

A TWO-PARAMETER FAMILY OF COMPLEX HADAMARD MATRICES OF ORDER 6 INDUCED BY HYPOCYCLOIDS

FERENC SZÖLLŐSI

(Communicated by Marius Junge)

ABSTRACT. We construct a 2-parameter family of complex Hadamard matrices of order 6 by a natural block construction. We combine this family with an earlier result of Zauner to derive a 2-parameter family of *triplets of mutually unbiased bases* (MUBs) in \mathbb{C}^6 . This invalidates some numerical evidence given by Brierley and Weigert and sheds new light on the problem of determining the maximal number of MUBs in \mathbb{C}^6 .

1. INTRODUCTION

Complex Hadamard matrices were originally studied for their connection to von Neumann algebras and pairs of orthogonal maximal Abelian $*$ -subalgebras of the matrix algebra $M_n(\mathbb{C})$, as initiated by Popa [15]. A specific problem of interest was the construction of *circulant* complex Hadamard matrices in connection with the existence of bi-unimodular sequences. Results of Björck [3], de la Harpe and Jones [10], and Munemasa and Watatani [14] showed that non-classical bi-unimodular sequences exist for all prime order $p \geq 7$. For $p = 2, 3, 5$ only classical bi-unimodular sequences exist, the case $p = 5$ being settled by Haagerup [9].

In the past decade there has been renewed interest in complex Hadamard matrices after it was shown by Werner [21] that these matrices play an important rôle in several constructions in quantum-information theory. Protocols in quantum-cryptography also rely on the existence of Hadamard matrices (see e.g. [7]). To describe the state of the art, Tadej and Życzkowski compiled a catalogue [18] of all known complex Hadamard matrices up to order 16 and have been regularly updating it in an online version [19] with new results emerging in the literature (e.g. [1], [13]). Full characterisation of complex Hadamard matrices is available only up to order 5 in [9]. For order 6 such classification remains elusive despite recent efforts [1], [8], [13], [17]. Particular motivation to study the 6×6 case comes from the problem of determining the maximal number of mutually unbiased bases (MUBs) in \mathbb{C}^6 , a notorious open problem in quantum-information theory. Recall that two orthonormal bases $\{e_1, \dots, e_d\}$ and $\{f_1, \dots, f_d\}$ are mutually unbiased in \mathbb{C}^d if $|\langle e_i, f_j \rangle| = 1/\sqrt{d}$. It is well-known that the maximal number of pairwise mutually unbiased bases in \mathbb{C}^d is not greater than $d + 1$, and this upper bound is attained whenever d is a prime power (see e.g. [12], [23]). The first open case is

Received by the editors April 3, 2009.

2000 *Mathematics Subject Classification*. Primary 46L10; Secondary 05B20.

This work was supported by Hungarian National Research Fund OTKA-K77748.

dimension 6, and there has been considerable effort devoted to this case in the past few years, a recent survey being given in [2]. Numerical evidence [4], [6] suggests that the maximal number of MUBs in \mathbb{C}^6 is 3. However, the results of the present paper show that such numerical results might be misleading and must be interpreted with sufficient care. Nevertheless, we still believe that the maximal number of MUBs in \mathbb{C}^6 is indeed 3, and a discretization scheme introduced in [11] may achieve a rigorous proof of such a statement in the future.

This paper is organized as follows. In Section 2 we construct a *2-parameter family* of complex Hadamard matrices of order 6 by a natural block construction. In Section 3 we discuss connections between this new family and previously known families of complex Hadamard matrices. Finally, in Section 4 we recall a construction of Zauner [24] to prove the existence of a *2-parameter family of MUB-triplets* of order 6. This result is particularly interesting, as it invalidates some numerical evidence given recently in [5].

2. THE CONSTRUCTION

Recall that a *complex Hadamard matrix* is a square matrix with unimodular entries such that the rows (and therefore columns) are pairwise orthogonal.

We will consider complex unimodular matrices with highly symmetrical *block structure*. Such restriction made on the matrix implies that “almost all” orthogonality conditions will hold automatically. Consider the following $2m \times 2m$ matrix consisting of $m \times m$ blocks A, B and their adjoint A^*, B^* , respectively:

$$(2.1) \quad H = \begin{bmatrix} A & B \\ B^* & -A^* \end{bmatrix}.$$

For H to be a complex Hadamard matrix, we must exhibit unimodular matrices A, B satisfying the following conditions:

$$(2.2) \quad AA^* + BB^* = 2mI_m, \quad B^*B + A^*A = 2mI_m, \quad AB - BA = 0,$$

where I_m is the identity matrix of order m . If A and B are *circulant* matrices, they commute, and therefore the last equation holds automatically, while the first two are equivalent. Hence, putting $m = 3$, the building blocks of H can be taken as

$$(2.3) \quad A = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}, \quad B = \begin{bmatrix} d & e & f \\ f & d & e \\ e & f & d \end{bmatrix}.$$

Recall that two complex Hadamard matrices, H and K , are called *equivalent* if there exists D_1, D_2 unitary diagonal and P, Q permutational matrices, such that $H = D_1PKQD_2$. It is well-known (and obvious) that each complex Hadamard matrix is equivalent to a dephased one (i.e. one with its first row and column consisting of 1's). With the notation (2.3) we have H and its dephased form X_6 as

follows:

$$(2.4) \quad H = \left[\begin{array}{ccc|ccc} a & b & c & d & e & f \\ c & a & b & f & d & e \\ b & c & a & e & f & d \\ \hline \frac{1}{d} & \frac{1}{f} & \frac{1}{e} & -\frac{1}{a} & -\frac{1}{c} & -\frac{1}{b} \\ \frac{1}{e} & \frac{1}{d} & \frac{1}{f} & -\frac{1}{b} & -\frac{1}{a} & -\frac{1}{c} \\ \frac{1}{f} & \frac{1}{e} & \frac{1}{d} & -\frac{1}{c} & -\frac{1}{b} & -\frac{1}{a} \end{array} \right], \quad X_6 = \left[\begin{array}{cccccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \frac{a^2}{bc} & \frac{ab}{c^2} & \frac{af}{cd} & \frac{ad}{ce} & \frac{ae}{cf} \\ 1 & \frac{ac}{b^2} & \frac{a^2}{bc} & \frac{ae}{bd} & \frac{af}{be} & \frac{ad}{bf} \\ 1 & \frac{ad}{bf} & \frac{ad}{ce} & -1 & -\frac{ad}{ce} & -\frac{ad}{bf} \\ 1 & \frac{ae}{bd} & \frac{ae}{cf} & -\frac{ae}{bd} & -1 & -\frac{ae}{cf} \\ 1 & \frac{af}{be} & \frac{af}{cd} & -\frac{af}{cd} & -\frac{af}{be} & -1 \end{array} \right].$$

As we have observed earlier it is necessary and sufficient for H to be a complex Hadamard matrix where the complex numbers a, b, c, d, e, f have modulus 1 and satisfy

$$(2.5) \quad \frac{a}{b} + \frac{b}{c} + \frac{c}{a} + \frac{d}{e} + \frac{e}{f} + \frac{f}{d} = 0.$$

Let us denote by $\varphi : \mathbb{T} \times \mathbb{T} \rightarrow \mathbb{C}$ the following fundamental function of ours:

$$(2.6) \quad \varphi[x, y] := x + y + \frac{1}{xy}.$$

Observe that we have $\varphi[\frac{a}{b}, \frac{b}{c}] = \frac{a}{b} + \frac{b}{c} + \frac{c}{a}$. Hence to satisfy (2.5) one should look for certain x, y, u and $v \in \mathbb{T}$, such that for some $\alpha \in \text{ran}\varphi$,

$$(2.7) \quad \varphi[x, y] = \alpha \quad \text{and} \quad \varphi[u, v] = -\alpha$$

hold simultaneously. It is straightforward to calculate that $\text{ran}\varphi$ is a so-called *deltoid* being bordered by the three-sided hypocycloid $\varphi[x, x] = 2x + \frac{1}{x^2}$ (see Figure 1). Let us introduce the notation $\mathbb{D} := \text{ran}\varphi \cap \text{ran}(-\varphi)$. It is clear that for any $\alpha \in \mathbb{D}$ one can define a complex Hadamard matrix in the following way: take any value of $\varphi^{-1}[\alpha]$, say (x, y) . Then define $a = 1, b = \bar{x}, c = \bar{x}y$. Similarly, take $\varphi^{-1}[-\alpha]$ to obtain the value (u, v) and define $d = 1, e = \bar{u}, f = \bar{u}v$. After substituting back to (2.4) we get

$$(2.8) \quad X_6(\alpha) \equiv X_6(x, y, u, v) = \left[\begin{array}{cccccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x^2y & xy^2 & \frac{xy}{uv} & uxy & vxy \\ 1 & \frac{x}{y} & x^2y & \frac{x}{u} & \frac{x}{v} & uvx \\ 1 & uvx & uxy & -1 & -uxy & -uvx \\ 1 & \frac{x}{u} & vxy & -\frac{x}{u} & -1 & -vxy \\ 1 & \frac{x}{v} & \frac{xy}{uv} & -\frac{xy}{uv} & -\frac{x}{v} & -1 \end{array} \right].$$

Next we describe an algebraic way of inverting φ ; i.e. how we can determine x, y and u, v from a given $\alpha \in \mathbb{D}$. The equation $\varphi[x, y] = \alpha$ and its conjugate read

$$(2.9) \quad x + y + \frac{1}{xy} = \alpha, \quad \frac{1}{x} + \frac{1}{y} + xy = \bar{\alpha}.$$

After multiplying the first equation by $x^2 \neq 0$ and the second by $x \neq 0$, one can eliminate the variable y to obtain the following *cubic* equation for x :

$$(2.10) \quad f_\alpha(x) := x^3 - \alpha x^2 + \bar{\alpha}x - 1 = 0.$$

By symmetry, this equation must hold for y as well. For $\alpha \in \text{int}\mathbb{D}$ the roots of (2.10) are distinct and of modulus 1. Let us denote them by r_1, r_2, r_3 . Hence, one can choose x as any of r_1, r_2, r_3 , and choose y as *any other* root. We therefore have 6 choices for the ordered pair (x, y) .

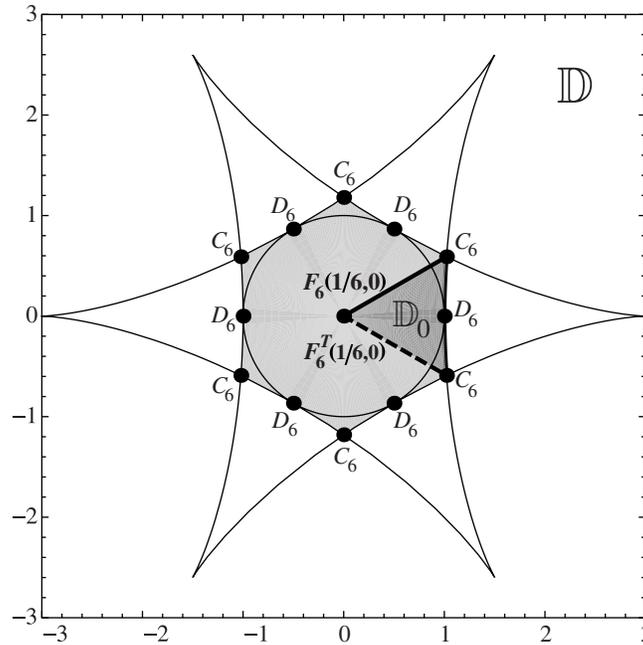


FIGURE 1. The intersection of the two deltoids \mathbb{D} consists of six equivalent sectors, one of which is the fundamental region \mathbb{D}_0 . The boundary of \mathbb{D} and the inscribed circle correspond to the families $B_6(y)$ and $D_6(c)$, respectively.

Finally, let us substitute $-\alpha$ into (2.10) and denote the roots by q_1, q_2, q_3 . The method to determine the values of u, v is completely analogous to what we have presented for x and y . As the arising equations are of degree three, x, y, u and v can be given explicitly in closed form. We spare the reader the details.

For $\alpha \in \text{int}\mathbb{D}$ we therefore have $6 \times 6 = 36$ choices for the ordered quadruple (x, y, u, v) . However, using the fact that $r_1 r_2 r_3 = 1$, we get an easy automatized calculation that shows that all of the emerging matrices $X_6(x, y, u, v)$ are equivalent to one of the two matrices $X_6(r_1, r_2, q_1, q_2)$ or $X_6^T(r_1, r_2, q_1, q_2)$ (note that a complex Hadamard matrix is generically not equivalent to its transpose).¹ On the boundary of \mathbb{D} , however, it is easy to show that $X_6(r_1, r_2, q_1, q_2)$ and $X_6^T(r_1, r_2, q_1, q_2)$ are equivalent and hence all choices of the quadruple (x, y, u, v) lead to equivalent matrices. Also, $X_6(r_1, r_2, q_1, q_2)$ is easily seen to be equivalent to its own conjugate, $\overline{X}_6(r_1, r_2, q_1, q_2)$, and hence $X_6^T(r_1, r_2, q_1, q_2)$ and $X_6^*(r_1, r_2, q_1, q_2)$ are equivalent as well.

We summarize the contents of this section in the following.

Theorem 2.1. *For $\alpha \in \mathbb{D}$ let $r_1(\alpha), r_2(\alpha), r_3(\alpha)$ denote the roots of equation (2.10), set as continuous functions of α . Similarly, substitute $-\alpha$ into (2.10) and denote the roots as $q_1(\alpha), q_2(\alpha), q_3(\alpha)$. Set $x = r_1(\alpha)$, $y = r_2(\alpha)$ and $u = q_1(\alpha)$, $v = q_2(\alpha)$. Then formula (2.8) and its transpose yield two 2-parameter families of complex*

¹We thank Ingemar Bengtsson for pointing out this fact.

Hadamard matrices of order 6, $X_6(x, y, u, v)$ and $X_6^T(x, y, u, v)$. Other choices of the roots $r_i(\alpha), q_j(\alpha)$ lead to equivalent matrices.

3. CONNECTIONS TO OTHER FAMILIES OF COMPLEX HADAMARD MATRICES

Throughout this section we use the standard notation of [19] for well-known families of complex Hadamard matrices, and we denote the standard basis of \mathbb{C}^6 by $e_i, i = 1, 2, \dots, 6$. We will analyze how our new family $X_6(\alpha)$ is related to previously discovered ones, such as $F_6(a, b)$, $D_6(c)$, and $B_6(y)$, respectively. In particular, we prove that both the Beauchamp–Nicoara family of self-adjoint complex Hadamard matrices $B_6(y)$ and Diță’s 1-parameter affine family $D_6(c)$ are contained in $X_6(\alpha)$. Thus our construction *unifies and extends* some of the previously discovered families.

We begin by noting that the region \mathbb{D} is being characterized algebraically by the discriminant function associated to equation (2.10),

$$(3.1) \quad D[\alpha] := |\alpha|^4 + 18|\alpha|^2 - 8\Re[\alpha^3] - 27,$$

and we have $\alpha \in \mathbb{D}$ if and only if $D[\alpha] \leq 0$ and $D[-\alpha] \leq 0$.

Next we discuss some internal equivalences within the family $X_6(\alpha)$, thus showing that it is possible to reduce \mathbb{D} to a smaller fundamental region. First, the transformation $\alpha \mapsto -\alpha$ establishes a trivial equivalence. Second, equation (2.10) is invariant under the substitutions $\alpha \mapsto \omega\alpha$ and $y \mapsto \omega y$, with $\omega = e^{2\pi i/3}$. The second transformation leaving the matrix $X_6(x, y, u, v)$ invariant establishes an equivalence between the matrices $X_6(\alpha)$ and $X_6(\omega\alpha)$. As a result, the region \mathbb{D} is found to consist of six equivalent sectors. We define the fundamental region $\mathbb{D}_0 := \{\alpha \in \mathbb{D} : -\pi/6 < \arg(\alpha) \leq \pi/6\}$.

Now we examine the extremal points of \mathbb{D}_0 . By equation (3.1) a straightforward computation shows the following: for $\alpha = 0$, $X_6(\alpha)$ and $X_6^T(\alpha)$ are equivalent to $F_6(1/6, 0)$ and $F_6^T(1/6, 0)$. The extremal point of \mathbb{D}_0 farthest from the origin can be obtained as $\alpha^{max} = \sqrt{-9 + 6\sqrt{3}}e^{2\pi i/12}$, and $X_6(\alpha^{max})$ is equivalent to Björck’s circulant matrix C_6 . The extremal point of \mathbb{D}_0 on the real axis is $\alpha^{min} = 1$, and $X_6(\alpha^{min})$ is equivalent to D_6 .

Let us next show that $X_6(\alpha)$ is indeed a *new* family; i.e. it is different from the only other known 2-parameter family of order 6, the generalized Fourier matrices $F_6(a, b)$. To see this, observe that $X_6(\alpha^{min})$ is equivalent to D_6 , which is not included in the families $F_6(a, b)$ or $F_6^T(a, b)$. Therefore, by continuity, in a small neighborhood \mathcal{U} of α^{min} the family $X_6(\alpha)$ is disjoint from $F_6(a, b)$ and $F_6^T(a, b)$. Within this neighborhood \mathcal{U} the possible intersections of $X_6(\alpha)$ and other known families such as $D_6(c)$, $B_6(y)$ or $M_6(x)$ can at most produce 1-parameter curves. This shows that the family $X_6(\alpha)$ is at least *locally* generically new, around $\alpha_0 = 1$. We conjecture that more is true: the family $X_6(\alpha)$ intersects the Fourier family only at $\alpha = 0$.

Next we show that the whole family $D_6(c)$ is included in our family $X_6(\alpha)$. In fact, this follows easily from an earlier result of Zauner [24].

Proposition 3.1 (cf. Ex. 5.7 from [24]). *With $c = t^3$ the family $D_6(c)$ (as given in [18]) is trivially permutation equivalent to the family with circulant blocks $D(t)$*

given below, which is thus included in the family $X_6(\alpha)$:

$$(3.2) \quad D(t) = \left[\begin{array}{ccc|ccc} 1 & \frac{i}{t} & it & 1 & \frac{1}{t} & -t \\ it & 1 & \frac{i}{t} & -t & 1 & \frac{1}{t} \\ \frac{i}{t} & it & 1 & \frac{1}{t} & -t & 1 \\ \hline 1 & -\frac{1}{t} & t & -1 & \frac{i}{t} & it \\ t & 1 & -\frac{1}{t} & it & -1 & \frac{i}{t} \\ -\frac{1}{t} & t & 1 & \frac{i}{t} & it & -1 \end{array} \right].$$

It is easy to show that $D(t)$ corresponds to $X_6(\alpha)$ with α being on the unit circle (see Figure 1).

Next we turn our attention to the family of self-adjoint complex Hadamard matrices $B_6(y)$ [1], [19] and show that this family is also contained in $X_6(\alpha)$.

Proposition 3.2. *Let B be a complex Hadamard matrix of the form*

$$(3.3) \quad B = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -\frac{1}{x} & -y & y & \frac{1}{x} \\ 1 & -x & 1 & y & \frac{1}{z} & -\frac{1}{xyz} \\ 1 & -\frac{1}{y} & \frac{1}{y} & -1 & -\frac{1}{xyz} & \frac{1}{xyz} \\ 1 & \frac{1}{y} & z & -xyz & 1 & -\frac{1}{x} \\ 1 & x & -xyz & xyz & -x & -1 \end{bmatrix}.$$

Define permutational matrices $P = [e_1, e_4, e_2, e_5, e_3, e_6]$, $Q = [e_5, e_1, e_3, e_4, e_6, e_2]$, and unitary diagonal matrices $D_1 = \text{Diag}(1, \sqrt[3]{z}, 1/\sqrt[3]{z}, 1/y, \sqrt[3]{z}, -1/(xy\sqrt[3]{z}))$, $D_2 = \text{Diag}(1, 1/\sqrt[3]{z}, 1/(\sqrt[3]{z})^2, 1, -xy(\sqrt[3]{z})^2, y\sqrt[3]{z})$, where $\sqrt[3]{z}$ denotes the principal cubic root of z . A straightforward calculation shows that D_1PBQD_2 is composed of circulant blocks and is therefore included in the family $X_6(\alpha)$. As the members of the family $B_6(y)$ are of the form (3.3), the family $B_6(y)$ is included in $X_6(\alpha)$.

It is easy to show that the family $B_6(y)$ corresponds to the boundary of \mathbb{D} (see Figure 1).

One might wonder whether the symmetric family $M_6(x)$ is included in $X_6(\alpha)$ as well. On the contrary: as the matrix M_6 and its conjugate $\overline{M_6}$ are inequivalent (see [13]), one can see that in a small neighborhood of M_6 the family $M_6(x)$ avoids $X_6(\alpha)$.

4. A TWO-PARAMETER FAMILY OF MUB-TRIPLETS IN \mathbb{C}^6

The maximal number of mutually unbiased bases (MUBs) in dimension 6 is not known. In general, the problem of MUBs seems to be deeply related to orthogonal Latin squares (see e.g. [16], [20], [22]). This would suggest that a complete system of 7 MUBs does not exist in \mathbb{C}^6 , a conjecture being supported further by numerical evidence [4], [6]. The maximal number of MUBs currently known in \mathbb{C}^6 is 3. Indeed, some isolated examples of MUB-triplets are presented in [2], while a 1-parameter infinite family of MUB-triplets is given explicitly in [11]. It also turned out that a scarcely known publication of Zauner [24] also contains a beautiful construction of another 1-parameter family of MUB-triplets. In the other direction, a discretization scheme followed by an exhaustive computer search [11] provided a rigorous proof that the standard basis and any member of the Fourier family $F(a, b)$ cannot be

extended to a MUB-quartet. Such a scheme could provide a rigorous full solution to the maximal number of MUBs in \mathbb{C}^6 in the future.

It turns out that the construction of Zauner [24] can be automatically combined with our family $X_6(\alpha)$, thus providing a new 2-parameter family of MUB-triplets in \mathbb{C}^6 . This is particularly interesting because a recent publication of Brierley and Weigert gave seemingly strong numerical evidence that members of the family $X_6(\alpha)$ cannot be part of MUB-triplets (although the authors very frankly admit that their result cannot be accepted as rigorous proof). This shows that such approximative numerical results might be misleading and in the same manner a MUB-quartet might be “hiding” somewhere. Therefore, the maximal number of MUBs in \mathbb{C}^6 must be considered wide open.

Let us recall the result of Zauner [24] relevant to us. A detailed exposition of this result in English is available in Appendix B of [11].

Proposition 4.1 (cf. Prop. 5.6 from [24]). *If T is a $2m \times 2m$ complex Hadamard matrix with $m \times m$ circulant blocks A, B, C, D , then there exist $2m \times 2m$ complex Hadamard matrices Z_1, Z_2 such that $T = \sqrt{2m}Z_1^{-1}Z_2$.*

Proposition 4.1 describes how to construct a triplet of MUBs from a given 2-circulant complex Hadamard matrix T . The assumption $T = \sqrt{2m}Z_1^{-1}Z_2$ implies that $\frac{1}{\sqrt{2m}}T = \frac{1}{2m}Z_1^*Z_2$, and hence $\{I_{2m}, \frac{1}{\sqrt{2m}}Z_1, \frac{1}{\sqrt{2m}}Z_2\}$ is a collection of 3 MUBs of order $2m$. Clearly, the members of our new family $X_6(\alpha)$ are suitable to take the rôle of T above. In summary, we have proved the following:

Theorem 4.2. *For each member of the family $X_6(\alpha)$ there exist complex Hadamard matrices $Z_1(\alpha), Z_2(\alpha)$ such that $\sqrt{6}X_6(\alpha) = Z_1^*(\alpha)Z_2(\alpha)$. In particular, there exists a 2-parameter family of MUB-triplets $(I_6, \frac{1}{\sqrt{6}}Z_1(\alpha), \frac{1}{\sqrt{6}}Z_2(\alpha))$ of order 6 emerging from the family $X_6(\alpha)$ via Zauner’s construction described in Proposition 4.1.*

Note that Proposition 4.1 allows the blocks to be different A, B, C, D , whereas the matrices $X_6(\alpha)$ contain blocks $A, B, B^*, -A^*$. Therefore Zauner’s construction may yield further results in the future.

We conclude our paper with the following observation: it is plausible that our new family $X_6(\alpha)$ intersects the Fourier families only at $\alpha = 0$. If one could exhibit similar families $X_6^{a,b}(\alpha)$ for all members $F(a, b)$ of the Fourier families, one would provide a rigorous proof of the existence of a 4-parameter family of complex Hadamard matrices of order 6. The existence of such a family is strongly indicated by the numerical results of [17]. This could possibly lead to a full classification of complex Hadamard matrices of order 6.

ACKNOWLEDGEMENTS

The author thanks Máté Matolcsi, Karol Życzkowski and Ingemar Bengtsson for various useful remarks concerning this manuscript.

REFERENCES

- [1] K. Beauchamp, R. Nicoara, Orthogonal maximal Abelian *-subalgebras of the 6×6 matrices, *Linear Algebra Appl.* **428**, No. 8-9, 1833–1853 (2008). MR2398121 (2009b:16068)
- [2] I. Bengtsson, W. Bruzda, Å. Ericsson, J. Larsson, W. Tadej, K. Życzkowski, Mutually unbiased bases and Hadamards of order six, *J. Math. Phys.* **48**, 052106 (2007).

- [3] G. Björck, Functions of modulus 1 on \mathbb{Z}_n , whose Fourier transform have constant modulus, and “cyclic n -roots”. Recent Advances in Fourier Analysis and Its Applications. NATO Adv. Sci. Int. Ser. C, Math. Phys. Sci., **315**, Kluwer, 131–140 (1990). MR1081347 (91k:42021)
- [4] S. Brierley, S. Weigert, Maximal sets of mutually unbiased quantum states in dimension six, Phys. Rev. A (3) **78**, no. 4 (2008). MR2491052
- [5] S. Brierley, S. Weigert, Constructing mutually unbiased bases in dimension six, preprint, arXiv:0901.4051v1 [quant-ph] (2009).
- [6] P. Butterley, W. Hall, Numerical evidence for the maximum number of mutually unbiased bases in dimension six, *Physics Letters A* **369**, 5–8 (2007).
- [7] N. J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Security of quantum key distribution using d -level systems, *Phys. Rev. Lett.* **88**, 127902 (2002).
- [8] P. Diță, Some results on the parametrization of complex Hadamard matrices, *J. Phys. A* **37**, no. 20, 5355–5374 (2004). MR2065675 (2005b:15045)
- [9] U. Haagerup, Orthogonal maximal Abelian $*$ -subalgebras of $n \times n$ matrices and cyclic n -roots, Operator Algebras and Quantum Field Theory (Rome, 1996), International Press, Cambridge, MA, 296–322 (1997). MR1491124 (98k:46087)
- [10] P. de la Harpe, V. F. R. Jones, Paires de sous-algèbres semi-simples et graphes fortement réguliers, *C.R. Acad. Sci. Paris* **311**, série I, 147–150 (1990). MR1065880 (92c:16004)
- [11] P. Jaming, M. Matolcsi, P. Móra, F. Szöllösi, M. Weiner, A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6, *J. Physics A: Math. and Theo.* **42**, no. 24 (2009), 245305.
- [12] A. Klappenecker, M. Rötteler, Constructions of Mutually Unbiased Bases. Finite fields and applications, Lecture Notes in Comput. Sci., **2948**, Springer, Berlin, 137–144 (2004). MR2092627 (2005f:81040)
- [13] M. Matolcsi, F. Szöllösi, Towards the classification of 6×6 complex Hadamard matrices, *Open Sys. & Inf. Dyn.* **15:2**, 93–108 (2008). MR2451755
- [14] A. Munemasa, Y. Watatani, Orthogonal pairs of $*$ -subalgebras and association schemes, *C.R. Acad. Sci. Paris* **314**, série I, 329–331 (1992). MR1153709 (92m:46090)
- [15] S. Popa, Orthogonal pairs of $*$ -subalgebras in finite von Neumann algebras, *J. Operator Theory* **9**, 253–268 (1983). MR703810 (84h:46077)
- [16] M. Saniga, M. Planat, Sets of mutually unbiased bases as arcs in finite projectives planes, *Chaos Solitons Fractals* **26**, 1267–1270 (2005). MR2149314 (2006d:81050)
- [17] A. J. Skinner, V. A. Newell, R. Sanchez, Unbiased bases (Hadamards) for 6-level systems: Four ways from Fourier, preprint, arXiv:0810.1761v1 [quant-ph] (2008).
- [18] W. Tadej, K. Życzkowski, A concise guide to complex Hadamard matrices, *Open Syst. Inf. Dyn.* **13**, 133–177 (2006). MR2244963 (2007f:15020)
- [19] Website for complex Hadamard matrices: <http://chaos.if.uj.edu.pl/~karol/hadamard/>
- [20] M. Weiner, A gap for the maximum number of mutually unbiased bases, preprint, arXiv:0902.0635v1 [math-ph] (2009).
- [21] R. F. Werner, All teleportation and dense coding schemes, *J. Phys. A* **34**, 7081–7094 (2001). MR1863141 (2002i:81063)
- [22] P. Wocjan, Th. Beth, New construction of mutually unbiased bases in square dimensions, *Quantum Information & Computation* **5:2**, 93–101 (2005). MR2132048 (2006g:05039)
- [23] W. K. Wootters, B. D. Fields, Optimal state-determination by mutually unbiased measurements, *Ann. Physics* **191**, 363–381 (1989). MR1003014 (90e:81019)
- [24] G. Zauner, Orthogonale Lateinische Quadrate und Anordnungen, Verallgemeinerte Hadamard-matrizen und Unabhängigkeit in der Quanten-Wahrscheinlichkeitstheorie, Master Thesis, Universität Wien (1991).

INSTITUTE OF MATHEMATICS AND ITS APPLICATIONS, CENTRAL EUROPEAN UNIVERSITY (CEU),
H-1051, NÁDOR U. 9, BUDAPEST, HUNGARY

E-mail address: szoferi@gmail.com