consecutive rows of $L(R)$, then $r_1\preceq r_2$, and analogously for the columns. Moreover, canonical matrices are necessarily dephased. Let σ be a permutation on r elements, and let $i\in\{1,\ldots,n\}$. Let us denote by $R^{(\sigma,i)}$ the matrix which can be obtained from R by permuting its rows according to σ, then swapping its first and ith columns, then dephasing it, and finally arranging its columns according to $\preceq$.

Lemma 3.6. *Let $n,r\geq 1$, and let R be an $r\times n$ matrix. The matrix R is canonical, if and only if $v(R)=\min\{v(R^{(\sigma,i)})\colon \sigma$ is a permutation on r elements; $i\in\{1,\ldots,n\}\}$.*

Proof. This is an immediate consequence of the fact that canonical matrices are dephased and their columns are sorted with respect to $\preceq$. □

Testing canonicity is the most time-consuming part of the search. The naive implementation of Lemma 3.6 requires to go through and test the combination of all $r!$ row permutations and all n column promotions. Note that the number of tests required is independent of the parameter q. In certain cases testing a permutation yields structural information which we can exploit in order to reduce the overall number of tests required. Implementing the following additional considerations could greatly improve the efficiency of testing canonicity.

For $k \in \{1, \ldots, r\}$ let R_k denote the leading $k \times n$ submatrix of the matrix R. Let σ be a permutation on r elements, and let $k \in \{1, \ldots, r\}$. The main idea is to look at the matrices $R_k^{(\sigma,i)}$ for fixed σ and k as i runs through every $\{1, \ldots, n\}$ and compare $v(R_k)$ with $v(R_k^{(\sigma,i)})$ with respect to the ordering $\preceq$. First, if for all $i \in \{1, \ldots, n\}$ we find that $R_k^{(\sigma,i)} \neq R_k$ and $v(R_k) \preceq v(R_k^{(\sigma,i)})$ then none of the row permutations τ for which $R_k^{(\sigma,1)} = R_k^{(\tau,1)}$ holds should be tested. Secondly, if there exists a column index $\iota \in \{1, \ldots, n\}$ such that $R_k^{(\sigma,\iota)} \neq R_k$ and $v(R_k^{(\sigma,\iota)}) \preceq v(R_k)$ then the matrix R cannot be canonical. Finally, when testing multiple matrices one after another for canonicity, say R and then S, then any potentially discovered pair (σ, ι) witnessing the non-canonicity of the matrix R could be stored in a temporary cache and then reused later as a first weak check on S. In particular, if $S^{(\sigma,\iota)} \neq S$ and $v(S^{(\sigma,\iota)}) \preceq v(S)$, then S can be discarded after this single test. An efficient algorithm for generating permutations with restricted prefixes is discussed in [28, Algorithm X].

Finally, we note one more property of canonical matrices.

Lemma 3.7. *Let $H \in \mathrm{BH}(n, q)$ in canonical form, and let r_2 and c_2 denote the second row and the second column of $L(H)$. Then $r_2 \in \mathcal{O}(n, q)$ and $c_2^T \in \mathcal{O}(n, q)$.*

Proof. This follows from the fact that H, whose columns are pairwise orthogonal, is necessarily dephased, and the rows and columns of $L(H)$ are ordered with respect to the ordering $\preceq$. □

The significance of Lemma 3.7 is that if the (transpose of the) logarithmic form of the second column of a rectangular orthogonal matrix is not a prefix of any of the elements of the set $\mathcal{O}(n, q)$, then that matrix can be discarded during the search. We refer to this look-ahead strategy as "pruning the search tree by the second column condition".

The matrices $H \in \mathrm{BH}(n, q)$ (more precisely, their logarithmic form) are generated in a row-by-row fashion. Every time a new row is appended we first test whether it is orthogonal to all previous rows by checking if the difference vectors belong to the set $\mathcal{O}(n, q)$ as described in Section 3.1. If the rows of the matrix are pairwise orthogonal, then we further check whether (the transpose of) its second column is a prefix of an element of the set $\mathcal{O}(n, q)$. Finally, we test whether it is in canonical form. Only canonical matrices will be processed further, the others will be discarded and backtracking takes place.

Remark 3.8. In a prequel to this work [36] we employed the method of canonical augmentation [42, Section 4.2.3] to solve the more general problem of classification

TABLE 1. Comparison of the size of the search trees.

r	BH(14, 4)	
	without pruning	with pruning
1	1	1
2	4	4
3	42	42
4	10141	9142
5	1601560	637669
6	21311746	2118948
7	17175324	189721
8	4234669	155777
9	1675882	108598
10	716604	56103
11	249716	17992
12	62739	5558
13	9776	3039
14	752	752

of all rectangular orthogonal matrices. That approach relies on a graph representation of Butson matrices (see [33], [34] for more details). Here we solve the relaxed problem of classification of those matrices which can be a constituent of an orderly-generated Butson matrix. The reader might wish to look at the impact of the second column pruning strategy on the number of $r \times 14$ submatrices in Table 1, where we compare the size of the search trees encountered with these two methods during the classification of BH$(14, 4)$ matrices.

3.3. **Augmenting rectangular orthogonal matrices.** Let $n, r \geq 1$, and let R be an $r \times n$ canonical matrix with pairwise orthogonal rows. Let r_i, $i \in \{1, \ldots, r\}$ denote the rows of $L(R)$. The goal of this section is to describe methods for generating the vectors $x \in \mathbb{Z}_q^n$ such that $\mathcal{E}_{n,q}(r_i - x) = 0$ hold simultaneously for every $i \in \{1, \ldots, r\}$. Note that since we are only interested in canonical Butson matrices, we assume that $x_1 = 0$.

The most straightforward way of generating the vectors x is to consider the permutations of the elements of the set $\mathcal{O}(n, q)$. Such a choice of x ascertains orthogonality to the first row. Indeed, the condition $\mathcal{E}_{n,q}(r_1 - x) = 0$ together with the assumption that x has a coordinate 0 is equivalent to $\mathrm{Sort}(x) \in \mathcal{O}(n, q)$ and therefore no other choice for x is possible. For all such vectors x, orthogonality to the other rows, namely, the conditions $\mathcal{E}_{n,q}(r_i - x) = 0$, $i \in \{2, \ldots, r\}$ should be further verified. This strategy of generating the rows works very well for small matrices, say, up to $n \leq 11$. One advantage of this naïve method is that permutations can be generated one after another, without the need of excessive amount of memory [28]. However, with growing n the impact of this part on the overall generating algorithm grows and a more sophisticated approach is requried.

In what follows we describe a more efficient meet-in-the-middle caching strategy [24, p. 157] for generating the vectors x. Let $m \in \{1, \ldots, n-1\}$ be some fixed parameter, and for every $i \in \{1, \ldots, r\}$ write $r_i = [a_i, b_i]$, and write $x = [c, d]$, where $a_i, c \in \mathbb{Z}_q^{n-m}$ and $b_i, d \in \mathbb{Z}_q^m$. The main idea is to precompute a lookup table $\mathcal{T}$ indexed by $\iota \in \mathbb{C}^r$, whose elements are the level sets of (r copies of what is essentially) the function $\mathcal{E}_{m,q}$, that is, $\mathcal{T}(\iota) := \{d \in \mathbb{Z}_q^m \colon [\mathcal{E}_{m,q}(b_1 - d), \ldots, \mathcal{E}_{m,q}(b_r - d)] = \iota\}$. Then, for every $c \in \mathbb{Z}_q^{n-m}$ we look up the vectors $d \in \mathcal{T}([-\mathcal{E}_{n-m,q}(a_1 - c), \ldots, -\mathcal{E}_{n-m,q}(a_r - c)])$. By construction, the vectors $x = [c, d]$ (and only they) satisfy the desired conditions for a new row of the orthogonal matrix R. In order to overcome the difficulty of indexing the table $\mathcal{T}$ by complex r-tuples, we offer

the next result which associates to the complex numbers $\mathcal{E}_{n,q}(x)$ a unique integer vector $\gamma(x)$. We denote by $\varphi(.)$ the Euler's totient function.

Lemma 3.9. *Let $n, q \geq 2$ be integers, and let $x \in \mathbb{Z}_q^n$. There exists a unique integer vector $\gamma(x) \in \mathbb{Z}^{\varphi(q)}$ such that $\mathcal{E}_{n,q}(x) = \sum_{i=1}^{\varphi(q)} \gamma(x)_i \zeta_q^{i-1}$.*

Proof. Consider the vector space of complex numbers $\mathbb{C}$ over the field of rationals $\mathbb{Q}$, and let $B := \{\zeta_q^i \colon i \in \{0, \ldots, \varphi(q)-1\}\}$. Since the qth cyclotomic polynomial Φ_q (which is the minimal polynomial of ζ_q) is of degree $\varphi(q)$, the set B is linearly independent. Moreover, for $k \geq \varphi(q)$ the polynomial equality $z^k = z^k - z^{k-\varphi(q)}\Phi_q(z)$ shows a recursive way to express ζ_q^k as an integer linear combination of elements of B. Consequently the set B generates the complex numbers $\mathcal{E}_{n,q}(x)$ for any $x \in \mathbb{Z}_q^n$. In particular, there exists a unique coordinate $\gamma(x) \in \mathbb{Z}^{\varphi(q)}$ such that $\mathcal{E}_{n,q}(x) = \sum_{i=1}^{\varphi(q)} \gamma(x)_i \zeta_q^{i-1}$. □

Now with the aid of Lemma 3.9 we can index $\mathcal{T}$ with vectors $\kappa \in \mathbb{Z}^{\varphi(q)r}$ in the following way: let $\mathcal{T}(\kappa) := \{d \in \mathbb{Z}_q^m \colon [\gamma(b_1 - d), \ldots, \gamma(b_r - d)] = \kappa\}$. Then, for every $c \in \mathbb{Z}_q^{n-m}$ we look up the vectors $d \in \mathcal{T}([-\gamma(a_1 - c), \ldots, -\gamma(a_r - c)])$ to have all $x = [c, d] \in \mathbb{Z}_q^n$.

The table $\mathcal{T}$ is generated once for every matrix R, and it is reused again when R is augmented with more than one row. To optimize the speed of the algorithm, m should be chosen close to $n/2$. However, with growing parameters, the size of the data structures increases, and a smaller value of m might have to be chosen due to memory constraints.

Remark 3.10. Continuing with the notation used in this section, for $q \in \{2, 3, 4, 6\}$ we point out yet another way to create a lookup table $\mathcal{T}$. The main idea is to exploit the fact that for these particular values of q the square of the Euclidean norm $\|\mathcal{E}_{n,q}(x)\|^2$ is a nonnegative integer. Let p_{big} be a (large) prime, and let $p_i \ll p_{\text{big}}$, $i \in \{1, \ldots, r\}$ be r other distinct primes. Let $\mu \in \mathbb{Z}_{p_{\text{big}}}$, and let $\mathcal{T}(\mu) := \{d \in \mathbb{Z}_q^m \colon \sum_{i=1}^r \|\mathcal{E}_{m,q}(b_i - d)\|^2 p_i \equiv \mu \pmod{p_{\text{big}}}\}$. For every $c \in \mathbb{Z}_q^{n-m}$ we look up the vectors $d \in \mathbb{Z}_q^m$ contained in the set $\mathcal{T}(k)$, where $k \in \mathbb{Z}_{p_{\text{big}}}$ is chosen so that $k \equiv \sum_{i=1}^r \|\mathcal{E}_{n-m,q}(a_i - c)\|^2 p_i \pmod{p_{\text{big}}}$ holds. Finally, the vectors $x = [c, d]$ should be tested for orthogonality.

4. Results and case studies

4.1. **Main results and discussion.** Based on the framework developed in Sections 2 and 3 we were able to enumerate the set $\mathrm{BH}(n, q)$ for $n \leq 11$ and $q \leq 17$ up to monomial equivalence (cf. [3, Theorem 7.10]). Several additional cases were also settled.

Theorem 4.1. *The known values of the exact number of $\mathrm{BH}(n, q)$ matrices, up to monomial equivalence, is displayed in Table 2.*

The legend for Table 2 is as follows. An entry in the table at position (n, q) indicates the known status of the existence of $\mathrm{BH}(n, q)$ matrices. Empty cells indicate cases where $\mathrm{BH}(n, q)$ matrices do not exist by Theorem 2.2; cells marked by an "E" indicate cases where $\mathrm{BH}(n, q)$ matrices are known to exist, but no full classification is available; cells marked by an "U" indicate that existence is unknown;

TABLE 2. The number of BH(n, q) matrices up to monomial equivalence.

$n \setminus q$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
2	1		1		1		1		1		1		1		1	
3		1			1			1			1			1		
4	1		2		2		3		3		4		4		5	
5				1	0				1		0			1		
6	0	1	1		4		3	1	0		11		0	1	5	
7					2	1			0		4		1			
8	1		15		36		143		299		756		1412	0	2807	
9		3			17			23	1		65		0	93		
10	0		10	1	34		60		51		577		0	1	310	
11					0				0	1	0		0	0		
12	1	2	319		8703		53024	8	293123		4497733		E	E	E	
13					436				0		E	1	0	0		
14	0		752		167776	3	E		E		E		E	U	E	
15		0		0	0			0	0		U		0	E		
16	5		1786763		E		E		E		E		E	U	E	
17					0				0		U		0	U		1
18	0	85	E		E		E	E	E		E		U	E	E	
19					E				0		E		0	U		
20	3		E	E	E		E		E		E		E	E	E	
21		72			E	0		E	0		E		0	E		

finally, cells displaying a number indicate the exact number of BH(n, q) matrices up to monomial equivalence.

Next we briefly review the contents of Table 2, and comment on the cases based on the parameter $q \in \{2, 3, \ldots, 17\}$. We note that most of the numbers shown are new.

$q = 2$: This is the real Hadamard case. Complete classification is available up to $n \leq 32$, see [19, Section 7.5], [25], [26]. The number of BH$(36, 2)$ matrices is at least 1.8×10^7 [40], while according to [31] the number of BH$(40, 2)$ matrices is at least 3.66×10^{11}.

$q = 3$: Complete classification is available up to $n \leq 21$, see Section 4.3. The case BH$(18, 3)$ was reported in [17] (see also [33]). Several cases of BH$(21, 3)$ were found by Brock and Murray as reported in [2] along with additional examples. There are no BH$(15, 3)$ matrices [17], [19, Theorem 6.65], [33, Theorem 3.2.2].

$q = 4$: Classification is known up to $n \leq 16$, see [36], [49] and Section 4.2. The difference matrices over $\mathbb{Z}_4$ with $\lambda = 4$ (essentially: the BH$(16, 4)$ matrices of type 4, see Section 4.2) were reported independently in [15], [18], [34]. A BH$(18, 4)$ can be constructed from a symmetric conference matrix [45, Theorem 3], [52].

$q = 5$: An example of BH$(10, 5)$ can be obtained from doubling [7]. An explicit example of BH$(20, 5)$ can be found in [48], based on [44, Theorem 1], while a BH$(15, 5)$ does not exist [10, Theorem 4.2], [19, Theorem 6.65], [33, Theorem 3.2.2].

$q = 6$: Examples of BH$(7, 6)$ matrices were presented in [5] and independently but slightly later in [42]. A BH$(10, 6)$ was reported in [1, p. 105]. Several unreal BH$(13, 6)$ were reported in [8]; additional examples were reported in [30]. A BH$(19, 6)$ was found in [47], based on the approach of [42]. A necessary condition on the existence of a BH$(n, 6)$ matrix comes from the determinant equation $\|\det(H)\|^2 = n^n$, where the left hand side is the norm of an Eisenstein integer and therefore is of the form $a^2 - ab + b^2$ for some integers a and b [5], [30], [54]. Consequently BH$(n, 6)$ matrices for $n \in \{5, 11, 15, 17\}$ do not exist.

$q = 7$: The BH$(14, 7)$ matrices come from a doubling construction [7], [48] while BH$(21, 7)$ matrices do not exist by [54, Theorem 5].

$q = 8$: Here $n = 1$, or $n \geq 2$ is necessarily even by Theorem 2.2. Existence follows from the existence of BH$(n, 4)$ matrices. A particular example of BH$(6, 8)$ matrix played an important role in disproving the "Spectral set conjecture" in $\mathbb{R}^3$, see [29].

This is one notable example of contemporary applications of complex Hadamard matrices.

$q = 9$: A BH$(15, 9)$ does not exist by [54, Theorem 5].

$q = 10$: Nonexistence of BH$(n, 10)$ for $n \in \{6, 7\}$ was proved in [3]. The discovery of a BH$(9, 10)$ matrix by Beauchamp and Nicoară (found also independently in [23]) was rather unexpected [6]. There are no BH$(11, 10)$ matrices (see [30]) or BH$(n, 10)$ matrices for $n \in \{13, 17, 21\}$ (see [5, Theorem 4.2]). To the best of our knowledge BH$(14, 10)$ matrices were not known prior to this work, and Example 2.1 shows a new discovery.

$q = 11$: The Fourier matrix F_{11} is unique [21].

$q = 12$: A BH$(5, 12)$ does not exist since all 5×5 complex Hadamard were shown to be equivalent to F_5 in [16]. A BH$(11, 12)$ does not exist by [5, Theorem 4.2] (see also [30, Section 3.3] and Table 6).

$q = 13$: The Fourier matrix F_{13} is unique [21].

$q = 14$: Several nonexistence results are known. The matrices BH$(n, 14)$ for $n \in \{6, 9, 10\}$ were shown to be nonexistent in [3]. The matrices BH$(11, 14)$ do not exist by Theorem 4.12 (see also [30]). The matrices BH$(n, 14)$ for $n \in \{13, 17, 19, 21\}$ do not exist by [54, Theorem 5]. Finally, there are no BH$(15, 14)$ matrices by [5, Theorem 4.2].

$q = 15$: There are no BH$(n, 15)$ matrices for $n \in \{8, 11, 13\}$, see Theorem 4.11, Theorem 4.12, and Theorem 4.13 respectively. See also [30] regarding the BH$(11, 15)$ case.

$q = 16$: Here $n = 1$ or $n \geq 2$ is necessarily even. Existence follows from the existence of BH$(n, 4)$ matrices.

$q = 17$: The Fourier matrix F_{17} was shown to be unique in [21].

Examples of matrices corresponding to the cases marked by "E" in Table 2 can be obtained in most cases either by viewing a matrix $H \in \mathrm{BH}(n, q)$ as a member of BH(n, r) where r is a divisor of q or by considering the Kronecker product of two smaller matrices [22, Lemma 4.2]. In particular, if $H \in \mathrm{BH}(n_1, q_1)$ and $K \in \mathrm{BH}(n_2, q_2)$ then $H \otimes K \in \mathrm{BH}(n_1 n_2, \mathrm{LCM}(q_1, q_2))$, where $\mathrm{LCM}(a, b)$ is the least commmon multiple of the positive integers a and b. This construction shows that Butson matrices of composite orders are abundant. In contrast, very little is known about the prime order case [42].

4.2. **Classification of the BH(16,4) matrices.** Classification of the quaternary complex Hadamard matrices is motivated by their intrinsic connection to real Hadamard matrices, which is best illustrated by the following classical result.

Theorem 4.2 ([9], [52])**.** *Let $n \geq 1$, and let A and B be $n \times n$ $\{-1, 0, 1\}$-matrices such that $A + \zeta_4 B \in \mathrm{BH}(n, 4)$. Then $A \otimes \left[\begin{smallmatrix} 1 & -1 \\ 1 & \end{smallmatrix}\right] + B \otimes \left[\begin{smallmatrix} -1 & 1 \\ 1 & 1 \end{smallmatrix}\right] \in \mathrm{BH}(2n, 2)$.*

It is conjectured [22, p. 68] that BH$(n, 4)$ matrices exist for all even n. The resolution of this "complex Hadamard conjecture" would imply the celebrated Hadamard Conjecture by Theorem 4.2.

The current classification of BH$(16, 4)$ matrices involves several steps. First we generate the set $\mathcal{O}(16, 4)$. We note that $|\mathcal{O}(16, 4)| = 8$ by Lemma 3.3, and these elements can be obtained from Lemma 3.1 by simple hand calculations. Then, we break up the task of classification into 5 smaller subproblems of increasing difficulty based on the presence of certain substructures. This allowed us to experiment with the simpler cases and to develop and test algorithms used for the more involved

TABLE 3. Comparison of the search trees of the BH(16, 4) and BH(16, 2) cases.

r	BH(16, 4)					BH(16, 2)
	Type 0	Type 1	Type 2	Type 3	Type 4	
2	1	1	1	1	1	1
3	9	9	49	26	10	1
4	1397	8633	56097	32893	1679	3
5	1194940	7100100	45512519	14340921	193820	2
6	110431982	334154285	1739437037	250825832	784744	3
7	376589253	529596667	2085549171	126133829	95814	4
8	45784720	30437221	78690938	1960798	1088	4
9	88353309	29707820	49967830	521903	260	4
10	123354601	24749147	28354094	132072	188	7
11	131598863	17398376	14649819	30142	70	7
12	102432783	10364363	6091931	6600	21	15
13	56174515	4729081	1987727	1477	48	8
14	23306156	1981269	739324	778	57	8
15	6999913	579250	246614	327	22	5
16	1599355	136583	50704	106	15	5

TABLE 4. The automorphism group sizes of BH(16, 4) matrices.

|Aut|	#	|Aut|	#	|Aut|	#	|Aut|	#
20643840	1	12288	12	1024	863	96	594
589824	1	8192	54	768	94	64	67186
196608	1	6144	16	512	2410	56	6
172032	4	4096	74	448	2	48	820
98304	4	3840	1	384	212	32	204627
65536	1	3584	1	336	2	28	6
49152	6	3072	47	320	2	24	706
36864	2	2688	3	256	6112	16	406213
24576	6	2048	266	192	260	12	141
21504	2	1536	64	128	18540	8	554877
16384	10	1280	2	112	6	4	522506

ones. In the following we introduce the type of a BH$(n, 4)$ matrix, a concept which is invariant up to monomial equivalence. A similar idea was used during the classification of BH$(32, 2)$ matrices [25].

Definition 4.3. Let $n, r \geq 2$, let R be an $r \times n$ orthogonal matrix with 4th root entries, and let r_1 and r_2 be distinct rows of $L(R)$. Let m denote the number of 0 entries in the difference vector $r_1 - r_2 \in \mathbb{Z}_4^n$, and let $k := \min\{m, n/2 - m\}$. Then the subset of rows $\{r_1, r_2\}$ is said to be of type k. The matrix R is said to be of type k, if $L(R)$ has no two rows which are of type ℓ for any $\ell < k$.

Secondly, we fixed $k \in \{0, \ldots, 4\}$ and generated the 5×16 canonical (see Section 3.2) type-k matrices surviving the second column pruning strategy. Thirdly, we augmented each of these with three additional rows to obtain all 8×16 matrices, but during this process a depth-first-search approach was employed, and the $r \times 16$ submatrices were not kept for $r \in \{6, 7\}$. Finally, we finished the search by using breadth-first-search to generate all $r \times 16$ matrices step-by-step for each $r \in \{9, \ldots, 16\}$. The reader is invited to compare the size of the search trees involved with the BH$(16, 2)$ case displayed in Table 3 and with the BH$(14, 4)$ case displayed in Table 1.

The search, which relied on only the standard C++ libraries and 448 computing cores, took about 30 CPU years, and yielded the following classification result.

Theorem 4.4. *The number of* BH$(16, 4)$ *matrices is* 1786763 *up to monomial equivalence.*

In Table 4 the automorphism group sizes along with their frequencies is exhibited.

Corollary 4.5. *The total number of* BH$(16, 4)$ *matrices* (*not considering equivalence*) *is exactly* $188203175684505523864602703152281912650676305920000 0 \approx 1.882 \cdot 10^{51}$.

Proof. Let $\mathcal{H}$ be a complete set of representatives of BH$(16,4)$ matrices up to monomial equivalence. Then the size of the set BH$(16,4)$ can be inferred from an application of the Orbit-stabilizer theorem [24, Theorem 3.20]. We have $|\mathrm{BH}(16,4)| = |G|\sum_{H\in\mathcal{H}} 1/|\mathrm{Aut}(H)|$. Combining $|G| = (16!)^2 \times 4^{32}$ with the numbers shown in Table 4 yields the result. □

There are two main reasons for the existence of such a huge number of equivalence classes. First, Kronecker-like constructions can lift up the BH$(8,4)$ matrices resulting in multi-parametric families of complex Hadamard matrices [11], [51]. The second reason is the presence of type-0 (that is: real) pair of rows. It is known that such a substructure can be "switched" [40] in a continuous way [50] thus escaping the monomial equivalence class of the matrices is possible. In contrast, matrices which cannot lead to continuous parametric families of complex Hadamard matrices are called isolated [51]. A concept to bound the number of free parameters which can be introduced into a given matrix is the defect [51]. We remark that when $q \in \{2,3,4,6\}$ then computing the defect boils down to a rank computation of integer matrices which can be performed efficiently using exact integer arithmetic.

Corollary 4.6. *There are at least* 7978 *isolated* BH$(16,4)$ *matrices.*

Proof. This is established by counting the number of BH$(16,4)$ matrices with defect 0. There are no isolated BH$(16,4)$ matrices of type 0, because they contain a real pair of rows as a substructure. It is easy to see that such matrices cannot be isolated once the size of the matrices $n > 2$, see [50]. Computation reveals that there are no type-k matrices with vanishing defect for $k \in \{1,3,4\}$, and there are exactly 7978 type-2 matrices with defect 0. Since the defect is an upper bound on the number of smooth parameters which can be introduced [51], these matrices are isolated. □

Finally, we note a result connecting BH$(2n,4)$ matrices with unreal BH$(n,6)$ matrices.

Theorem 4.7. *Let $n \geq 1$, and let A and B be $n \times n$ $\{-1,0,1\}$-matrices such that $A_{i,j}B_{i,j} = 0$ for $i,j \in \{1,\ldots,n\}$, and $\zeta_3 A + \zeta_3^2 B \in$ BH$(n,6)$. Then $H := A \otimes \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right] + B \otimes \left[\begin{smallmatrix} \zeta_4 & -1 \\ -1 & \zeta_4 \end{smallmatrix}\right] \in$ BH$(2n,4)$.*

Proof. Let $X := \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$ and $Y := \left[\begin{smallmatrix} \zeta_4 & -1 \\ -1 & \zeta_4 \end{smallmatrix}\right]$. We have $XX^* = YY^* = -(XY^* + YX^*) = 2I_2$. Since $(\zeta_3 A + \zeta_3^2 B)(\zeta_3^2 A^T + \zeta_3 B^T) = nI_n$, we have $AB^T = BA^T$. Every entry of H is some 4th root of unity, and $HH^* = (AA^T + BB^T) \otimes (2I_2) + AB^T \otimes (XY^* + YX^*) = 2nI_{2n}$. □

The significance of this observation is that it implies the following recent result.

Corollary 4.8 ([8])**.** *Let $n \geq 1$ be an integer. If there exists a* BH$(n,6)$ *matrix with no ± 1 entries, then there exists a* BH$(4n,2)$.

Proof. Combine Theorem 4.2 with Theorem 4.7. □

4.3. **Classification of BH(21,3) matrices.** In this section we briefly report on our computational results regarding the BH$(21,3)$ matrices. The classification of BH$(18,3)$ matrices was reported earlier in [17] and independently in [33], while several examples of BH$(21,3)$ matrices were reported in [2].

The major difference between this case and the case of BH$(16,4)$ matrices discussed in Section 4.2 is that due to the lack of building blocks (such as a BH$(7,3)$)

TABLE 5. The automorphism group sizes of BH(21, 3) matrices.

|Aut|	#	|Aut|	#	|Aut|	#	|Aut|	#	|Aut|	#
1008	2	504	4	54	8	36	10	18	12
720	2	72	8	48	6	24	12	12	8

for Kronecker-like constructions here one does not expect many solutions to be found, and therefore one may try to approach this problem by employing slightly different techniques. In what follows we describe a general method based on clique search which can be combined with the framework of orderly generation.

Let n, $q \geq 2$. The first step is to classify all $r \times n$ orderly-generated rectangular orthogonal qth root matrices with the second column pruning technique as described earlier for small r. In the second step we consider each of these $r \times n$ starting-point matrices, say R, one-by-one, and generate a set V containing those row vectors which are simultaneously (i) normalized; (ii) lexicographically larger than the rth row of R; and (iii) orthogonal to each r rows of R. Then, following ideas used in [46], we create the compatibility graph $\Gamma(R)$ on $|V|$ vertices, where two vertices, say x and y, indexed by elements of V, are adjacent if and only if the row vectors $x \in V$ and $y \in V$ are pairwise orthogonal. With this terminology the task is then to decide if $\Gamma(R)$ contains a clique of size $n-r$. If there is no such a clique, then the starting-point matrix R should be rejected. Otherwise for all cliques found the matrix R should be augmented with $n - r$ new rows prescribed by the clique arranged in lexicographically increasing order, and then should be tested for canonicity.

The value of the parameter r greatly affects the size of $|V|$, and therefore should be chosen carefully. This method works best when there are no cliques of size $n-r$ because then the starting-point matrix R can be rejected during early stages of the search. The Cliquer software [39], based on [41], was used in the current work to prune inextendible matrices in this way.

Theorem 4.9. *The number of* BH(21, 3) *matrices is* 72 *up to monomial equivalence.*

Proof. The first step is to classify all $r \times 21$ orderly-generated rectangular orthogonal 3rd root matrices with the second column pruning technique: there are exactly 1, 1, 12, 145, and 74013 such matrices up to monomial equivalence for $r \in \{1, 2, \ldots, 5\}$. The second step is to consider each of these 5×21 starting-point matrices, say R, one-by-one, and create the compatibility graph $\Gamma(R)$. The task is then to decide if $\Gamma(R)$ contains a clique of size 16. It turns out that in most cases it does not, and therefore we can reject most of the starting-point matrices. In total, 72 matrices were found. □

In Table 5 we display the automorphism group sizes of the BH(21, 3) matrices along with their frequencies.

It was estimated that around 500 CPU years is required to solve this case with the methods of [17]. However, we have completed this task in just over 18 CPU days.

4.4. **Nonexistence results.** In this section we report on several exhaustive computational searches which proves the nonexistence of Butson matrices with certain parameters. To the best of our knowledge Theorem 4.11 and Theorem 4.13 presented below are new results. Nonexistence results for Butson matrices were obtained earlier in [3], [5], [10], [30], [32], and in [54]. We recall the following result for reference.

TABLE 6. The nonexistence of $\mathrm{BH}(11, q)$ matrices for various q.

r	$\mathrm{BH}(11,6)$	$\mathrm{BH}(11,10)$	$\mathrm{BH}(11,12)$	$\mathrm{BH}(11,14)$	$\mathrm{BH}(11,15)$
1	1	1	1	1	1
2	5	5	32	4	3
3	499	0	168564	2091	584
4	33655		7950174	2572	94
5	42851		561071	14	22
6	171		578	0	0
7	0		0		

Theorem 4.10 ([5, Theorem 4.2])**.** *Let $H \in \mathrm{BH}(n, q)$ with n odd. Then the square-free part of n can have no prime factors p of even order f modulo q, such that $p^{f/2} \equiv -1 \pmod{q}$.*

In particular, by Theorem 4.10 matrices $\mathrm{BH}(13, 10)$ and $\mathrm{BH}(17, 10)$ do not exist.

Next we report on our computational nonexistence results. All of these computations were done in two different ways. First, we established nonexistence by using Cliquer, which heavily pruned the search tree, that is, reduced the number of cases to be considered. This was very efficient due to the lack of complete matrices. Once nonexistence was established, we verified it during a second run, but this time without relying on Cliquer. This was done in order to be able to prudently document the search, and to avoid the use of external libraries.

Theorem 4.11. *There does not exist a $\mathrm{BH}(8, 15)$ matrix.*

Proof. The proof is computational. We have generated the $r \times 8$ orthogonal matrices with 15th root of unity entries with the orderly algorithm using the second column pruning strategy, and we found 1, 1, 6, and 0 such matrices for $r \in \{1, 2, 3, 4\}$, respectively. Therefore there exist no $\mathrm{BH}(8, 15)$ matrices. □

The next result was obtained independently, but slightly earlier in [30] with similar computational methods. In addition, the nonexistence of $\mathrm{BH}(11, 20)$ matrices is claimed in [30].

Theorem 4.12 ([30, Section 3.3])**.** *There does not exist a $\mathrm{BH}(11, q)$ matrix for $q \in \{10, 14, 15\}$.*

Proof. The proof is computational, and goes along the lines of the Proof of Theorem 4.11. Refer to Table 6 for the number of orderly-generated, rectangular orthogonal $r \times 11$ matrices with qth roots of unity (where $q \in \{10, 14, 15\}$) surviving the second column pruning strategy. In each of the four cases no such matrices were found for some $r \in \{1, \ldots, 11\}$, hence $\mathrm{BH}(11, q)$ matrices do not exist. For comparison, the cases $\mathrm{BH}(11, 6)$ and $\mathrm{BH}(11, 12)$ are also presented. □

Theorem 4.13. *There does not exist a $\mathrm{BH}(13, 15)$ matrix.*

Proof. The proof is computational, and goes along the lines of the Proof of Theorem 4.11. We have generated the $r \times 13$ orthogonal matrices with 15th root of unity entries with the orderly algorithm using the second column pruning strategy, and we found 1, 2, 2280, 1014, and 0 such matrices for $r \in \{1, \ldots, 5\}$, respectively. Therefore there exist no $\mathrm{BH}(13, 15)$ matrices. □

5. Verification of the results

In this section we discuss several techniques to perform a consistency check of the computations. Let $n, q \geq 2$ be integers, and assume that we are given a

TABLE 7. The number of $\mathrm{BH}(n,q)$ matrices up to Hadamard equivalence.

$n \setminus q$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
2	1		1		1		1		1		1		1		1	
3		1			1			1			1			1		
4	1		2		2		3		2		4		2		4	
5				1	0				1		0			1		
6	0	1	1		4		3	1	0		10		0	1	4	
7					1	1			0		2		1			
8	1		15		35		134		136		629		366	0	1224	
9		2			10			10	1		33		0	22		
10	0		8	1	33		43		29		448		0	1	124	
11					0				0	1	0		0	0		
12	1	1	309		5758		28361	4	76085		1832602		E	E	E	
13					218				0		E	1	0	0		
14	0		520		92325	2	E		E		E		E	U	E	
15		0		0	0			0	0		U		0	E		
16	5		1111624		E		E		E		E		E	U	E	
17					0				0		U		0	U		1
18	0	53	E		E		E	E	E		E		U	E	E	
19					E				0		E		0	U		
20	3		E	E	E		E		E		E		E	E	E	
21		36			E	0		E	0		E		0	E		

set $\mathcal{H}$ containing a complete set of representatives of the $\mathrm{BH}(n,q)$ matrices up to monomial equivalence. If the computations are correct, then $\mathcal{H}$ should satisfy certain counting formulae.

Recall, that several authors (see e.g. [22, Definition 4.12], [36]) consider two $\mathrm{BH}(n,q)$ matrices Hadamard equivalent if either can be obtained from the other by (i) performing a finite sequence of monomial equivalence preserving operations; and (ii) by replacing every entry by its image under a fixed automorphism of $\mathbb{Z}_q$. For $H \in \mathcal{H}$, let $\Psi(H) := \{\psi(H) \colon \psi \in \mathrm{Aut}(\mathbb{Z}_q)\}$, and let $c(\Psi(H))$ denote the number of $\mathrm{BH}(n,q)$ matrices in the set $\Psi(H)$ up to monomial equivalence. The next result shows how to enumerate the number of $\mathrm{BH}(n,q)$ matrices up to Hadamard equivalence. We denote this reduced set by $\mathrm{BH}(n,q)^\dagger$.

Lemma 5.1. *Let $n, q \geq 2$ and let $\mathcal{H}$ be a complete set of representatives of the $\mathrm{BH}(n,q)$ matrices up to monomial equivalence. Then $|\mathrm{BH}(n,q)^\dagger| = \sum_{H\in\mathcal{H}}(1/c(\Psi(H)))$.*

Proof. Observe that the Hadamard equivalence classes are formed by the union of certain monomial equivalence classes. Within a Hadamard equivalence class, represented by $H \in \mathcal{H}$, the monomial-inequivalent matrices are necessarily Hadamard equivalent to H via a group automorphism. Their number is exactly $c(\Psi(H))$. □

Corollary 5.2. *Let $n, q \geq 2$ and let $\mathcal{H}$ be a complete set of representatives of the $\mathrm{BH}(n,q)$ matrices up to monomial equivalence. Then $|\mathrm{BH}(n,q)^\dagger| = \sum_{i=1}^{\varphi(q)}(k_i/i)$, where k_i denotes the frequency distribution of the number i occurring as the value of $c(\Psi(H))$ while it runs through all $H \in \mathcal{H}$. In particular, $k_i \equiv 0 \pmod{i}$ for every $i \in \{2, \ldots, \varphi(q)\}$, and $|\mathcal{H}| = \sum_{i=1}^{\varphi(q)} k_i$.*

Proof. Split the sum in Lemma 5.1 as follows: $|\mathrm{BH}(n,q)^\dagger| = \sum_{i=1}^{\varphi(q)} \sum_{\substack{H\in\mathcal{H} \\ c(\Psi(H))=i}} (1/i)$. □

In Table 7 (cf. Table 2) we present the number of $\mathrm{BH}(n,q)$ matrices up to Hadamard equivalence.

Corollary 5.2 provides some validation of the classification, but the check it describes is not always strong (e.g., if $q = 4$, $\varphi(q) = 2$ and there is a high probability that an erroneous count will pass the check). For a more rigorous test, one should therefore more specifically make sure that for all $H \in \mathcal{H}$, every element of the set $\Psi(H)$ is monomial equivalent to some matrix in $\mathcal{H}$.

Remark 5.3. The transpose of a Butson matrix is a Butson matrix. This transformation can be also used for validation purposes. A weak check is that the number of matrices that are not monomial equivalent to their transpose should be even, and a stronger check is that for each $H \in \mathcal{H}$, H^T should be monomial equivalent to some matrix in $\mathcal{H}$.

6. Open problems

We conclude the paper with the following problems.

Problem 6.1. Extend Table 2 further by classifying some of the remaining cases of $\mathrm{BH}(n, q)$ matrices in the range $n \leq 21$ and $q \leq 17$, and possibly beyond.

Some results regarding the classification of real Hadamard matrices of order 36 can be found in [4], [40].

Problem 6.2 (cf. [4, Conjecture 1])**.** Classify all $\mathrm{BH}(36, 2)$ matrices. Is it true that every $H \in \mathrm{BH}(36, 2)$ has an equivalent form with constant row sum?

For the context regarding Problem 6.3 we refer the reader to [29].

Problem 6.3 (Spectral set conjecture in $\mathbb{R}^2$)**.** Let n and q be positive integers, such that $n \nmid q^2$. Are there rectangular matrices A and B with elements in $\mathbb{Z}_q$ of size $n \times 2$ and $2 \times n$, respectively, such that $AB \equiv L(H) \pmod{q}$ for some $H \in \mathrm{BH}(n, q)$?

For the context regarding Problem 6.4 we refer the reader to [32] (see also Remark 3.5).

Problem 6.4 (cf. [3, Conjecture 7.6])**.** Let $n, q \geq 2$, let $H \in \mathrm{BH}(n, q)$, and let $r_1, r_2 \in \mathbb{Z}_q^n$ be distinct rows of $L(H)$. Can $r_1 - r_2 \in \mathbb{Z}_q^n$ represent an "asymmetric" minimal n-term vanishing sum of qth roots of unity? In other words, is it possible that $\mathrm{Sort}(r_1 - r_2)$ is minimal in the sense that it has no constituent of m-term vanishing subsums for $m < n$, yet it is not of the form $[0, 1, \ldots, p-1] \in \mathbb{Z}_q^n$ where p is some prime divisor of q?

Several $\mathrm{BH}(n, q)$ matrices with large n and q were constructed in [42], leading to infinite, parametric families of complex Hadamard matrices of prime orders for $n \equiv 1 \pmod{6}$.

Problem 6.5 (cf. [30, Conjecture 3.3.1])**.** Find new examples of $\mathrm{BH}(n, q)$ matrices of prime orders $n \equiv 5 \pmod{6}$.

Problem 6.6 asks if a non-Desarguesian projective plane of prime order p exists [21].

Problem 6.6 (cf. [20])**.** Let p be a prime number. Decide the uniqueness of $F_p \in \mathrm{BH}(p, p)$.

The next problem asks for the classification of qth root mutually unbiased bases [23].

Problem 6.7. Let $n, q \geq 2$, and let $H, K \in \mathrm{BH}(n, q)$. Classify all pairs (H, K) for which $(HK^*)/\sqrt{n} \in \mathrm{BH}(n, q)$.

Acknowledgements

We are grateful to Bernhard Schmidt for pointing out [5, Theorem 4.2], and we thank Wojciech Bruzda for communicating to us reference [30].

References

1. S.S. Agaian: Hadamard matrices and their applications, Springer-Verlag Berlin (1980)
2. K. Akiyama, M. Ogawa, C. Suetake: On $\mathrm{STD}_6[18,3]$'s and $\mathrm{STD}_7[21,3]$'s admitting a semiregular automorphism group of order 9, *Electron. J. Combin.*, **16**, #R148 21 pp. (2009)
3. T. Banica, J. Bichon, J.-M. Schlenker: Representation of quantum permutation algebras, *J. Funct. Anal.*, **257**, 2864–2910 (2009)
4. I. Bouyukliev, V. Fack, J. Winne: 2-$(31,15,7)$, 2-$(35,17,8)$ and 2-$(36,15,6)$ designs with automorphisms of odd prime order, and their related Hadamard matrices and codes, *Des. Codes Cryptogr.*, **51**, 105–122 (2009)
5. B.W. Brock: Hermitian congruence and the existence and completion of generalized Hadamard matrices, *J. Combin. Theory Ser. A*, **49**, 233–261 (1988)
6. W. Bruzda, W. Tadej, K. Życzkowski: Web page for complex Hadamard matrices, `http://chaos.if.uj.edu.pl/~karol/hadamard/`
7. A.T. Butson: Generalized Hadamard matrices, *Proc. Amer. Math. Soc.*, **13**, 894–898 (1962)
8. B. Compton, R. Craigen, W. de Launey: Unreal $\mathrm{BH}(n,6)$'s and Hadamard matrices, *Des. Codes Cryptogr.*, **79**, 219–229 (2016)
9. R. Craigen, W. Holzmann, H. Kharaghani: Complex Golay sequences: structure and applications, *Discrete Math.*, **252**, 73–89 (2002)
10. W. de Launey: On the non-existence of generalised Hadamard matrices, *J. Statist. Plann. Inference*, **10**, 385–396 (1984)
11. P. Diţă: Some results on the parametrization of complex Hadamard matrices, *J. Phys. A: Math. Gen.*, **37**, 5355 (2004)
12. D.Ž. Đoković: Good matrices of orders 33, 35 and 127, *J. Combin. Math. Combin. Comput.*, **14**, 145–152 (1993)
13. R. Egan, D. Flannery, P. Ó Catháin: Classifying cocyclic Butson Hadamard matrices. In: Colbourn C. (eds) Algebraic Design Theory and Hadamard Matrices. Springer Proceedings in Mathematics & Statistics, **133**, 93–106 (2015)
14. I.A. Faradžev: Constructive enumeration of combinatorial objects, *Colloq. Inter. CNRS* **260** 131–135 (1978)
15. P.B. Gibbons, R. Mathon: Enumeration of Generalized Hadamard Matrices of Order 16 and Related Designs, *J. Combin. Des.*, **17**, 119–135 (2009)
16. U. Haagerup: Orthogonal maximal abelian $*$-subalgebras of the $n \times n$ matrices and cyclic n-roots, in: S. Doplicher (Ed.), et al., Operator Algebras and Quantum Field Theory, International Press, 296–322 (1997)
17. 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, *Electron. J. Combin.*, **17**, #R171 (2010)
18. M. Harada, C. Lam, V.D. Tonchev: Symmetric (4,4)-nets and generalized Hadamard matrices over groups of order 4, *Des. Codes Crpytogr.*, **34**, 71–87 (2005)
19. A.S. Hedayat, N.J.A. Sloane, J. Stufken: Orthogonal Arrays, Springer (1999)
20. G. Hiranandani, J.-M. Schlenker: Small circulant complex Hadamard matrices of Butson type, *European. J. Combin.*, **51**, 306–314 (2016)
21. M. Hirasaka, K.-T. Kim, Y. Mizoguchi: Uniqueness of Butson Hadamard matrices of small degrees, *J. Discrete Algorithms*, **34**, 70–77 (2015)
22. K. Horadam: Hadamard Matrices and Their Applications, Princeton University Press (2006)
23. B. Karlsson: BCCB complex Hadamard matrices of order 9, and MUBs, *Linear Algebra Appl.*, **504**, 309–324 (2016)
24. P. Kaski, P.R.J. Östergård: Classification Algorithms for Codes and Designs, Springer Berlin, (2006)
25. H. Kharaghani, B. Tayfeh-Rezaie: Hadamard matrices of order 32, *J. Combin. Des.*, **21**, 212–221 (2013)

26. H. Kharaghani, B. Tayfeh-Rezaie: On the classification of Hadamard matrices of order 32, *J. Combin. Des.*, **18**, 328–336 (2010)
27. H. Kimura: Classification of Hadamard matrices of order 28, *Discrete Math.*, **133**, 171–180 (1994)
28. D.E. Knuth: The Art of Computer Programming: Generating All Tuples and Permutations, **4**:2, Addison–Wesley, (2010)
29. M.N. Kolountzakis, M. Matolcsi: Complex Hadamard matrices and the spectral set conjecture, *Collect. Math.*, Vol. Extra. 281–291 (2006)
30. A.J. LaClair: A Survey on Hadamard Matrices, Honors Thesis, University of Tennessee (2016)
31. C. Lam, S. Lam, V. Tonchev: Bounds on the number of affine, symmetric, and Hadamard designs and matrices, *J. Combin. Theory Ser. A*, **92**, 186–196 (2000)
32. T.Y. Lam, K.H. Leung: On vanishing sums of roots of unity, *J. Algebra*, **224**, 91–109 (2000)
33. P.H.J. Lampio: Classification of difference matrices and complex Hadamard matrices, PhD Thesis, Aalto University, (2015)
34. P.H.J. Lampio, P.R.J. Östergård: Classification of difference matrices over cyclic groups, *J. Stat. Plan. Inference*, **141**, 1194–1207 (2011)
35. P.H.J. Lampio, P.R.J. Östergård, F. Szöllősi: Dataset for Orderly Generation of Butson Hadamard Matrices [Dataset]. Zenodo. `http://doi.org/10.5281/zenodo.2585765` (2019)
36. P.H.J. Lampio, F. Szöllősi, P.R.J. Östergård: The quaternary complex Hadamard matrices of order 10, 12, and 14, *Discrete Math.*, **313**, 189–206 (2013)
37. D. McNulty, S. Weigert: Isolated Hadamard matrices from mutually unbiased product bases, *J. Math. Phys.*, **53**, 122202 (2012)
38. R. Nicoară: Subfactors and Hadamard matrices, *J. Operator Theory*, **64**, 453–468 (2010)
39. S. Niskanen, P.R.J. Östergård: Cliquer user's guide, version 1.0, *Technical Report T48*, Communications Laboratory, Helsinki University of Technology, Espoo, (2003)
40. W.P. Orrick: Switching operations for Hadamard matrices, *SIAM J. Discrete Math.*, **22**, 31–50 (2008)
41. P.R.J. Östergård: A fast algorithm for the maximum clique problem, *Discrete Appl. Math.*, **120**, 197–207 (2002)
42. M. Petrescu: Existence of continuous families of complex Hadamard matrices of prime dimensions, *PhD Thesis*, University of California, Los Angeles (1997)
43. R.C. Read: Every one a winner, or how to avoid isomorphism search when cataloguing combinatorial configurations, *Ann. Discrete Math.*, **2**, 107–120 (1978)
44. J. Seberry: A construction for generalized Hadamard matrices, *J. Statist. Plann. Inference*, **4**, 365–368 (1980)
45. J. Seberry: Complex Hadamard matrices, *Linear Multilinear Algebra*, **1**, 257–272 (1973)
46. E. Spence: Classification of Hadamard matrices of order 24 and 28, *Discrete Math.*, **140**, 185–243 (1995)
47. F. Szöllősi: A note on the existence of BH$(19, 6)$ matrices, *Australas. J. Combin.*, **55**, 31–34 (2013)
48. F. Szöllősi: Mutually Unbiased Bases, Gauss sums, and the asymptotic existence of Butson Hadamard matrices, *RIMS Kokyuroku*, **1872**, 39–48 (2014)
49. F. Szöllősi: On quaternary complex Hadamard matrices of small orders, *Adv. Math. Commun.*, **5**, 309–315 (2011)
50. F. Szöllősi: Parametrizing complex Hadamard matrices, *European J. Combin.*, **29**, 1219–1234 (2008)
51. W. Tadej, K. Życzkowski: A concise guide to complex Hadamard matrices, *Open Syst. Inf. Dyn.*, **13**, 133–177 (2006)
52. R.J. Turyn: Complex Hadamard matrices. In: R. Guy (Ed.), Combinatorial Structures and their Applications, Gordon and Breach, New York, 435–437, (1970)
53. R.F. Werner: All teleportation and dense coding schemes, *J. Phys. A: Math. Gen.*, **34**, 7081–7094 (2001)
54. A. Winterhof: On the non-existence of generalized Hadamard matrices, *J. Statist. Plann. Inference*, **84**, 337–342 (2000)

P.H.J. L., P.R.J. Ö., and F. Sz.: Department of Communications and Networking, Aalto University School of Electrical Engineering, P.O. Box 15400, 00076 Aalto, Finland

E-mail address: pekka.lampio@aalto.fi, patric.ostergard@aalto.fi, szoferi@gmail.com