AN APPLICATION OF POSITIVE DEFINITE FUNCTIONS TO THE PROBLEM OF MUBS

MIHAIL N. KOLOUNTZAKIS, MÁTÉ MATOLCSI, AND MIHÁLY WEINER

ABSTRACT. We present a new approach to the problem of mutually unbiased bases (MUBs), based on positive definite functions on the unitary group. The method provides a new proof of the fact that there are at most $d+1$ MUBs in $\mathbb{C}^d$, and it may also lead to a proof of non-existence of complete systems of MUBs in dimension 6 via a conjectured algebraic identity.

1. INTRODUCTION

In this paper we present a new approach to the problem of mutually unbiased bases (MUBs) in $\mathbb{C}^d$. Our approach has been motivated by two recent results in the literature. First, in [21] one of the present authors described how the Fourier analytic formulation of Delsarte's LP bound can be applied to the problem of MUBs. Second, in [24, Theorem 2] F. M. Oliveira Filho and F. Vallentin proved a general optimization bound which can be viewed as a generalization of Delsarte's LP bound to non-commutative settings (and they applied the theorem to packing problems in Euclidean spaces). As the MUB-problem is essentially a problem over the unitary group, it is natural to combine the two ideas above. Here we present another version of the non-commutative Delsarte scheme in the spirit of [21, Lemma 2.1]. Our formulation in Theorem 2.3 below describes a less general setting than [24, Theorem 2], but it makes use of the underlying group structure and is very convenient for applications. It fits the MUB-problem naturally, and leads us to consider positive definite functions on the unitary group.

The paper is organized as follows. In the Introduction we recall some basic notions and results concerning mutually unbiased bases (MUBs). In Section 2 we describe a non-commutative version of Delsarte's scheme in Theorem 2.3. We believe that this general scheme will be useful for several other applications, too. We then apply the method in Theorem 2.4 to give a new proof of the fact that there are at most $d + 1$ MUBs in $\mathbb{C}^d$. While the result itself has been proved by other methods, we believe that this approach is particularly suited for the MUB-problem and may lead to non-existence proofs in the future. In particular, in Section 3 we speculate on how the non-existence of complete systems of MUBs could be proved in dimension 6 via an algebraic identity conjectured in [22].

Throughout the paper we follow the convention that inner products are linear in the first variable and conjugate linear in the second.

Recall that two orthonormal bases in $\mathbb{C}^d$, $\mathcal{A} = \{\mathbf{e}_1, \ldots, \mathbf{e}_d\}$ and $\mathcal{B} = \{\mathbf{f}_1, \ldots, \mathbf{f}_d\}$ are called *unbiased* if for every $1 \leq j, k \leq d$, $|\langle \mathbf{e}_j, \mathbf{f}_k \rangle| = \dfrac{1}{\sqrt{d}}$. A collection $\mathcal{B}_1, \ldots \mathcal{B}_m$ of orthonormal bases is said to be (pairwise) *mutually unbiased* if any two of them are unbiased. What is the maximal number of mutually unbiased bases (MUBs) in $\mathbb{C}^d$? This problem has its origins in quantum information theory, and has received considerable attention over the past decades (see e.g. [14] for a recent comprehensive survey on MUBs). The following upper bound is well-known (see e.g. [1, 3, 30]):

Theorem 1.1. *The number of mutually unbiased bases in $\mathbb{C}^d$ is less than or equal to $d + 1$.*

We will give a new proof of this fact in Theorem 2.4 below. Another important result concerns the existence of complete systems of MUBs in prime-power dimensions (see e.g. [1, 11, 12, 17, 20, 30]).

Theorem 1.2. *A collection of $d + 1$ mutually unbiased bases (called a complete system of MUBs) exists (and can be constructed explicitly) if the dimension d is a prime or a prime-power.*

However, if the dimension $d = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ is not a prime-power, very little is known about the maximal number of MUBs. By a tensor product construction it is easy to see that there are at least $p_j^{\alpha_j} + 1$ MUBs in $\mathbb{C}^d$ where $p_j^{\alpha_j}$ is the smallest of the prime-power divisors of d. One could be tempted to conjecture the maximal number of MUBs always equals $p_j^{\alpha_j} + 1$, but this is already known to be false: for some

specific square dimensions $d = s^2$ a construction of [29] yields more MUBs than $p_j^{\alpha_j} + 1$ (the construction is based on orthogonal Latin squares). Another important phenomenon, proved in [28], is that the maximal number of MUBs cannot be exactly d (it is either $d + 1$ or strictly less than d).

The following basic problem remains open for all non-primepower dimensions:

Problem 1.3. *Does a complete system of $d + 1$ mutually unbiased bases exist in $\mathbb{C}^d$ if d is not a prime-power?*

For $d = 6$ it is widely believed among researchers that the answer is negative, and the maximal number of MUBs is 3. The proof still eludes us, however, despite considerable efforts over the past decade ([3, 4, 5, 6, 18]). On the one hand, some *infinite families* of MUB-triplets in $\mathbb{C}^6$ have been constructed ([18, 31]). On the other hand, numerical evidence strongly suggests that there exist no MUB-quartets [5, 6, 8, 31]. For non-primepower dimensions other than 6 we are not aware of any conjectures as to the exact maximal number of MUBs.

It will also be important to recall the relationship between mutually unbiased bases and *complex Hadamard matrices*. A $d \times d$ matrix H is called a complex Hadamard matrix if all its entries have modulus 1 and $\frac{1}{\sqrt{d}}H$ is unitary. Given a collection of MUBs $\mathcal{B}_1, \ldots, \mathcal{B}_m$ we may regard the bases as unitary matrices $U_1, \ldots, U_m$ (with respect to some fixed orthonormal basis), and the condition of the bases being pairwise unbiased amounts to $U_i^* U_j$ being a complex Hadamard matrix scaled by a factor of $\frac{1}{\sqrt{d}}$ for all $i \neq j$. That is, $U_i^* U_j$ is a unitary matrix (which is of course automatic) whose entries are all of absolute value $\frac{1}{\sqrt{d}}$.

A complete classification of MUBs up to dimension 5 (see [7]) is based on the classification of complex Hadamard matrices (see [16]). However, the classification of complex Hadamard matrices in dimension 6 is still out of reach despite recent efforts [2, 19, 23, 26, 27].

In this paper we will use the above connection of MUBs to complex Hadamard matrices. In particular, we will describe a Delsarte scheme for non-commutative groups in Theorem 2.3, and apply it to the MUB-problem with an appropriate witness function $h(Z)$ on the unitary group $U(d)$ in Theorem 2.4.

2. Mutually unbiased bases and a non-commutative Delsarte scheme

In this section we describe a non-commutative version of Delsarte's scheme, and show how the problem of mutually unbiased bases fit into this scheme. The commutative analogue was described in [21].

Let G be a compact group, the group operation being multiplication and the unit element being denoted by 1. We will denote the normalized Haar measure on G by μ. Let a symmetric subset $A = A^{-1} \subset G$, $1 \in A$, be given. We think of A as the 'forbidden' set. We would like to determine the maximal cardinality of a set $B = \{b_1, \ldots b_m\} \subset G$ such that all the quotients $b_j^{-1} b_k \in A^c \cup \{1\}$ (in other words, all quotients avoid the forbidden set A). When G is commutative, some well-known examples of this general scheme are present in coding theory ([13]), sphere-packings ([9]), and sets avoiding square differences in number theory ([25]). We will discuss the non-commutative case here.

Recall that the convolution of $f, g \in L^1(G)$ is defined by $f * g(x) = \int f(y)g(y^{-1}x)d\mu(y)$.

Recall also the notion of positive definite functions on G. A function $h : G \to \mathbb{C}$ is called positive definite, if for any m and any collection $u_1, \ldots, u_m \in G$, and $c_1, \ldots, c_m \in \mathbb{C}$ we have $\sum_{i,j=1}^m h(u_i^{-1} u_j)\overline{c_i}c_j \geq 0$. When h is continuous, the following characterization is well-known.

Lemma 2.1. (cf. [15, Proposition 3.35]) *If G is a compact group, and $h : G \to \mathbb{C}$ is a continuous function, the following are equivalent.*

(i) h is of positive type, i.e.

$$
(1) \qquad \int (\tilde{f} * f)h \geq 0
$$

for all functions $f \in L^2(G)$ (here $\tilde{f}(x) = \overline{f(x^{-1})}$)

(ii) h is positive definite

This statement is fully contained in the more general Proposition 3.35 in [15]. In fact, for compact groups Proposition 3.35 in [15] shows that instead of $L^2(G)$ the smaller class of continuous functions $C(G)$ or the wider class of absolute integrable functions $L^1(G)$ could also be taken in (i). All these cases are equivalent, but for us it will be convenient to use $L^2(G)$ in the sequel.

We formulate another important property of positive definite functions.

Lemma 2.2. *Let G be a compact group and μ the normalized Haar measure on G. If $h : G \to \mathbb{C}$ is a continuous positive definite function then $\alpha = \int_G h d\mu \geq 0$, and for any $\alpha_0 \leq \alpha$ the function $h - \alpha_0$ is also positive definite. In other words, for any m and any collection $u_1, \ldots, u_m \in G$ and $c_1, \ldots, c_m \in \mathbb{C}$ we have*

$$(2) \qquad \sum_{i,j=1}^{m} h(u_i^{-1} u_j) \overline{c_i} c_j \geq \alpha \Big| \sum_{i=1}^{m} c_i \Big|^2.$$

Proof. Let $f \in L^2(G)$ and define a linear operator $H : L^2(G) \to L^2(G)$ by

$$(Hf)(x) = \int h(x^{-1}y) f(y) \, d\mu(y).$$

As h is assumed to be positive definite, H is positive self-adjoint. Also, writing $\mathbf{1}$ for the constant one function on G we have

$$H\mathbf{1} = \alpha\mathbf{1}, \quad \langle H\mathbf{1}, \mathbf{1} \rangle = \alpha \geq 0.$$

Let us use the notation $\beta = \int f$. We have the orthogonal decomposition

$$f = \beta\mathbf{1} + f_2, \quad \text{where } f_2 \perp \mathbf{1}.$$

Using the invariance of the Haar measure and exchanging the order of integration we have

$$\langle Hf, \mathbf{1} \rangle = \int (Hf)(x), \overline{\mathbf{1}(x)} d\mu(x) = \int h(x) d\mu(x) \int f(y) d\mu(y) = \alpha\beta$$

Therefore,

$$\alpha\beta = \langle Hf, \mathbf{1} \rangle = \langle H(\beta\mathbf{1} + f_2), \mathbf{1} \rangle = \alpha\beta + \langle Hf_2, \mathbf{1} \rangle,$$

and hence $\langle Hf_2, \mathbf{1} \rangle = 0$.

To show that $h - \alpha$ is positive definite we need to check that

$$\langle Hf, f \rangle - |\beta|^2 \alpha \geq 0,$$

for all $f \in L^2(G)$. We have

$$\langle Hf, f \rangle = \langle \beta\alpha\mathbf{1} + Hf_2, \beta\mathbf{1} + f_2 \rangle = |\beta|^2 \alpha + \langle Hf_2, f_2 \rangle$$

since $f_2 \perp \mathbf{1}$ and $Hf_2 \perp \mathbf{1}$. Hence $\langle Hf, f \rangle - |\beta|^2 \alpha = \langle Hf_2, f_2 \rangle \geq 0$. $\quad\square$

After these preliminaries we can describe the non-commutative analogue of Delsarte's LP bound. (To the best of our knowledge the commutative version was first introduced by Delsarte in connection with binary codes with prescribed Hamming distance [13]. Another formulation of the non-commutative version is given in [24]).

Theorem 2.3. *(Non-commutative Delsarte scheme for compact groups) Let G be a compact group, μ the normalized Haar measure, and let $A = A^{-1} \subset G$, $1 \in A$, be given. Assume that there exists a positive definite function $h : G \to \mathbb{R}$ such that $h(x) \leq 0$ for all $x \in A^c$, and $\int h d\mu > 0$. Then for any $B = \{b_1, \ldots b_m\} \subset G$ such that $b_j^{-1} b_k \in A^c \cup \{1\}$ the cardinality of B is bounded by $|B| \leq \frac{h(1)}{\int h d\mu}$.*

Proof. Consider

$$S = \sum_{u,v \in B} h(u^{-1}v). \tag{3}$$

On the one hand,

$$S \leq h(1)|B|, \tag{4}$$

since all the terms $u \neq v$ are non-positive by assumption.

On the other hand, applying (2) with $\alpha = \int h d\mu$, $u, v \in B$ and $c_u = c_v = 1$, we get

$$S \geq \alpha |B|^2. \tag{5}$$

Comparing the two estimates (5), (4) we obtain $|B| \leq \frac{h(1)}{\int h d\mu}$. $\square$

The function h in the Theorem above is usually called a *witness function*.

We will now describe how the problem of mutually unbiased bases fits into this scheme. Consider the group $U(d)$ of unitary matrices, being given with respect to some fixed orthonormal basis of $\mathbb{C}^d$. Consider the set CH of complex Hadamard matrices. Following the notation of the Delsarte scheme above define $A^c = \frac{1}{\sqrt{d}} CH \subset U(d)$, i.e. let the *complement* of the forbidden set be the set of scaled complex Hadamard matrices. Then the maximal number of MUBs in $\mathbb{C}^d$ is exactly the maximal cardinality of a set $B = \{b_1, \ldots b_m\} \subset U(d)$ such that all the quotients $b_j^{-1} b_k \in A^c \cup \{1\}$. After finding an appropriate witness function we can now give a new proof of the fact the number of MUBs in $\mathbb{C}^d$ cannot exceed $d + 1$.

Theorem 2.4. *The function $h(Z) = -1 + \sum_{i,j=1}^{d} |z_{i,j}|^4$ (where $Z = (z_{i,j})_{i,j=1}^{d} \in U(d)$) is positive definite on $U(d)$, with $h(1) = d - 1$ and $\int h = \frac{d-1}{d+1}$. Consequently, the number of MUBs in dimension d cannot exceed $d + 1$.*

Proof. Consider the function $h_0(Z) = \sum_{i,j=1}^{d} |z_{i,j}|^4$. First we prove that h_0 is positive definite. For this, recall that the Hilbert-Schmidt inner product of matrices is defined as $\langle X, Y \rangle_{HS} = \text{Tr}(XY^*)$, and for any

vector v in a finite dimensional Hilbert space H the (scaled) projection operator P_v is defined as $P_v u = \langle u, v \rangle v$. For any two vectors $u, v \in H$ we have $|\langle u, v \rangle|^2 = \operatorname{Tr} P_u P_v$. Also, recall that the inner product on $H \otimes H$ is given by $\langle u_1 \otimes u_2, v_1 \otimes v_2 \rangle = \langle u_1, v_1 \rangle \langle u_2, v_2 \rangle$.

Let $U_1, \ldots, U_m$ be unitary matrices, $c_1, \ldots, c_m \in \mathbb{C}$, and let $\{e_1, \ldots, e_d\}$ be the orthonormal basis with respect to which the matrices in $U(d)$ are given. Then

$$(6) \quad |\langle U_r^* U_t e_j, e_k \rangle|^4 = |\langle U_t e_j, U_r e_k \rangle|^4 = |\langle U_t e_j \otimes U_t e_j, U_r e_k \otimes U_r e_k \rangle|^2 =$$

$$\operatorname{Tr} P_{U_t e_j \otimes U_t e_j} P_{U_r e_k \otimes U_r e_k}.$$

Therefore, with the notation $Q_t = \sum_{j=1}^m P_{U_t e_j \otimes U_t e_j}$ we have

$$(7) \qquad h(U_r^* U_t) = \sum_{j,k} |\langle U_r^* U_t e_j, e_k \rangle|^4 = \operatorname{Tr} Q_t Q_r.$$

Finally,

$$(8) \qquad \sum_{r,t=1}^m h(U_r^* U_t) \overline{c_r} c_t = \| \sum_{t=1}^m c_t Q_t \|_{HS}^2 \geq 0,$$

as desired.

It is known [10] that the integral of h_0 on $U(d)$ is $\frac{2d}{d+1}$. By applying Lemma 2.2 to h_0 with $\alpha_0 = 1 < \int h_0$ we get that h is also positive definite. Note also that h vanishes on the set $\frac{1}{\sqrt{d}} CH$ of scaled complex Hadamard matrices, $h(1) = d - 1$, and $\int h = \frac{2d}{d+1} - 1 = \frac{d-1}{d+1}$. Therefore, Theorem 2.3 implies that the number of MUBs in $\mathbb{C}^d$ is less than or equal to $\frac{h(1)}{\int h} = d + 1$. $\qquad \square$

We remark here that one could consider the witness functions $h_\beta = h_0 - \beta$ for any $1 \leq \beta \leq \frac{2d}{d+1}$. All these functions satisfy the conditions of Theorem 2.3. However, an easy calculation shows that the best bound is achieved for $\beta = 1$.

3. Dimension 6

The function $h(Z) = -1 + \sum_{i,j=1}^d |z_{i,j}|^4$ in Theorem 2.4 was a fairly natural candidate, as it vanishes on the set of (scaled) complex Hadamard matrices $\frac{1}{\sqrt{d}} CH$, for any d. Other such candidates are $h_k(Z) = -\frac{1}{n^{k-2}} + \sum_{i,j=1}^d |z_{i,j}|^{2k}$ for any $k \geq 2$, but they give worse upper bounds than h. Furthermore, Theorem 1.2 implies that the result of Theorem 2.4

is sharp whenever d is a prime-power, and hence we cannot hope to construct better witness functions than h, *in general*. However, let us examine the situation more closely in dimension $d = 6$, and discuss why we hope that the non-existence of a complete system of MUBs could be proved by this method.

For $d = 6$ we have other functions which are *conjectured* to vanish on $\frac{1}{\sqrt{d}}CH$. Namely, Conjecture 2.3 in [22] provides a selection of such functions. Let

$$(9) \qquad m_1(Z) = \sum_{\pi \in S_6} \sum_{j=1}^{6} z_{\pi(1),j} z_{\pi(2),j} z_{\pi(3),j} \overline{z_{\pi(4),j} z_{\pi(5),j} z_{\pi(6),j}},$$

where S_6 denotes the permutation group on 6 elements. Also, let $m_2(Z) = m_1(Z^*)$. Then m_1 and m_2 are real-valued (because each term appears with its conjugate), and they are conjectured to vanish on $\frac{1}{\sqrt{d}}CH$. Furthermore, as the inner sum in (9) is conjectured to be zero for all $\pi \in S_6$, we may even multiply each term with $(-1)^{\text{sgn }\pi}$, if we wish. This leads to other possible choices of m_1 and m_2.

The algebraic identity (9) makes dimension 6 very special and provides some further natural candidates of witness functions for the MUB-problem. Namely, let

$$m(Z) = (m_1(Z) + m_2(Z))^2, \quad \text{or}$$

$$m(Z) = m_1^2(Z) + m_2^2(Z), \quad \text{or}$$

$$m(Z) = (m_1(Z)m_2(Z))^2.$$

In all three cases $m(I) = 0$, and $\int_{Z \in U(d)} m(Z)d\mu > 0$. Therefore, if for any $\varepsilon > 0$ the function $h(Z) + \varepsilon m(Z)$ is positive definite, we get a better bound than in Theorem 2.4, and obtain that the number of MUBs in dimension 6 is strictly less than 7, i.e. a complete system of MUBs does not exist. This leads us to the following general problem.

Problem 3.1. *Given a polynomial function $f(Z)$ of the matrix elements $z_{i,j}$ and their conjugates $\overline{z_{i,j}}$, what is a necessary and sufficient condition for f to be positive definite on the unitary group $U(d)$?*

Finally, it would also be interesting to find any analogue of Conjecture 2.3 in [22] for any dimensions other than $d = 6$.

References

[1] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury & F. Vatan, *A New Proof for the Existence of Mutually Unbiased Bases.* Algorithmica **34** (2002), 512-528.

[2] K. Beauchamp & R. Nicoara, *Orthogonal maximal Abelian ∗-subalgebras of the 6 × 6 matrices.* Linear Algebra Appl. **428** (2008), 1833–1853.

[3] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-A. Larsson, W. Tadej & K. Życzkowski, *Mutually unbiased bases and Hadamard matrices of order six.* J. Math. Phys. **48** (2007), no. 5, 052106, 21 pp.

[4] P. O. Boykin, M. Sitharam, P. H.Tiep, & P. Wocjan, *Mutually unbiased bases and orthogonal decompositions of Lie algebras.* Quantum Inf. Comput. **7** (2007), no. 4, 371–382.

[5] S. Brierley & S. Weigert, *Maximal sets of mutually unbiased quantum states in dimension six.* Phys. Rev. A (3) **78** (2008), no. 4, 042312, 8 pp.

[6] S. Brierley & S. Weigert, *Constructing Mutually Unbiased Bases in Dimension Six.* Phys. Rev. A (3) **79** (2009), no. 5, 052316, 13 pp.

[7] S. Brierley, S. Weigert & I. Bengtsson, *All Mutually Unbiased Bases in Dimensions Two to Five.* Quantum Information and Computing **10**, (2010), 803-820.

[8] P. Butterley & W. Hall, *Numerical evidence for the maximum number of mutually unbiased bases in dimension six.* Physics Letters A **369** (2007) 5-8.

[9] H. Cohn & N. Elkies, *New upper bounds on sphere packings I.* Ann. of Math. (2) **157** (2003), no. 2, 689–714.

[10] B. Collins & P. Sniady *Integration with respect to the Haar measure on unitary, orthogonal and symplectic group.* Commun. Math. Phys. **264** (2006), 773-795.

[11] M. Combescure, *Circulant matrices, Gauss sums and mutually unbiased bases. I. The prime number case.* Cubo **11** (2009), no. 4, 73–86.

[12] M. Combescure, *Block-circulant matrices with circulant blocks, Weil sums, and mutually unbiased bases. II. The prime power case.* J. Math. Phys. **50** (2009), no. 3, 032104, 12 pp.

[13] P. Delsarte, *Bounds for unrestricted codes, by linear programming.* Philips Res. Rep. 27 (1972), 272–289.

[14] T. Durt, B. G. Englert, I. Bengtsson & K. Życzkowski, *On mutually unbiased bases.* International Journal of Quantum Information, Vol. **8**, No. 4 (2010) 535–640

[15] G. B. Folland *A Course in Abstract Harmonic Analysis.* CRC Press, Boca Raton, 1995.

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

[17] I. D. Ivanovic, *Geometrical description of quantal state determination.* J. Phys. A **14** (1981), 3241.

[18] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi, M. Weiner, *A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6.* J. Physics A: Mathematical and Theoretical, Vol. 42, Number 24, 245305, 2009.

[19] B. R. KARLSSON, *Three-parameter complex Hadamard matrices of order 6.* Linear Algebra and its Applications, Volume 434, Issue 1, 1 January 2011, Pages 247258

[20] A. KLAPPENECKER & M. RÖTTELER, *Constructions of Mutually Unbiased Bases.* Finite fields and applications, 137–144, Lecture Notes in Comput. Sci., **2948**, Springer, Berlin, 2004.

[21] M. MATOLCSI, *A Fourier analytic approach to the problem of mutually unbiased bases.* Stud. Sci. Math. Hung., Vol. 49, No. 4 (2012), 482-491.

[22] M. MATOLCSI, I. Z. RUZSA & M. WEINER *Systems of mutually unbiased Hadamard matrices containing real and complex matrices.* Australasian J. Combinatorics, Volume 55 (2013), Pages 3547.

[23] M. MATOLCSI & F. SZÖLLŐSI, *Towards a classification of 6x6 complex Hadamard matrices.* Open Systems & Information Dynamics, **15**, Issue:2, (June 2008), 93-108.

[24] F. M. OLIVEIRA DE FILHO & F. VALLENTIN *Mathematical optimization for packing problems.* SIAG/OPT Views and News **23**(2) (2015) 5-14.

[25] I. Z. RUZSA, *Difference sets without squares.* Period. Math. Hungar. 15 (1984), no. 3, 205–209.

[26] A. J. SKINNER, V. A. NEWELL & R. SANCHEZ, *Unbiased bases (Hadamards) for 6-level systems: Four ways from Fourier.* J. Math. Phys. **50** (2009), no. 1, 012107, 7 pp.

[27] F. SZÖLLŐSI, *Complex Hadamard matrices of order 6: a four-parameter family.* J. London Math Soc., **85:2** (2012), 616632.

[28] M. WEINER, *A gap for the maximum number of mutually unbiased bases.* Proc. Amer. Math. Soc. 141 (2013), 1963-1969.

[29] P. WOCJAN & T. BETH, *New construction of mutually unbiased bases in square dimensions.* Quantum Inf. Comput. **5** (2005), 93-101.

[30] W. K. WOOTTERS & B. D. FIELDS, *Optimal state-determination by mutually unbiased measurements.* Ann. Physics **191** (1989), 363–381.

[31] G. ZAUNER, *Quantendesigns Grundzüge einer nichtkommutativen Designtheorie.* PhD thesis, Universität Wien, 1999. (available at http://www.mat.univie.ac.at/∼neum/ms/zauner.pdf)

M. N. K.: DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS, UNIVERSITY OF CRETE, VOUTES CAMPUS, 700 13 HERAKLION, GREECE.
E-mail address: `kolount@gmail.com`

M. M.: BUDAPEST UNIVERSITY OF TECHNOLOGY AND ECONOMICS (BME), H-1111, EGRY J. U. 1, BUDAPEST, HUNGARY (ALSO AT ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, H-1053, REALTANODA U 13-15, BUDAPEST, HUNGARY)
E-mail address: `matomate@renyi.hu`

M. W.: BUDAPEST UNIVERSITY OF TECHNOLOGY AND ECONOMICS (BME), H-1111, EGRY J. U. 1, BUDAPEST, HUNGARY
E-mail address: `mweiner@renyi.hu`