A FOURIER ANALYTIC APPROACH TO THE PROBLEM OF MUTUALLY UNBIASED BASES

MÁTÉ MATOLCSI

ABSTRACT. We give a new approach to the problem of mutually unbiased bases (MUBs), based on a Fourier analytic technique borrowed from additive combinatorics. The method provides a short and elegant generalization of the fact that there are at most $d+1$ MUBs in $\mathbb{C}^d$. It may also yield a proof that no complete system of MUBs exists in some composite dimensions – a long standing open problem.

2010 Mathematics Subject Classification. Primary 15A30, Secondary 05B10, 47L05

Keywords and phrases. *Mutually unbiased bases, complex Hadamard matrices, difference sets, Delsarte's method*

1. Introduction

In this paper we introduce a novel approach to the problem of mutually unbiased bases in $\mathbb{C}^d$. Surprisingly, the required Fourier analytic technique is borrowed from additive combinatorics – a seemingly unrelated branch of mathematics.

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 how the problem of MUBs fits into a general scheme in additive combinatorics – a scheme we will call *Delsarte's method.* We then apply this method to prove Theorem 2.2, an elegant generalization of the fact that there are at most $d+1$ MUBs in $\mathbb{C}^d$. Finally, in Section 3 we indicate the limitations of the method by introducing the notion of pseudo-MUBs, and discuss the possible existence of such in the case $d=6$.

Recall that given an orthonormal basis $\mathcal{A} = \{\mathbf{e}_1, \dots, \mathbf{e}_d\}$ in $\mathbb{C}^d$, a unit vector $\mathbf{v}$ is called *unbiased* to $\mathcal{A}$ if $|\langle \mathbf{v}, \mathbf{e}_k\rangle| = \dfrac{1}{\sqrt{d}}$ for all $1 \leq$

M. Matolcsi was supported by the ERC-AdG 228005, and OTKA Grants No. K77748, K81658, and the Bolyai Scholarship.

$k \leq d$. Two orthonormal bases in $\mathbb{C}^d$, $\mathcal{A} = \{\mathbf{e}_1, \dots, \mathbf{e}_d\}$ and $\mathcal{B} = \{\mathbf{f}_1, \dots, \mathbf{f}_d\}$ are called *unbiased* if for every $1 \leq j, k \leq d$, $|\langle \mathbf{e}_j, \mathbf{f}_k \rangle| = \frac{1}{\sqrt{d}}$. A collection $\mathcal{B}_0, \dots \mathcal{B}_m$ of orthonormal bases is said to be *(pairwise) mutually unbiased* if every two of them are unbiased. What is the maximal number of pairwise mutually unbiased bases (MUBs) in $\mathbb{C}^d$? This question originates from quantum information theory and has been investigated thoroughly over the past decades (see [16] for a recent comprehensive survey on MUBs). The following result is well-known (see e.g. [1, 4, 30]):

Theorem 1.1. *The number of mutually unbiased bases in $\mathbb{C}^d$ cannot exceed $d + 1$.*

We will generalize this fact in Theorem 2.2 below. The other important well-known result concerns prime-power dimensions (see e.g. [1, 12, 13, 14, 18, 22, 30]).

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

However, if the dimension $d = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ is composite then very little is known except for the fact that there are at least $p_j^{\alpha_j} + 1$ mutually unbiased bases in $\mathbb{C}^d$ where $p_j^{\alpha_j}$ is the smallest of the prime-power divisors. In some specific square dimensions there is a construction based on orthogonal Latin squares which yields more MUBs than $p_j^{\alpha_j} + 1$ (see [29]). Also, it is known [28] that the maximal number of MUBs cannot be exactly d (either $d + 1$ or strictly less than d).

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

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

The answer is not known even for $d = 6$, despite considerable efforts over the past few years ([4, 5, 6, 7, 8, 19]). The case $d = 6$ is particularly tempting because it seems to be the simplest to handle with algebraic and numerical methods. As of now, some *infinite families* of MUB-triplets in $\mathbb{C}^6$ have been constructed ([19, 31]), but numerical evidence suggests that there exist no MUB-quartets [6, 7, 10, 31].

It will also be important for us to recall that mutually unbiased bases are naturally related to *complex Hadamard matrices*. Indeed, if the bases $\mathcal{B}_0, \dots, \mathcal{B}_m$ are mutually unbiased we may identify each

$\mathcal{B}_l = \{\mathbf{e}_1^{(l)}, \dots, \mathbf{e}_d^{(l)}\}$ with the *unitary* matrix

$$[H_l]_{j,k} = \left[\left\langle \mathbf{e}_j^{(0)}, \mathbf{e}_k^{(l)} \right\rangle_{1 \le k,j \le d} \right],$$

i.e. the k-th column of H_l consists of the coordinates of the k-th vector of $\mathcal{B}_l$ in the basis $\mathcal{B}_0$. (Throughout the paper the scalar product $\langle .,. \rangle$ of $\mathbb{C}^d$ is conjugate-linear in the first variable and linear in the second.) With this convention, $H_0 = I$ the identity matrix and all other matrices are unitary and have entries of modulus $1/\sqrt{d}$. Therefore, the matrices $H_l' = \sqrt{d} H_l$ have all entries of modulus 1 and complex orthogonal rows (and columns). Such matrices are called *complex Hadamard matrices.* It is thus clear that the existence of a family of mutually unbiased bases $\mathcal{B}_0, \dots, \mathcal{B}_m$ is equivalent to the existence of a family of complex Hadamard matrices $H_1', \dots, H_m'$ such that for all $1 \le j \ne k \le m$, $\frac{1}{\sqrt{d}} H_j'^{*} H_k'$ is again a complex Hadamard matrix. In such a case we will say that these complex Hadamard matrices are *mutually unbiased.*

A complete classification of MUBs up to dimension 5 (see [9]) is based on the classification of complex Hadamard matrices (see [17]). However, the classification of complex Hadamard matrices in dimension 6 is still out of reach despite recent efforts [2, 20, 21, 23, 25, 26, 27].

In this paper we will use the above connection of MUBs to complex Hadamard matrices to apply a Fourier analytic approach, borrowed from additive combinatorics.

2. Mutually unbiased bases, difference sets and Delsarte's method

In this section we describe a general scheme in additive combinatorics, and show how the problem of mutually unbiased bases fit into this scheme.

Let G be a compact Abelian group, and let a symmetric subset $A = -A \subset G$, $0 \in A$ be given. We will call A the 'forbidden' set. We would like to determine the maximal cardinality of a set $B = \{b_1, \dots b_m\} \subset G$ such that all differences $b_j - b_k \in A^c \cup \{0\}$ (in other words, all differences avoid the forbidden set A). Some well-known examples of this general scheme are present in coding theory ([15]), sphere-packings ([11]), and sets avoiding square differences in number theory ([24]).

We will also need the dual group $\hat{G}$, i.e the group of multiplicative characters from G to $\mathbb{C}$. In this note we will use the additive notation for the operation of the dual group, i.e. for $\gamma_1, \gamma_2 \in \hat{G}$ and $x \in G$ we define $(\gamma_1 + \gamma_2)(x) = \gamma_1(x)\gamma_2(x)$. (This notation reflects that in the concrete situations below the characters γ are of the type $\gamma(x) = e^{2i\pi\langle v,x\rangle}$.) In particular, the unit element of the dual group (i.e. the constant 1 function) will be denoted by $0 \in \hat{G}$.

We now describe a general method to tackle such problems. To the best of my knowledge it was first introduced by Delsarte in connection with binary codes with prescribed Hamming distance. The method is also 'folklore' in the additive combinatorics community and I was introduced to it by Imre Z. Ruzsa (personal communication).

We are looking for a 'witness' function $h : G \to \mathbb{R}$ with the following properties.

- h is an even function, $h(x) = h(-x)$, such that the Fourier inversion formula holds for h (in particular, h can be any finite linear combination of characters on G).
- $h(x) \leq 0$ for all $x \in A^c$
- $\hat{h}(\gamma) \geq 0$ for all $\gamma \in \hat{G}$
- $\hat{h}(0) = 1$.

Lemma 2.1. *(Delsarte's method)*
Given a function $h : G \to \mathbb{R}$ with the properties above, we can conclude that for any $B = \{b_1, \dots b_m\} \subset G$ such that $b_j - b_k \in A^c \cup \{0\}$ the cardinality of B is bounded by $|B| \leq h(0)$.

Proof. For any $\gamma \in \hat{G}$ define $\hat{B}(\gamma) = \sum_{j=1}^{m} \gamma(b_j)$. Now, evaluate

$$S = \sum_{\gamma \in \hat{G}} |\hat{B}(\gamma)|^2 \hat{h}(\gamma). \tag{1}$$

All terms are nonnegative, and the term corresponding to $\gamma = 0$ (the trivial character, i.e. $\gamma(x) = 1$ for all $x \in G$) gives $|\hat{B}(0)|^2 \hat{h}(0) = |B|^2$. Therefore

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

On the other hand, $|\hat{B}(\gamma)|^2 = \sum_{j,k} \gamma(b_j - b_k)$, and therefore $S = \sum_{\gamma,j,k} \gamma(b_j - b_k)\hat{h}(\gamma)$. Summing up for fixed j, k we get
$\sum_{\gamma} \gamma(b_j - b_k)\hat{h}(\gamma) = h(b_j - b_k)$ (the Fourier inversion formula), and therefore $S = \sum_{j,k} h(b_j - b_k)$. Notice that $j = k$ happens $|B|$-many times, and all the other terms (when $j \neq k$) are non-positive because $b_j - b_k \in A^c$, and h is required to be non-positive there. Therefore

$$S \leq h(0)|B|. \tag{3}$$

Comparing the two estimates (2), (3) we obtain $|B| \le h(0)$. □

We will now describe how mutually unbiased bases fit into this scheme.

Assume that a family $H_1, \dots H_m$ of m mutually unbiased complex Hadamard matrices exists. Then all entries of all matrices are of modulus 1, and the columns (and thus the rows) within each matrix are complex orthogonal, and we have the unbiasedness condition: for any two columns $\mathbf{u}, \mathbf{v}$ coming from different matrices we have $|\langle \mathbf{u}, \mathbf{v} \rangle| = \sqrt{d}$. (Recall that we have re-normalized the matrices by a factor of $\sqrt{d}$.)

After multiplying rows and columns by appropriate scalars if necessary, we can assume that all coordinates of the first row and column of H_1 are 1's, and all coordinates of the first row of all other matrices are 1's (i.e. we assume that all appearing columns have first coordinate 1, and the first column in H_1 consists of 1's. This is standard and trivial normalization.) All the other coordinates in the matrices are complex numbers of modulus 1, i.e. they are of the form $e^{2\pi i \rho}$ with $\rho \in [-1/2, 1/2)$. Therefore, we can associate to each column vector $(1, e^{2\pi i \rho_1}, \dots, e^{2\pi i \rho_{d-1}})$ the vector $(0, \rho_1, \dots, \rho_{d-1}) \in \mathbb{T}^d$, the real d-dimensional torus, $\mathbb{T}^d = [-1/2, 1/2)^d$. Also, note that the first coordinate always automatically becomes 0, because each column starts with coordinate 1. Therefore we make the more useful association that a column $\mathbf{c} = (1, e^{2\pi i \rho_1}, \dots, e^{2\pi i \rho_{d-1}})$ is represented by $\mathbf{u} = (\rho_1, \dots \rho_{d-1}) \in \mathbb{T}^{d-1}$, the $d-1$-dimensional torus. There are altogether md column vectors in the Hadamard matrices $H_1, \dots H_m$, and we will denote the associated vectors in $\mathbb{T}^{d-1}$ by $\mathbf{u}_1, \dots \mathbf{u}_{md}$ (we will see that in this approach it is not really relevant to indicate which vector comes from which basis. But let us agree for convenience that $\mathbf{u}_1 = (0, \dots, 0)$, corresponding to the first column of H_1.)

Two columns $\mathbf{c}_1 = (1, e^{2\pi i \rho_1}, \dots, e^{2\pi i \rho_{d-1}})$ and $\mathbf{c}_2 = (1, e^{2\pi i \mu_1}, \dots, e^{2\pi i \mu_{d-1}})$ are orthogonal if and only if $1 + \sum_{j=1}^{d-1} e^{2\pi i(-\rho_j + \mu_j)} = 0$, and they are unbiased if and only if $|1 + \sum_{j=1}^{d-1} e^{2\pi i(-\rho_j + \mu_j)}| = \sqrt{d}$. Therefore it is natural to introduce the following definitions.

Definition 2.1. *Let ORT_d denote the set of vectors $(\alpha_1, \dots \alpha_{d-1}) \in \mathbb{T}^{d-1}$, in the $d-1$-dimensional torus, such that $1 + \sum_{j=1}^{d-1} e^{2\pi i \alpha_j} = 0$. Also, let UB_d denote the set of vectors $(\alpha_1, \dots \alpha_{d-1}) \in \mathbb{T}^{d-1}$, such that $|1 + \sum_{j=1}^{d-1} e^{2\pi i \alpha_j}| = \sqrt{d}$. Let us also define the 'forbidden' set $A_d = (ORT_d \cup UB_d)^c$.*

We conclude that the vectors $\mathbf{u}_1, \dots \mathbf{u}_{md}$ satisfy that the difference of any two of them (the difference being taken *mod* 1 in each coordinate, i.e. we take the difference in the group $\mathbb{T}^{d-1}$) lies in $A_d^c \cup \{0\}$. Therefore, we have arrived exactly to the scheme of Lemma 2.1.

As a preliminary remark we note that the dual group of $G = \mathbb{T}^{d-1}$ is $\hat{G} = \mathbb{Z}^{d-1}$. And the action of a character $\gamma \in \mathbb{Z}^{d-1}$ on a point $x \in \mathbb{T}^{d-1}$ is given as $\gamma(x) = e^{2\pi i \langle \gamma, x \rangle}$. In particular, $\gamma = 0$ is the trivial character (constant 1). The Fourier transform of a function $f : G \to \mathbb{C}$ is a function $\hat{f} : \hat{G} \to \mathbb{C}$ given as $\hat{f}(\gamma) = \int_{x \in G} f(x)\gamma(x)dx$.

Let us see whether we can find a good 'witness' function in this situation. At first sight things do not look promising because we have no understanding of the geometry of the sets ORT_d and UB_d inside the torus $\mathbb{T}^{d-1}$. However, it turns out such geometric understanding is not necessarily required and we easily prove the following generalization of Theorem 1.1.

Theorem 2.2. *Let $\mathcal{A}$ be an orthonormal basis in $\mathbb{C}^d$, and let $B = \{\mathbf{c}_1, \dots \mathbf{c}_r\}$ consist of unit vectors which are all unbiased to $\mathcal{A}$. Assume that for all $1 \leq j \neq k \leq r$ the vectors $\mathbf{c}_j$ and $\mathbf{c}_k$ are either orthogonal or unbiased to each other, i.e. either $\langle \mathbf{c}_j, \mathbf{c}_k \rangle = 0$ or $|\langle \mathbf{c}_j, \mathbf{c}_k \rangle| = 1/\sqrt{d}$. Then $r \leq d^2$.*

Proof. As we saw in the discussion above, the vectors $\mathbf{u}_1, \dots \mathbf{u}_r \in \mathbb{T}^{d-1}$ (associated to $\sqrt{d}\mathbf{c}_1, \dots \sqrt{d}\mathbf{c}_r$) satisfy $\mathbf{u}_j - \mathbf{u}_k \in A_d^c \cup \{0\}$ for all $1 \leq j, k \leq r$. Therefore Lemma 2.1 can be applied.

Define the 'witness' function $h : \mathbb{T}^{d-1} \to \mathbb{R}$ as follows:
(4)
$$h(x_1, \dots x_{d-1}) = \frac{1}{(d-1)d} \left| 1 + \sum_{j=1}^{d-1} e^{2\pi i x_j} \right|^2 \left(|1 + \sum_{j=1}^{d-1} e^{2\pi i x_j}|^2 - d \right).$$

It is straightforward to check that h satisfies all requirements. Indeed, h is an even function which vanishes on $ORT_d \cup UB_d$. The Fourier coefficients of h are simply the coefficients of the exponential terms after expanding the brackets, and these are clearly nonnegative. Also $\hat{h}(0) = 1$ because $\hat{h}(0)$ is the integral of h, which is just the constant term. Also, $h(0, \dots 0) = d^2$, so that we conclude from Lemma 2.1 that $|B| \leq d^2$. $\square$

Remark 2.3. As shown by Theorem 1.2 the result of Theorem 2.2 is sharp if d is a prime-power. However, if d is not a prime-power, then it could be possible to find a better witness function than above. The function h above uses simply the *definition* of the sets ORT_d and UB_d. In principle, it could be possible to find some structural properties of these sets in dimension 6 (or any other composite dimension), in order to construct a better witness function and get a sharper bound on r. Any upper bound $r < d^2$ would mean that a complete set of MUBs does not exist in dimension d. We have not been able to make such improvement for any d so far. $\square$

Another observation is that if $r = d^2$ in Theorem 2.2 then both estimates (2), (3) must hold with equality. On the one hand, it is trivial that (3) automatically becomes an equality for the h above (because h is zero on ORT_d and UB_d). On the other hand, inequality (2) becomes an equality *if only if* $|\hat{B}(\gamma)|^2\hat{h}(\gamma) = 0$ for all $\gamma \neq 0$. These are non-trivial conditions and we obtain the following corollary, which is a generalization of Theorem 8 in [3].

Corollary 2.4. *Let $\mathcal{A}$ be an orthonormal basis in $\mathbb{C}^d$, and let $B = \{\mathbf{c}_1, \dots \mathbf{c}_{d^2}\}$ consist of unit vectors which are all unbiased to $\mathcal{A}$. Assume that for all $1 \leq j \neq k \leq d^2$ the vectors $\mathbf{c}_j$ and $\mathbf{c}_k$ are either orthogonal or unbiased to each other. Write B as a $d \times d^2$ matrix, the columns of which are the vectors $\mathbf{c}_j$, $j = 1, \dots d^2$. Let $\mathbf{r}_1, \dots \mathbf{r}_d$ denote the rows of the matrix B, and let $\mathbf{r}_{j/k} = \mathbf{r}_j/\mathbf{r}_k$ denote the coordinate-wise quotient of the rows. Then the vectors $\mathbf{r}_{j/k}$ ($1 \leq j \neq k \leq d$) are orthogonal to each other in $\mathbb{C}^{d^2}$, and they are all orthogonal to the vector $(1, 1, \dots 1) \in \mathbb{C}^{d^2}$.*

Proof. This is a direct consequence of the proof of Lemma 2.1. Indeed, for (2) to be an equality $\hat{B}(\gamma)$ must be zero whenever $\hat{h}(\gamma) \neq 0$ and $\gamma \neq 0$. Looking at the definition of h, $\hat{h}(\gamma) \neq 0$ happens exactly when $\gamma(x_1, \dots x_{d-1}) = e^{2\pi i((x_j - x_k) + (x_q - x_s))}$, for any quadruple $0 \leq j, k, q, s \leq d - 1$, where we use the convention that $x_0 = 0$. Using the definition of $\hat{B}(\gamma)$ we obtain that $\hat{B}(\gamma) = 0$ means exactly that $\mathbf{r}_{j/k}$ and $\mathbf{r}_{s/q}$ are orthogonal to each other. $\square$

3. Linear duality and pseudo-MUBs

We can view the set B in Lemma 2.1 as a 0-1-valued measure on G. Also, observe that B does not directly enter the proof, but instead the function $|\hat{B}(\gamma)|^2 = \widehat{B - B}(\gamma)$ is essential. For any $y \in \mathbb{T}^{d-1}$ let $f(y)$ denote the number of ways of writing y as a difference of two elements of B. Then, for any $\gamma \in \hat{G} = \mathbb{Z}^{d-1}$ we have $|\hat{B}(\gamma)|^2 = \sum_{j,k} \gamma(b_j - b_k) = \sum_y f(y) e^{2\pi i \langle \gamma, y \rangle}$. Therefore, we can view f as a non-negative measure on G which has the following essential properties:

• f is supported on $A^c \cup \{0\} = ORT_d \cup UB_d \cup \{0\}$, and the Fourier transform $\hat{f}(\gamma) = \sum_y f(y) e^{2\pi i \langle \gamma, y\rangle}$ is nonnegative for all $\gamma \in \mathbb{Z}^{d-1}$.

• the coefficients $f(y)$ are nonnegative integers.

• the sum of the coefficients $\sum_y f(y) = |B|^2$.

• $f(0) = |B|$.

Given any such measure f we can repeat the proof of Lemma 2.1 with the 'witness' function h defined in (4), and conclude that

$$\frac{\sum_y f(y)}{f(0)} \le \frac{h(0)}{\hat{h}(0)} = d^2. \tag{5}$$

This motivates the following definition:

Definition 3.1. *We will call a nonnegative measure f on $G = \mathbb{T}^{d-1}$ a complete pseudo-MUB-system in dimension d (or complete pseudo-MUB-d in short) if it satisfies the following conditions:*

• *f is nonnegative, the support of f is finite and is contained in $ORT_d \cup UB_d \cup \{0\}$*

• *the finite exponential sum $\hat{f}(\gamma) = \sum_y f(y) e^{2\pi i \langle \gamma, y\rangle}$ is nonnegative for all $\gamma \in \mathbb{Z}^{d-1}$.*

• *the sum of the coefficients $\sum_y f(y) = d^4$.*

• *$f(0) = d^2$.*

Notice that in this definition f is not required to be integer valued. As discussed above, a complete set of $d+1$ MUBs always gives rise to a complete pseudo-MUB-system. Indeed, let $B \subset \mathbb{T}^{d-1}$ denote the d^2 columns of the corresponding d mutually unbiased Hadamards, and let $f(y) = (B - B)(y)$, meaning the number of ways y can be written as a difference $b_j - b_k$. Then f is a complete pseudo-MUB-system. The converse is not necessarily true: a complete pseudo-MUB-system does not directly imply the existence of a complete set of MUBs.

In any dimension d, if we find a complete pseudo-MUB-d measure f then it could serve as a 'dual-witness' testifying that our function h in equation (4) is best possible, and it would mean that the Delsarte method *alone* cannot prove the non-existence of $d+1$ MUBs in dimension d. We emphasize that it would *not* mean that a complete system of $d+1$ MUBs exists. It would only mean that a complete pseudo-MUB-system exists.

Let us examine the situation in dimension $d = 6$.

One natural idea is to fix some m, and look for a complete pseudo-MUB-6 measure such that its support contains vectors only whose coordinates are mth roots of unity. The reason is that all known complete sets of MUBs consist of such vectors. It is also convenient because such vectors belonging to ORT_6 and UB_6 can easily be listed by a computer code. Furthermore, the restriction $\hat{f}(\gamma) \geq 0$ needs to be checked only as γ ranges over the cube $[0, m-1]^5$, due to periodicity. Finally, we fix $f(0) = 1$ (which is a somewhat more convenient normalization than $f(0) = d^2$ in the definition), and maximize $M = \sum_y f(y)$ by linear programming (a complete pseudo-MUB-6 would have the value 36 here). We have tried this and the results are the following:

- $m = 12$, $M = 17.5$
- $m = 8$, $M = 21.6$
- $m = 16$, $M = 21.6$

As these values are strictly less than 36, we can conclude the following:

Corollary 3.1. *For $m = 8, 12, 16$ there exists no complete system of MUBs in dimension 6 such that the coordinates of all appearing vectors are mth roots of unity. Moreover, complete pseudo-MUB systems supported on such vectors do not exist either.*

Unfortunately, larger values of m are out of our computational power. However, we expect that complete pseudo-MUB-6 systems do exist for some larger values of m, such as $m = 72$ or 144.

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] A. Belovs & J. Smotrovs, *A Criterion for Attaining the Welch Bounds with Applications for Mutually Unbiased Bases.* Lecture Notes In Computer Science, Vol. 5393, Mathematical Methods in Computer Science: Essays in Memory of Thomas Beth, Section: Quantum Computing, (2008), 50 – 69.

[4] 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.

[5] 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.

[6] 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.

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

[8] S. Brierley & S. Weigert, *Mutually Unbiased Bases and Semi-definite Programming.* J. Phys.: Conf. Ser. 254 012008

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

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

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

[12] M. Combescure, *The mutually unbiased bases revisited.* Adventures in mathematical physics, 29–43, Contemp. Math., **447**, Amer. Math. Soc., Providence, RI, 2007.

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

[14] 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.

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

[16] 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

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

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

[19] 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.

[20] B. R. Karlsson, *Two-parameter complex Hadamard matrices for $N = 6$.* J. Math. Phys. **50** (2009), no. 8, 082104, 8 pp.

[21] 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

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

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

[25] 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.

[26] F. Szöllősi, *A two-parameter family of complex Hadamard matrices of order 6 induced by hypocycloids.* Proc. Amer. Math. Soc. **138** (2010), no. 3, 921–928.

[27] F. Szöllősi, *Complex Hadamard matrices of order 6: a four-parameter family.* J. London Math Soc., to appear.

[28] M. Weiner, *A gap for the maximum number of mutually unbiased bases.* Proceedings of the AMS, to appear.

[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. M.: Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences POB 127 H-1364 Budapest, Hungary Tel: (+361) 483-8307, Fax: (+361) 483-8333

E-mail address: matomate@renyi.hu