ON QUATERNARY COMPLEX HADAMARD MATRICES OF SMALL ORDERS

FERENC SZÖLLÖSI

Abstract. One of the main goals of design theory is to classify, characterize and count various combinatorial objects with some prescribed properties. In most cases, however, one quickly encounters a combinatorial explosion and even if the complete enumeration of the objects is possible, there is no apparent way how to study them in details, store them efficiently, or generate a particular one rapidly. In this paper we propose a novel method to deal with these difficulties, and illustrate it by presenting the classification of quaternary complex Hadamard matrices up to order 8. The obtained matrices are members of only a handful of parametric families, and each inequivalent matrix, up to transposition, can be identified through its fingerprint.

2010 Mathematics Subject Classification. Primary 05B20, secondary 46L10.
Keywords and phrases: Complex Hadamard matrix, Butson matrix, Fingerprint.

1. Introduction
A complex Hadamard matrix \(H\) of order \(n\) is an \(n \times n\) matrix with unimodular entries satisfying \(HH^* = nI\) where \(*\) is the conjugate transpose and \(I\) is the identity matrix of order \(n\). In other words, any two distinct rows (or columns) of \(H\) are complex orthogonal. Complex Hadamard matrices have important applications in quantum optics, high-energy physics \([1]\), operator theory \([16]\) and in harmonic analysis \([11]\), \([20]\). They also play a crucial rôle in quantum information theory, for construction of teleportation and dense coding schemes \([21]\), and they are strongly related to mutually unbiased bases (MUBs) \([8]\). In finite mathematics and in particular, in design and coding theory, the real Hadamard matrices and their discrete generalization, the \(n \times n\) Butson-type matrices \([3]\), composed of \(q\)-th roots of unity appear frequently. These matrices are the main algebraic objects behind the Fourier and Walsh–Hadamard Transforms and perfect quaternary sequences. They can also be utilized to obtain high performance quaternary error-correcting codes and low correlation \(Z_4\)-sequence families \([13]\), and shall be denoted through this paper by \(BH(q,n)\). The notations \(BH(2,n)\) and \(BH(4,n)\) correspond to the real and quaternary Hadamard matrices, respectively.

One of the main features of these \(BH(q,n)\) matrices is the large symmetry they have, which allows one to introduce some free parameters into them obtaining a continuous family of complex Hadamard matrices. This idea was used in a series of papers \([5]\), \([6]\), \([7]\), \([14]\), \([18]\), where new, previously unknown complex Hadamard matrices were constructed in this way. The parametrization of \(BH(q,n)\) matrices is in some sense the continuous analogue of the switching operation, a well-known technique in design theory, and allows one to escape equivalence classes and therefore collect many inequivalent matrices into a single parametric family.

Date: May, 2010., Preprint.
This work was supported by the Hungarian National Research Fund OTKA-K77748.
The aim of this paper is to illustrate how powerful these continuous families are by presenting the complete characterization of the $BH(4,n)$ matrices up to $n = 8$, and describing them in a compact and elegant form in terms of parametric families of complex Hadamard matrices. Interestingly, up to transposition, all equivalence classes can be identified through a recently introduced invariant, the fingerprint \cite{17}. Constructing these matrices and identifying a member from each equivalence class took only a few days of computer search, and we do not consider it a deep mathematical achievement. The main result of this paper, however, is the way we present the representatives of the equivalence classes, as with the aid of only a handful of parametric families of complex Hadamard matrices we can encode a lot of inequivalent $BH(4,n)$ matrices simultaneously. In principle, by introducing $m$ free affine parameters into a $BH(q,n)$ matrix one can obtain as many as $q^m$ inequivalent matrices of the same type, therefore describing an exponential number of equivalence classes through a single matrix. We believe that the concept of parametrization shall turn out to be a useful tool in discrete mathematics as well, and by utilizing this method one shall be able to obtain new lower bounds on the number of various combinatorial objects in the future.

In the following section we give a full characterization of quaternary complex Hadamard matrices of orders 1-8, and describe them as members of parametric families of complex Hadamard matrices. Throughout the paper we adopt the notation from \cite{19} for well-known families of Hadamard matrices, such as $F_8^{(5)}(a,b,c,d,e)$, etc.

2. List of quaternary complex Hadamard matrices of small orders

It is easily seen that quaternary complex Hadamard matrices of order $n$ can exist only if $n = 1$ or $n$ is even, and it is conjectured that this condition is sufficient \cite{13}. It is trivial to check that there is a unique complex Hadamard matrix of orders $n = 1, 2$, however, for composite orders starting from $n = 4$ one encounters infinite families already. It has been shown that all complex Hadamard matrices of order 4 are members of the following 1-parameter family, depending on the unimodular complex number $a$ given in \cite{4} as

$$H_4(a) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & a & -a \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -a & a \end{bmatrix}.$$

Note that all $2 \times 2$ blocks of $H_4(a)$ are complex Hadamard matrices. Matrices arising in this fashion are called Ditkă-type (cf. \cite{14}). Recall that Hadamard matrices $H$ and $K$ are equivalent, if there exists permutation matrices $P_1, P_2$ and unitary diagonal matrices $D_1, D_2$ such that $P_1 D_1 H D_2 P_2 = K$ holds. We denote this property by $H \sim K$. Clearly, one can consider matrices containing a full row and column of numbers 1 due to equivalence. Such matrices are called dephased. Let us remark here that the transpose of a Hadamard matrix $H^T$ is also Hadamard, but not necessarily equivalent to $H$.

It is not apparent at first, how many equivalence classes of $BH(4,4)$ matrices are contained in the family $H_4(a)$ for various values of $a$. To quickly check that matrices $H_4(1)$ and $H_4(i)$ are inequivalent, we can utilize Haagerup’s invariant $\Lambda(H)$, defined for complex Hadamard matrices $H$ of order $n$, which is the following set \cite{9}:

$$\Lambda(H) := \{h_{ij} \overline{h_{kl}} \overline{h_{il}} \overline{h_{kj}} : i,j,k,l = 1,2,\ldots,n\}.$$
We readily see that \( \Lambda(H_4(1)) \) and \( \Lambda(H_4(i)) \) are different, therefore these matrices are inequivalent. Also, by exchanging rows 2, 4 one can see that \( H(a) \sim H(-a) \) and hence \( H(1) \sim H(-1) \) and \( H(i) \sim H(-i) \). Clearly the Haagerup invariant corresponding to \( BH(q,n) \) matrices can contain the \( q \)-th roots of unity only.

Remark 2.1. It might happen that a complex Hadamard matrix \( H \) does not look like a \( BH(q,n) \) matrix, but is equivalent to one; however, \( BH(q,n) \) matrices can be quickly recognized. Indeed, after dephasing \( H \) all of its entries should be some \( q \)-th roots of unity, otherwise \( \Lambda(H) \) would contain an entry which is not a \( q \)-th root of unity showing that \( H \) cannot be equivalent to a \( BH(q,n) \) matrix at all. This implies that checking the number of inequivalent \( BH(q,n) \) matrices in dephased parametric families is a finite process.

The above remark and the paragraph just before it easily allow to show that there are precisely 2 inequivalent \( BH(4,4) \) matrices: \( H_4(1) \) and \( H_4(i) \), respectively.

An interesting 1-parameter family of complex Hadamard matrices of order 6 was discovered by Zauner [22] (and independently, but slightly later by Dit\u{a} [5]) who used the 2-circulant form of the following matrix

\[
D_6(c) = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & i & -ic & -i & ic \\
1 & i & -1 & ic & -i & -ic \\
1 & -ic & ic & -1 & i & -i \\
1 & -i & -i & i & -1 & i \\
1 & ic & -ic & -i & i & -1 \\
\end{bmatrix}
\]

as a seed matrix to exhibit an infinite family of MUB triplets in \( \mathbb{C}^6 \). A quick computer search amongst all possible \( BH(4,6) \) matrices confirms that despite the 1-parameter freedom we have here, there is only a single equivalence class of \( BH(4,6) \) matrices. One might wonder why the matrices \( D_6(1) \) and \( D_6(i) \) are equivalent. This is not trivial to realize, as one need to emphase one of the matrices to obtain the other one. This particular family of complex Hadamard matrices has been utilized in harmonic analysis as well. Considering the scaled logarithm of the \( BH(8,6) \) matrix \( D_6((1+i)/\sqrt{2}) \), one finds a \( 6 \times 6 \) integer matrix having rank 3 over \( \mathbb{Z}_8 \) leading to the disproval of Fuglede’s conjecture in dimension 3 [11].

Now we turn to the classification of \( BH(4,8) \) matrices. An exhaustive computer search revealed after a few days the following

**Proposition 2.2.** There are precisely 15 \( BH(4,8) \) matrices, up to equivalence; 5 of these matrices are equivalent to a symmetric one, while another 10 are inequivalent to their transpose.

Now, having all inequivalent \( BH(4,8) \) matrices at our disposal, our goal is to describe them as members of certain parametric families of complex Hadamard matrices of order 8. It turns out that all matrices found in Proposition [22] appear as members of 3 distinct well-known parametric families of complex Hadamard matrices that we will now present. For each of these families we will give the classes of quaternary Hadamard matrices among them.
The first infinite family we have here is the 5-parameter generalized Fourier family, stemming from the $8 \times 8$ Fourier matrix as the following:

$$F^{(5)}_8(a, b, c, d, e) = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & a & b & c & -1 & -a & -b & -c \\
1 & d & -1 & -d & 1 & d & -1 & -d \\
1 & e & -b & -ace & -1 & -e & b & ace \\
1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 \\
1 & -a & b & -c & -1 & a & b & c \\
1 & -d & -1 & d & 1 & -d & -1 & d \\
1 & -e & -b & ace & -1 & e & b & -ace 
\end{bmatrix}.$$  

We have chosen the nonstandard parametrization here to emphasize the fact that one can obtain $BH(4, 8)$ matrices stemming from the matrix above if and only if the values of $a, b, c, d$ and $e$ are fourth roots of unity (see Remark 2.1).

**Remark 2.3.** As $F^{(5)}_8(a, b, c, d, e)$ features two rows and columns with entries $\pm 1$ it is an infinite family of jacket matrices (cf. [12]). Note that $F^{(5)}_8(aw, bw^2, cw^3, dw^2, ew^3)$ where $w = e^{\frac{2\pi}{t}}$ is an eighth root of unity coincides with the matrix listed in [19], and hence is of Diţă-type. The matrix corresponding to $F^{(5)}_8(-1/t^2, i, -i/t^2, -i, -i/t^2)$ is equivalent to an infinite family of circulant matrices containing in particular Horadam’s matrix $K_d(1)$ (cf. [13] p. 88).

After evaluating the matrix $F^{(5)}_8(a, b, c, d, e)$ at the $4^8 = 1024$ possible quintuples, we obtained the following

**Proposition 2.4.** The family $F^{(5)}_8(a, b, c, d, e)$ contains 8 inequivalent $BH(4, 8)$ matrices: the symmetric matrices $F^{(5)}_8(1, 1, 1, 1, 1), F^{(5)}_8(1, i, i, i, i), F^{(5)}_8(i, 1, i, 1, i), F^{(5)}_8(1, 1, i, 1, i)$ and further the matrices $F^{(5)}_8(1, i, 1, 1, i), F^{(5)}_8(1, 1, i, i, i), i,$ and their transpose.

To prove that the matrices in Proposition 2.4 are indeed inequivalent, we need to recall a more powerful invariant than the Haagerup set. The fingerprint of a complex Hadamard matrix $H$ of order $n \geq 4$ was introduced in [17] and reads

$$\Phi(H) := \left\{ \{v_i(d), m_i(d)\} : i \in I(d) \right\} : d = 2, \ldots, \lfloor n/2 \rfloor,$$

where $I(d)$ is a finite index set counting the number of different moduli $v_i(d)$ taken by the $d \times d$ minors of $H$, the multiplicity of these values being denoted by $m_i(d)$, respectively. Note that $\Phi(H)$ is an ordered set. For instance, the fingerprint of the $8 \times 8$ real Hadamard matrix is given by $\Phi(F^{(5)}_8(1, 1, 1, 1)) = \left\{ \{(0, 336), (2, 448)\}, \{(0, 1344), (4, 1792)\}, \{(0, 1428), (8, 3136), (16, 336)\} \right\}$.

That is, for $d = 2$, 336 minors are 0 and 448 have modulus 2, etc. In theory, the fingerprint is a more sophisticated invariant than the Haagerup set, because instead of looking at the $2 \times 2$ minors only it takes into account the higher order minors as well, therefore capturing some of the global properties of complex Hadamard matrices. One of the limitations of the fingerprint is, however, that it cannot distinguish a matrix from its transpose.

Now with the aid of this invariant one readily verifies that the 15 matrices appearing in Proposition 2.1 correspond to 10 different fingerprints, that is each matrix can be identified, up to transposition, with its own. It is straightforward to check that the 8 matrices
appearing in Proposition 2.4 have 6 different fingerprints, and as the family $F_S^{(5)}(a, b, c, d, e)$ is self-cognate (cf. [19]), it follows that the transpose of the non-symmetric matrices are members of the family as well. Indeed, we have $\left(F_S^{(5)}(1, 1, 1, 1, 1)\right)^T = F_S^{(5)}(1, 1, i, 1, 1)$ and $\left(F_S^{(5)}(1, 1, i, i, i)\right)^T = F_S^{(5)}(1, i, 1, 1, i)$.

The list of the $BH(4, 8)$ matrices is not complete yet, as in [14] another family of $8 \times 8$ complex Hadamard matrices were obtained from tiling abelian groups:

$$S_S^{(4)}(a, b, c, d) = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & d & -d & -d & -1 & cd & -cd & d \\
1 & ad & bd & -bd & 1 & -1 & -1 & -ad \\
1 & a & -b & b & -1 & cd & -cd & -a \\
1 & -1 & -bd & bd & 1 & c & -c & -1 \\
1 & -d & b & -b & -1 & d & d & -d \\
1 & -ad & -1 & -1 & 1 & -c & c & ad \\
1 & -a & d & d & -1 & -d & -d & a
\end{bmatrix}.$$  

It was shown in [14] that the matrix $S_S^{(4)}(i, i, i, i, 1)$ is not of Dit\u01d\u0111-type, and hence a small neighborhood around it avoids the family $F_S^{(5)}(a, b, c, d, e)$ completely. The matrix corresponding to $S_S^{(4)}(1, 1, i, i, i)$ is equivalent to the “jacket conference matrix” $J_S$ [12]. By evaluating the matrix $S_S^{(4)}(a, b, c, d)$ at the fourth roots of unity we found the following

**Proposition 2.5.** The family $S_S^{(4)}(a, b, c, d)$ and its transpose contain 8 inequivalent $BH(4, 8)$ matrices: the real Hadamard matrix $S_S^{(4)}(1, 1, 1, 1)$ and the matrix $S_S^{(4)}(1, 1, i, i)$, which are equivalent to a symmetric matrix, and further the matrices $S_S^{(4)}(1, 1, 1, i)$, $S_S^{(4)}(1, i, 1, i)$, $S_S^{(4)}(1, 1, i, 1)$, and their transpose.

By analyzing the fingerprint of the obtained matrices, one can see that the following equivalences hold: $S_S^{(4)}(1, 1, 1, 1) \sim F_S^{(5)}(1, 1, 1, 1, 1)$ and $\left(S_S^{(4)}(1, 1, i, i)\right)^T \sim F_S^{(5)}(1, 1, 1, 1, i)$, and therefore a further family is required to describe all of the 15 $BH(4, 8)$ matrices.

The following matrix was constructed from MUBs of order 4 by Dit\u01d\u0111 [7] very recently:

$$D_{SB}^{(5)}(a, b, c, d, e) = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & a & -a & d & -d & -a & a \\
1 & b & b\overline{c}e & -d & d & -b\overline{c}e & -b \\
1 & c & -e & -1 & -1 & e & -c \\
1 & -c & e & -1 & -1 & -e & c \\
1 & -b & b\overline{c}e & -d & d & b\overline{c}e & b \\
1 & -a & a & d & -d & a & -a \\
1 & -1 & -1 & 1 & 1 & -1 & -1
\end{bmatrix}.$$  

We will see shortly that the family $D_{SB}^{(5)}(a, b, c, d, e)$ is essentially different from the families $F_S^{(5)}(a, b, c, d, e)$ and $S_S^{(4)}(a, b, c, d)$, as it accounts for most of the $BH(4, 8)$ matrices. We remark here that the family $\left(D_{SB}^{(5)}(a, b, c, 1, e)\right)^T$ is equivalent to the 3-parameter matrix $P_3$ reported in [2]. We have the following
Proposition 2.6. The family $D_{SB}^{(5)}(a, b, c, d, e)$ together with its transpose contain 11 inequivalent $BH(4, 8)$ matrices, namely the real Hadamard matrix $D_{SB}^{(5)}(1, 1, 1, 1, 1)$, $D_{SB}^{(5)}(1, 1, i, 1, 1)$ and the matrix $D_{SB}^{(5)}(1, i, i, 1, 1)$, which are equivalent to symmetric matrices, and the matrices $D_{SB}^{(5)}(1, 1, 1, 1, i)$, $D_{SB}^{(5)}(1, 1, 1, i, i)$, $D_{SB}^{(5)}(1, 1, i, i, 1)$, $D_{SB}^{(5)}(1, i, i, 1, i)$, and their transpose.

In particular, the matrix $D_{SB}^{(5)}(1, 1, 1, i, 1)$ is not a member of any of the families $F_{8}^{(5)}(a, b, c, d, e)$, $S_{8}^{(4)}(a, b, c, d)$ or $\left(S_{8}^{(4)}(a, b, c, d)\right)^T$. We are ready to state the main result concerning $BH(4, 8)$ matrices.

Theorem 2.7. There are precisely 15 inequivalent $BH(4, 8)$ matrices, which can be described through the parametric families $F_{8}^{(5)}(a, b, c, d, e)$, $S_{8}^{(4)}(a, b, c, d)$ and $D_{SB}^{(5)}(a, b, c, d, e)$. Five of these matrices are equivalent to a symmetric matrix, namely $F_{8}^{(5)}(1, 1, 1, 1, 1)$, $F_{8}^{(5)}(1, i, i, i, i)$, $F_{8}^{(5)}(1, i, i, 1, i)$, $F_{8}^{(5)}(1, 1, i, 1, i)$, and $S_{8}^{(4)}(1, 1, i, i)$. The other 10 matrices are given by $F_{8}^{(5)}(1, 1, 1, 1, i)$, $F_{8}^{(5)}(1, 1, i, 1, i)$, $S_{8}^{(4)}(1, 1, 1, i)$, $S_{8}^{(4)}(1, i, 1, i)$, $S_{8}^{(4)}(1, 1, i, i)$, and their transpose. These matrices, up to transposition, can be distinguished by their fingerprint.

Finally, we would like to point out that another well-known invariant of $BH(4, n)$ matrices, the Smith normal form (SNF, cf. [15]) can detect 6 equivalence classes only. In particular, the inequivalent matrices $F_{8}^{(5)}(1, i, i, i, i)$ and $S_{8}^{(4)}(1, 1, i, i)$ share a common SNF. This is not surprising, as this invariant does not take into account the distribution of the minors of complex Hadamard matrices.

3. Concluding Remarks

In this paper we have described all quaternary complex Hadamard matrices up to order 8. The number of equivalence classes for $n = 1, 2, 4, 6, 8$ read 1, 1, 2, 1, 15, respectively. By utilizing continuous parametric families we could present the inequivalent matrices in a compact and elegant form, which allows one to study, display, and store these matrices efficiently. We remark here that the classification of the $n \times n$ generalized Hadamard matrices over groups of order 4 has been completed up to $n = 16$ very recently [10], and we intend to continue this work and attempt to describe in a similar fashion the remaining $BH(4, n)$ matrices of size $n = 10, 12$ or even higher orders too in a forthcoming paper.

Acknowledgements

The author would like to thank the referees very much for their valuable comments and suggestions.

References

[1] G. Auberson, A. Martin and G. Mennessier, On the reconstruction of a unitary matrix from its moduli, Commun. Math. Phys., 140 (1991), 417–436.
[2] S. Bouguezel, M. O. Ahmed and M. N. S. Swami, A new class of reciprocal-orthogonal parametric transforms, IEEE Trans. Circuits and Syst. I, 56 (2009), 795–805.
[3] A. T. Butson, Generalized Hadamard matrices, Proc. Amer. Math. Soc., 13 (1962), 894–898.
[4] R. Craigen, Equivalence classes of inverse orthogonal and unit Hadamard matrices, Bull. Austral. Math. Soc., 44 (1991), 109–115.
[5] P. Dită, Some results on the parametrization of complex Hadamard matrices, J. Phys. A, 20 (2004), 5355–5374.
[6] P. Diţă, *Complex Hadamard matrices from Sylvester inverse orthogonal matrices*, Open Systems & Information Dynamics, 16 (19), 387–405. (See the errata at arXiv:0901.0982v2)

[7] P. Diţă, *Hadamard Matrices from mutually unbiased bases*, J. Math. Phys., 51, (2010)

[8] T. Durt, B.-H. Englert, I. Bengtsson and K. Życzkowski, *On mutually unbiased bases*, International Journal of Quantum Information, 8, (2010), 535–640.

[9] U. Haagerup, *Orthogonal maximal Abelian *-subalgebras of n × n matrices and cyclic n-roots*, Operator Algebras and Quantum Field Theory (Rome), MA International Press, (1996), 296–322.

[10] M. Harada, C. Lam and V. D. Tonchev, *Symmetric (4, 4)-nets and generalized Hadamard matrices over groups of order 4*, Designs, Codes and Cryptography, 34 (2005), 71–87.

[11] M. N. Kolountzakis and M. Matolcsi, *Complex Hadamard matrices and the spectral set conjecture*, Collectanea Mathematica, Vol. Extra (2006), 281–291.

[12] M. H. Lee and V. Vl. Vavrek, *Jacket conference matrices and Paley transformation*, Eleventh International Wokshop on Algebraic and Combinatorial Coding Theory, Pamaporovo, Bulgaria, (2008), 181–185.

[13] K. J. Horadam, “*Hadamard Matrices and Their Applications*”, Princeton University Press, Princeton 2007.

[14] M. Matolcsi, J. Réffy and F. Szőlősi, *Constructions of complex Hadamard matrices via tiling Abelian groups*, Open Systems & Information Dynamics, 14 (2007), 247–263.

[15] T. S. Michael, W. D. Wallis, *Skew-Hadamard Matrices and the Smith Normal Form*, Designs, Codes and Cryptography, 13 (1998), 173–176.

[16] S. Popa, *Orthogonal pairs of *-subalgebras in finite von Neumann algebras*, J. Operator Theory, 9 (1983), 253–268.

[17] F. Szőlősi, *Exotic complex Hadamard matrices and their equivalence*, Cryptography and Communications, 2 (2010), 187–198.

[18] F. Szőlősi, *Parametrizing complex Hadamard matrices*, European J. Combin., 29 (2008), 1219–1234.

[19] W. Tadej and K. Życzkowski, *A concise guide to complex Hadamard matrices*, Open Syst. Inf. Dyn., 13 (2006), 133–177.

[20] T. Tao, *Fuglede’s conjecture is false in 5 and higher dimensions*, Math Res. Letters, 11 (2004), 251–258.

[21] R. F. Werner, *All teleportation and dense coding schemes*, J. Phys. A, 34 (2001), 7081–7094.

[22] G. Zauner, “*Quantumdesigns: The foundations of a noncommmutative design theory*”, (German) [Quantumdesigns: Grundzüge einer nichtkommutativen Designtheorie], Ph.D thesis, Universität Wien, (available at http://www.mat.univie.ac.at/~neum/ms/zauner.pdf), 1999.

Department of Mathematics and its Applications, Central European University, H-1051, Nádor u. 9, Budapest, Hungary

E-mail address: szoferi@gmail.com