SYSTEMS OF MUTUALLY UNBIASED HADAMARD MATRICES CONTAINING REAL AND COMPLEX MATRICES

M. MATOLCSI, I.Z. RUZSA, AND M. WEINER

Dedicated to Prof. Kathy J. Horadam on the occasion of her 60th birthday

Abstract. We use combinatorial and Fourier analytic arguments to prove various non-existence results on systems of real and complex unbiased Hadamard matrices. In particular, we prove that a complete system of complex mutually unbiased Hadamard matrices (MUHs) in any dimension cannot contain more than one real Hadamard matrix. We also give new proofs of several known structural results in low dimensions.

1. Introduction

A new approach to the problem of mutually unbiased bases (MUBs) was recently given in [18], based on a general scheme in additive combinatorics. In this paper we continue the investigations along this line, and prove several non-existence results concerning complete systems of MUBs, as well as some structural results in low dimensions. Let us remark here that the existence of MUBs is equivalent to the existence of mutually unbiased Hadamard matrices (MUHs) as explained below. In most of the paper it will be more convenient to deal with MUHs.

The paper is organized as follows. The introduction contains a standard summary of relevant notions and results concerning MUBs and MUHs. We also recall some elements of the general combinatorial scheme which was used in [18]. In Section 2 we use discrete Fourier analysis to prove several structural results on MUHs in low dimensions. Finally, in Section 3 we prove non-existence results including the main result of the paper: a complete system of MUHs can contain at most one real Hadamard matrix. We also give a new proof, without using

M.M supported by the ERC-AdG 228005, and OTKA Grants No. K81658, K77748, and the Bolyai Scholarship. I.Z. R. supported by ERC-AdG 228005, and OTKA Grant No. K81658. M. W. supported in part by the ERC-AdG 227458 OACFT.

computer algebra, of the fact the Fourier matrix F_6 cannot be part of a complete system of MUHs in dimension 6.

Recall that 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 $1 \le j, k \le d$, $|\langle \mathbf{e}_j, \mathbf{f}_k \rangle| = \frac{1}{\sqrt{d}}$. In general, we will say that two unit vectors $\mathbf{u}$ and $\mathbf{v}$ are *unbiased* if $|\langle \mathbf{u}, \mathbf{v} \rangle| = \frac{1}{\sqrt{d}}$. 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. The motivation behind studying MUBs is that if a physical system is prepared in a state of one of the bases, then all outcomes are equally probable when we conduct a measurement in any other basis, and this fact finds applications in dense coding, teleportation, entanglement swapping, covariant cloning, and state tomography (see [9] for a recent comprehensive survey on MUBs and its applications). The following result is well-known (see e.g. [1, 3, 24]):

Theorem 1.1. *The maximal number of mutually unbiased bases in $\mathbb{C}^d$ is at most $d + 1$.*

Another important result concerns prime-power dimensions (see e.g. [1, 12, 16, 24]).

Theorem 1.2. *A collection of $d + 1$ mutually unbiased bases (called a complete set of MUBs) exists 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 [23]). It is also known [22] that the maximal number of MUBs cannot be exactly d (i.e. 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 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 ([3, 6, 7, 13, 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, numerical evidence suggests that the maximal number of MUBs for $d = 6$ is 3 (see [6, 7, 8, 25]).

It will also be important for us to recall that mutually unbiased bases are naturally related to mutually unbiased *complex Hadamard matrices*. Indeed, if the bases $\mathcal{B}_0, \ldots, \mathcal{B}_m$ are mutually unbiased we may identify each $\mathcal{B}_l = \{\mathbf{e}_1^{(l)}, \ldots, \mathbf{e}_d^{(l)}\}$ with the *unitary* matrix

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

i.e. the k-th column of U_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, $U_0 = I$ the identity matrix, and all other matrices are unitary and have all entries of modulus $1/\sqrt{d}$. Therefore, for $1 \leq l \leq m$ the matrices $H_l = \sqrt{d}U_l$ 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 $m + 1$ mutually unbiased bases $\mathcal{B}_0, \ldots, \mathcal{B}_m$ is equivalent to the existence of a family of m complex Hadamard matrices $H_1, \ldots, H_m$ such that for all $1 \leq j \neq k \leq m$, $\frac{1}{\sqrt{d}} H_j^* H_k$ is again a complex Hadamard matrix. In such a case we will say that these complex Hadamard matrices are *mutually unbiased* (MUHs).

A system $H_1, \ldots, H_m$ of MUHs is called *complete* if $m = d$ (cf. Theorem 1.1). We remark that there has been a recent interest in *real* unbiased Hadamard matrices [4, 11, 17], and the main result of this paper is that no pair of real unbiased Hadamard matrices can be part of a complete system of MUHs (see Corollary 3.2). The system $H_1, \ldots H_m$ of MUHs will be called *normalized* if the first column of H_1 has all coordinates 1, and all the columns in all the matrices have first coordinate 1. It is clear that this can be achieved by appropriate multiplication of the rows and columns by umimodular complex numbers. We will also use the standard definition that two complex Hadamard matrices H_1 and H_2 are equivalent, $H_1 \cong H_2$, if $H_1 = D_1 P_1 H_2 P_2 D_2$ with unitary diagonal matrices D_1, D_2 and permutation matrices P_1, P_2.

One possible approach to the MUB problem in dimension 6 is to try to classify (up to equivalence) all complex Hadamard matrices of order 6. However, such a full classification is still out of reach, despite some promising recent developments [14, 15, 20].

The crucial observation in [18] is that the columns of $H_1, \dots, H_m$ can be regarded as elements of the group $\mathcal{G} = \mathbb{T}^d$, where $\mathbb{T}$ stands for the complex unit circle. By doing so, we can use Fourier analysis on $\mathcal{G}$ to investigate the problem of MUHs. We will now collect some notations that will be used in later sections (the notations in this paper are somewhat different and more convenient than in [18]). The group operation in $\mathcal{G}$ is complex multiplication in each coordinate. The dual group is $\hat{\mathcal{G}} = \mathbb{Z}^d$, and the action of a character $\gamma = (r_1, r_2, \dots, r_d) \in \mathbb{Z}^d$ on a group element $\mathbf{v} = (v_1, v_2, \dots, v_d) \in \mathbb{T}^d$ is given by exponentiation in each coordinate $\gamma(\mathbf{v}) = \mathbf{v}^\gamma = v_1^{r_1} v_2^{r_2} \dots v_d^{r_d}$. The Fourier transform of (the indicator function of) a set $S \subset \mathcal{G}$ is given as $\hat{S}(\gamma) = \sum_{\mathbf{s} \in S} \mathbf{s}^\gamma$.

As in [18], introduce the orthogonality set $\mathrm{ORT}_d = \{\mathbf{v} = (v_1, \dots, v_d) \in \mathbb{T}^d \ : \ v_1 + \dots + v_d = 0\}$, and the unbiasedness set $\mathrm{UB}_d = \{\mathbf{v} = (v_1, \dots, v_d) \in \mathbb{T}^d \ : \ |v_1 + \dots + v_d|^2 - d = 0\}$. Then the (coordinate-wise) quotient $\mathbf{v}/\mathbf{u} = (v_1/u_1, v_2/u_2, \dots, v_d/u_d)$ of any two columns from the matrices $H_1, \dots H_m$ will fall into either ORT_d (if $\mathbf{v}$ and $\mathbf{u}$ are in the same matrix) or into UB_d (if $\mathbf{v}$ and $\mathbf{u}$ are in different matrices). This enables one to invoke the general combinatorial scheme which we called "Delsarte's method": we refer the reader to [18] for the details.

2. Structural results on MUBs in low dimensions

In what follows we will assume that a *complete* system of MUHs $H_1, \dots H_d$ is given. In fact, much of the discussion below remains valid for non-complete systems after appropriate modifications, but it will be technically easier to restrict ourselves to the complete case. The general aim is to establish structural properties of $H_1, \dots H_d$ which give restrictions on what a complete system may look like. If some of these properties were to contradict each other in a non-primepower dimension d, then we could conclude that a complete system of dimension d does not exist. This is one of the main tasks for future research, mainly for $d = 6$. We will give some non-existence results in this direction in Section 3.

Consider each appearing complex Hadamard matrix H_j as a d-element set in $\mathbb{T}^d$ (the elements are the columns $\mathbf{c}_1, \dots \mathbf{c}_d$ of the matrix; the dependence on j is suppressed for simplicity), and introduce its Fourier transform

$$g_j(\gamma) := \hat{H}_j(\gamma) = \sum_{k=1}^{d} \mathbf{c}_k^\gamma \qquad \text{for each } \gamma \in \mathbb{Z}^d. \tag{1}$$

Notice that the orthogonality of the *rows* of H_j implies that if $\rho \in \mathbb{Z}^d$ is any permutation of the vector $(1, -1, 0, 0, \dots, 0)$ then

$$g_j(\rho) = 0. \tag{2}$$

Also, note that conjugation is the same as taking reciprocal for unimodular numbers, i.e. $\overline{g_j(\gamma)} = \sum_{k=1}^d \mathbf{c}_k^{-\gamma}$, and therefore the square of the modulus of $g_j(\gamma)$ can be written as

$$G_j(\gamma) := |g_j(\gamma)|^2 = \sum_{k,l=1}^d (\mathbf{c}_k/\mathbf{c}_l)^\gamma \qquad \text{for each } \gamma \in \mathbb{Z}^d. \tag{3}$$

Also, introduce the notation

$$G(\gamma) := \sum_{j=1}^d G_j(\gamma) \qquad \text{for each } \gamma \in \mathbb{Z}^d. \tag{4}$$

In similar fashion, introduce the Fourier transform of the whole system as

$$f(\gamma) := \sum_{j=1}^d g_j(\gamma) \qquad \text{for each } \gamma \in \mathbb{Z}^d, \quad \text{and} \tag{5}$$

$$F(\gamma) := |f(\gamma)|^2 = \sum_{\mathbf{u},\mathbf{v}}^d (\mathbf{u}/\mathbf{v})^\gamma \qquad \text{for each } \gamma \in \mathbb{Z}^d, \tag{6}$$

where the summation goes for all pairs of columns $\mathbf{u}, \mathbf{v}$ in the matrices $H_1, \dots, H_d$.

The main advantage of taking Fourier transforms is that any polynomial relation (such as orthogonality or unbiasedness) among the entries of the matrices H_j will be turned into a *linear* relation on the Fourier side. We will collect here linear equalities and inequalities concerning the functions $F(\gamma)$ and $G(\gamma)$.

Let $\pi_r = (0, 0, \dots 0, 1, 0, \dots 0) \in \mathbb{Z}^d$ denote the vector with the rth coordinate equal to 1. Then for each $j = 1, \dots d$ we have

$$\sum_{r=1}^d G_j(\gamma+\pi_r) = \sum_{r=1}^d \left(\sum_{k,l=1}^d (\mathbf{c}_k/\mathbf{c}_l)^{\gamma+\pi_r} \right) = \sum_{k,l=1}^d (\mathbf{c}_k/\mathbf{c}_l)^\gamma \left(\sum_{r=1}^d (\mathbf{c}_k/\mathbf{c}_l)^{\pi_r} \right),$$

and observe that the last sum is zero by orthogonality if $k \neq l$, while it is d if $k = l$. This means that for each $j = 1, \dots d$,

$$\sum_{r=1}^d G_j(\gamma + \pi_r) = d^2 \qquad \text{for each } \gamma \in \mathbb{Z}^d, \tag{7}$$

which then implies

$$\sum_{r=1}^{d} G(\gamma+\pi_r) = d^3 \qquad \text{for each } \gamma \in \mathbb{Z}^d. \tag{8}$$

In a similar fashion we can turn the unbiasedness relations also to linear constraints on the Fourier side. Let $\mathbf{u}/\mathbf{v} = (z_1, z_2 \dots, z_d) \in \mathbb{T}^d$ be the coordinate-wise quotient of any two columns from two *different* matrices from $H_1, \dots H_d$. Then $\mathbf{u}$ and $\mathbf{v}$ are unbiased, which means that

$$0 = |\sum_r z_r|^2 - d = \sum_{r\neq t} z_r/z_t. \tag{9}$$

Using this we can write

(10)

$$\sum_{r\neq t} F(\gamma+\pi_r-\pi_t) - \sum_{r\neq t} G(\gamma+\pi_r-\pi_t) = \sum_{\mathbf{u},\mathbf{v}} (\mathbf{u}/\mathbf{v})^\gamma \left(\sum_{r\neq t} (\mathbf{u}/\mathbf{v})^{\pi_r-\pi_t} \right) = 0,$$

where the summation on $\mathbf{u}, \mathbf{v}$ goes for all pairs of columns from *different* matrices, and the last equality is satisfied because each inner sum is zero by (9). Also, by (8) we have $dG(\gamma) + \sum_{r\neq t} G(\gamma+\pi_r-\pi_t) = d^4$, and we can use this to rewrite (10) as

$$dG(\gamma) + \sum_{r\neq t} F(\gamma+\pi_r-\pi_t) = d^4, \tag{11}$$

which is somewhat more convenient than (10).

We also have some further trivial constraints on F and G. Namely,

$$F(0) = d^4, \quad G(0) = d^3, \qquad \text{and} \tag{12}$$

$$0 \le F(\gamma) \le d^4, \quad 0 \le G(\gamma) \le d^3, \quad \text{for each } \gamma \in \mathbb{Z}^d. \tag{13}$$

Also, by the Cauchy-Schwartz inequality we have

$$F(\gamma) \le dG(\gamma), \qquad \text{for each } \gamma \in \mathbb{Z}^d. \tag{14}$$

Note that the linear constraints (8), (11), (12), (13), (14) put severe restrictions on the functions F and G. In fact, it turns out that *all* the structural results on complete systems of MUHs in dimensions 2, 3, 4, 5 follow from these constraints. These structural results are not new (cf. [5]) but nevertheless we list here the two most important ones as an illustration of the power of this Fourier approach. The first one is a celebrated theorem of Haagerup [10] which gives a full classification of complex Hadamard matrices of order 5. In the original paper [10] the author combines several clever ideas with lengthy calculations to

derive the result, whereas it follows almost for free from the formalism above.

Proposition 2.1. *Any complex Hadamard matrix of order 5 is equivalent to the Fourier matrix F_5, given by $F_5(j,k) = \omega^{(j-1)(k-1)}$, $(j,k = 1,\dots,5)$, where $\omega = e^{2i\pi/5}$.*

Proof. Let H_1 be a complex Hadamard matrix of order 5. Then the function $G_1(\gamma) = |\hat{H}_1(\gamma)|^2$ satisfies equation (7) for all $\gamma \in \mathbb{Z}^5$. Now, regard each $G_1(\gamma)$ as a *variable* as γ ranges through the following set: $\Gamma = \{\gamma = (\gamma_1, \dots \gamma_5) \in \mathbb{Z}^5 : |\gamma_1| + \cdots + |\gamma_5| \leq 10\}$. (We remark that it is possible to reduce the number of variables considerably due to permutation equivalences. However, it does not change the essence of the forthcoming argument, only makes the computations much quicker). Let $\rho = (5, -5, 0, 0, 0) \in \mathbb{Z}^5$. Set the following linear programming problem: minimize $G_1(\rho)$ subject to the conditions (7), and $G_1(0) = 25$, and $0 \leq G_1(\gamma) \leq 25$ for all $\gamma \in \Gamma$. A short computer code testifies that the solution to this linear programming problem is $G_1(\rho) \geq 25$, which actually implies $G_1(\rho) = 25$. And the same holds for any permutation of ρ.

Also, we may assume without loss of generality that H_1 is normalized (i.e. its first row and column are made up of 1s), and then the information above implies that all other entries of H_1 are 5th roots of unity. It is then trivial to check that there is only one way (up to equivalence) to build up a complex Hadamard matrix from 5th roots of unity, namely the matrix F_5. □

We remark here that all the linear programming problems mentioned in this paper have rational coefficients, so no numerical errors are encountered, and each result is certifiable (by hand, if necessary). Let us also remark that Proposition 2.1 is the only *non-trivial* result concerning MUHs and MUBs in dimensions $d \leq 5$. The classification of complex Hamamard matrices and MUBs is more or less trivial for $d = 2, 3, 4$ due to the geometry of complex unit vectors. We give here the essence of this classification (for full details see [5]).

Proposition 2.2. *In any normalized complete system of MUHs in dimension $d = 3, 4, 5$ all entries of the matrices are dth roots of unity. For $d = 2$ all entries are 4th roots of unity.*

Proof. The proof of this statement is similar to that of Proposition 2.1. Let $d = 3, 4, 5$. Assume $H_1, \dots H_d$ is a normalized complete system of MUHs. Then the functions F and G must satisfy the linear constraints (8), (11), (12), (13), (14). Regarding each $F(\gamma)$ and $G(\gamma)$ as a non-negative variable (as γ ranges through a sufficiently large cube around

the origin in $\mathbb{Z}^d$), a short linear programming code testifies that under these conditions $F(\rho) = d^4$ for all such $\rho \in \mathbb{Z}^d$ which is a permutation of $(d, -d, 0, \dots, 0)$. This means that all entries in all of the matrices must be dth roots of unity. The proof is analogous for $d = 2$ except that in this case we can only conclude $F(4, -4) = 16$, so that the matrices contain 4th roots of unity. □

Let us make a remark here about $d = 4$. In this case it is *not true* that all normalized Hadamard matrices must be composed of 4th roots of unity. However, it is true that a complete system of MUHs must be composed of such. This phenomenon shows up very clearly in our linear programming codes. Writing the constraints (7) on $G_1(\gamma)$, and $G_1(0) = 16$, and $0 \le G_1(\gamma) \le 16$ does not enable us to conclude that $G_1(\rho) = 16$ with ρ being a permutation of $(4, -4, 0, 0)$. However, writing all the constraints (8), (11), (12), (13), (14) on the functions F and G we can indeed conclude that $F(\rho) = 4G(\rho) = 256$.

We end this section with a few remarks concerning $d = 6$. If we could similarly conclude that

$$F(\rho) = 6^4 \qquad \text{for all } \rho \text{ being a permutation of } (6, -6, 0, 0, 0, 0) \tag{15}$$

then it would mean that a complete system of normalized MUHs in dimension 6 can only be composed of 6th roots of unity. Such a structural information would be wonderful, as it is proven in [3] that no such complete system of MUHs exists. Therefore, we could conclude that a complete system of MUHs does not exist at all. Unfortunately, the constraints (8), (11), (12), (13), (14) do not seem to imply (15). At least, we have run a linear programming code with γ ranging through as large a cube as possible (due to computational limitations), and could not conclude (15). Nevertheless, our main strategy for future research in dimension 6 must be as follows: using the linear constraints on F and G try to establish some structural information on the vectors appearing in a hypothetical complete system of MUHs, and then show by other means (e.g. a brute force computer search) that such constraints cannot be satisfied. We formulate here one conjecture which could be crucial in proving the non-existence of a complete system of MUHs in dimension 6.

Conjecture 2.3. *Let H_1 be any complex Hadamard matrix of order 6, not equivalent to the isolated matrix S_6 (cf. [21] for the matrix S_6). Let ρ be any permutation of the vector $(1, 1, 1, -1, -1, -1)$. Then $g_1(\rho) = 0$ for the function g_1 defined in (1).*

This conjecture is supported heavily by numerical data. We have tried hundreds of matrices randomly from each known family of complex Hadamard matrices of order 6 (including numerically given matrices from the most recent 4-parameter family [20]). Currently we cannot prove this conjecture, but in Section 3 we will show an example of how it could be used in the proof of non-existence results (cf. Remark 3.4).

3. Non-existence results

We now turn to non-existence results, namely that complete systems of MUHs with certain properties do not exist. The first of these, which we regard as the main result of the paper, is that any pair of *real* unbiased Hadamard matrices cannot be part of a complete system of MUHs. In fact, we prove the following stronger statement.

Theorem 3.1. *Let $H_1, \dots H_d$ be a complete system of MUHs such that H_1 is a real Hadamard matrix. Then any column vector $\mathbf{v} = (v_1, \dots, v_d)$ of the other matrices $H_2, \dots H_d$ satisfies that $\sum_{k=1}^d v_k^2 = 0$.*

Proof. Let $0 \neq \rho = (r_1, \dots, r_d) \in \mathbb{Z}^d$ be such that $\sum_{k=1}^d r_k = 0$ and $\sum_{k=1}^d |r_k| \leq 4$. There are five types of these vectors (up to permutation): $(1, -1, 0, \dots, 0)$, $(2, -2, 0, \dots, 0)$, $(2, -1, -1, 0, \dots, 0)$, $(-2, 1, 1, 0, \dots, 0)$, and $(1, 1, -1, -1, 0, \dots 0)$. Then, Theorem 8 in [2] (or Corollary 2.4 in [18]) shows that the function f defined in (5) satisfies

$$f(\rho) = 0 \tag{16}$$

for all these vectors ρ.

Let $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_{d^2}$ denote the column vectors appearing in the system $H_1, \dots H_d$. For each $\gamma \in \mathbb{Z}^d$ let

$$\mathbf{v}(\gamma) = (\mathbf{c}_1^\gamma, \dots \mathbf{c}_{d^2}^\gamma) \in \mathbb{T}^{d^2} \tag{17}$$

for $k = 1, \dots d$. Consider the vectors $\gamma_k = (0, \dots 0, 2, 0, \dots 0) \in \mathbb{Z}^d$ with the 2 appearing in position k. Finally, consider the vector $\mathbf{w} = \sum_{k=1}^d \mathbf{v}(\gamma_k)$, and let us evaluate $\|\mathbf{w}\|^2$. On the one hand, the vectors $\mathbf{v}(\gamma_k)$ are all orthogonal to each other by (16), and they all have length $\|\mathbf{v}(\gamma_k)\|^2 = d^2$, and hence $\|\mathbf{w}\|^2 = d^3$. On the other hand *we know* the first d coordinates of $\mathbf{w}$. Each $\mathbf{v}(\gamma_k)$ has first d coordinates equal to 1, because H_1 is a real Hadamard matrix. Therefore the first d coordinates of $\mathbf{w}$ are all equal to d. Therefore, $\|\mathbf{w}\|^2 \geq d^3$ on account of the first d coordinates. Hence, all other coordinates of $\mathbf{w}$ must be zero, which is exactly the statement of the theorem. □

Theorem 3.1 implies immediately the following corollary.

Corollary 3.2. *Let $H_1, \dots H_d$ be a complete system of MUHs such that H_1 is a real Hadamard matrix. Then there is no further purely real column in any of the matrices $H_2, \dots, H_d$. In particular, it is impossible to have two real Hadamard matrices in a complete set of MUHs.*

This statement is sharp in the sense that for $d = 2, 4$ the complete systems of MUHs are known to contain *one* real Hadamard matrix. Also, in several dimensions $d = 4n^2$ pairs (and even larger systems) of real unbiased Hadamard matrices are known to exist [4, 11], so that the corollary above is meaningful and non-trivial.

Our next result is a new proof of the fact in dimension 6 the Fourier matrix F_6 cannot be part of a complete system of MUHs. This result is well-known, but the only proof we are aware of uses some computer algebra, while we present an easy conceptual proof here.

Proposition 3.3. *There exists no complete system of MUHs in dimension 6 which contains the Fourier matrix F_6.*

Proof. Assume by contradiction that such a system $H_1, \dots H_6$ exists, and assume $H_1 = F_6$. Consider the vectors $\gamma_1 = (1, 1, 1, 0, 0, 1)$, $\gamma_2 = (0, 0, 1, 1, 1, 1)$, $\gamma_3 = (1, 1, 0, 1, 1, 0)$, $\gamma_4 = (0, 1, 0, 1, 0, 2)$, $\gamma_5 = (1, 0, 0, 0, 1, 2)$, and $\gamma_6 = (0, 1, 0, 0, 2, 1)$, and consider the corresponding vectors $\mathbf{v}(\gamma_k)$ defined in (17), and let $\mathbf{w} = \sum_{k=1}^{6} \mathbf{v}(\gamma_k)$. All the vectors $\mathbf{v}(\gamma_k)$ are orthogonal to each other by (16), therefore $\|\mathbf{w}\|^2 = 216$. On the other hand, we know the first 6 coordinates of $\mathbf{w}$. It is easy to calculate that each of these coordinates has modulus 6, and therefore $\|\mathbf{w}\|^2 \geq 216$ on account of the first 6 coordinates. This implies that all the other coordinates of $\mathbf{w}$ must be zero. This yields a polynomial identity for the coordinates of any column vector appearing in the matrices $H_2, \dots, H_6$. Instead of using this identity directly, however, we observe that the same argument applies to the vectors $\gamma_1, \dots \gamma_5$ and $\gamma_6' = (2, 0, 0, 1, 0, 1)$, and $\mathbf{w}' = \mathbf{v}(\gamma_6') + \sum_{k=1}^{5} \mathbf{v}(\gamma_k)$. By considering the difference $\mathbf{w} - \mathbf{w}'$ we conclude that $\mathbf{v}(\gamma_6)$ and $\mathbf{v}(\gamma_6')$ must coincide in the last 30 coordinates. That is, if $(z_1, \dots, z_6)$ is any column vector in the matrices $H_2, \dots H_6$ then $z_2 z_5^2 z_6 = z_1^2 z_4 z_6$, and hence $z_2 z_5^2 = z_1^2 z_4$. Furthermore, one can permute the coordinates of γ_k in a cyclic manner, and the argument remains unchanged, yielding this time $z_5 z_2^2 = z_4^2 z_1$. Dividing these two equations finally gives $z_5/z_2 = z_1/z_4$ for each of the last 30 vectors in our complete system of MUHs. This means, by definition, that the last 30 coordinates of the vectors $\mathbf{v}(0, -1, 0, 0, 1, 0)$ and

$\mathbf{v}(1,0,0,-1,0,0)$ coincide. But this is a contradiction, because these vectors should be orthogonal to each other by (16). □

Remark 3.4. Finally, we discuss informally a non-existence result in which we use Conjecture 2.3 in the proof. Nevertheless, the result itself is not "conditional" because it was proved earlier in [13] by a massive computer search after a discretization scheme. The argument we present here is much more elegant though, and shows a possible way forward in proving the non-existence of complete systems of MUHs in dimension 6.

We claim that there exists no complete system $H_1, \dots, H_6$ of MUHs in dimension 6 which contains any of the matrices $F_6(a,b)$ of the Fourier family (cf. [21] for the Fourier family $F_6(a,b)$). We sketch the proof here, on the condition that Conjecture 2.3 is valid.

First, note that it is equivalent to prove the statement for the transposed family $F_6^T(a,b)$. To see this, assume in general that $H_1, \dots, H_6$ is a complete system of MUHs, and consider the extended system $H_1, \dots, H_6, \sqrt{d}I$ (where I is the identity matrix). Multiplying everything from the left by $\frac{1}{\sqrt{d}}H_1^*$ we see that $\sqrt{d}I, \frac{1}{\sqrt{d}}H_1^*H_2, \dots \frac{1}{\sqrt{d}}H_1^*H_6, H_1^*$ is also a complete system of MUHs. Therefore, H_1 can be part of a complete system of MUHs if and only if H_1^* can. Then conjugating each column in all the matrices we see that H_1^* can be part of a complete system of MUHs if and only if H_1^T can. The significance of this fact is that the transposed family $F_6^T(a,b)$ is technically easier to handle because each member of the family contains the three column vectors $\mathbf{c}_1 = (1,1,1,1,1,1)$, $\mathbf{c}_2 = (1,\omega,\omega^2,1,\omega,\omega^2)$ and $\mathbf{c}_3 = (1,\omega^2,\omega,1,\omega^2,\omega)$, where $\omega = e^{2i\pi/3}$.

Also, it is well-known (see [7]) that a complex Hadamard matrix equivalent to S_6 cannot be part of a complete system of MUHs (in fact, it cannot even be part of a pair of MUHs), so that we can assume without loss of generality that none of $H_1, \dots H_6$ are not equivalent to S_6. The significance of this fact is that now Conjecture 2.3 (if true) can be invoked.

Assume now, by contradiction, that $H_1 = F_6^T(a,b), H_2, \dots, H_6$ is a complete system of MUHs. One can make a clever selection of vectors in $\mathbb{Z}^6$ such that the same argument as in Proposition 3.3 can be used. Namely, let
$\gamma_1 = (0,0,0,0,0,0)$, $\gamma_2 = (0,0,1,-1,-1,1)$, $\gamma_3 = (0,0,1,0,0,-1)$,
$\gamma_4 = (0,0,2,-1,-1,0)$, $\gamma_5 = (0,1,0,0,-1,0)$, $\gamma_6 = 1(0,1,1,0,-1,-1)$,
$\gamma_7 = (1,0,0,-1,0,0)$, $\gamma_8 = (1,0,1,-1,0,-1)$, $\gamma_9 = (1,1,0,-1,-1,0)$,
$\gamma_{10} = (1,1,1,-1,-1,-1)$, $\gamma_{11} = (1,-1,1,0,-1,0)$, $\gamma_{12} = (1,0,1,0,-2,0)$,

while let $\gamma'_{11} = (-1, 1, 1, -1, 0, 0)$, $\gamma'_{12} = (0, 1, 1, -2, 0, 0)$. For the system $\gamma_1, , \ldots, \gamma_{10}, \gamma_{11}, \gamma_{12}$ all the vectors $\mathbf{v}(\gamma_k)$ are orthogonal to each other by either (16) or by Conjecture 2.3, so that $\|\mathbf{w}\|^2 = |\sum_{k=1}^{12} \mathbf{v}(\gamma_k)|^2 = 432$. (This is where we use Conjecture 2.3.) On the other hand, three coordinates of $\mathbf{w}$ corresponding to the columns $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3$ are known exactly, and they happen to be 12 (the vectors γ_k were chosen accordingly). As in Proposition 3.3 this leads us to conclude that all the other 33 coordinates of $\mathbf{w}$ must be zero. The same is true for the vector $\mathbf{w}'$ generated by the system $\gamma_1, , \ldots, \gamma_{10}, \gamma'_{11}, \gamma'_{12}$. By considering the difference $\mathbf{w} - \mathbf{w}'$ we conclude that if $(z_1, \ldots, z_6)$ is any column (different from $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3$) in our complete system of MUHs then the identity $\frac{z_1 z_3}{z_2 z_5} + \frac{z_1 z_3}{z_5^2} = \frac{z_2 z_3}{z_1 z_4} + \frac{z_2 z_3}{z_4^2}$ must hold. After simplifying by z_3 and conjugating the equation we get $z_1 z_4 (z_1 + z_4) = z_2 z_5 (z_2 + z_5)$. By applying a cyclic permutation to the coordinates of the selected γ_k's we can derive in the same manner that $z_2 z_5 (z_2 + z_5) = z_3 z_6 (z_3 + z_6)$. Furthermore, 30 of these columns $(z_1, \ldots, z_6)$ – the ones contained in $H_2, \ldots, H_6$ – must be unbiased to $\mathbf{c}_1 = (1, 1, 1, 1, 1, 1)$, and hence they must satisfy $|z_1 + \cdots + z_6| = \sqrt{6}$. It is not hard to show that there are exactly 56 vectors $(z_1, \ldots, z_6)$ satisfying all these constraints (one can write up the solutions exactly). However, one can form pairs among these 56 vectors such that in any pair the two vectors are neither orthogonal nor unbiased to each other. Therefore, our system can contain at most one vector from each pair, i.e. at most 28 vectors, a contradiction. □

We believe that the proof of the non-existence of complete systems of MUHs in dimension 6 will hinge on Conjecture 2.3. The reason is that it introduces yet another non-trivial linear constraint on the function G, and these constraints will ultimately lead to a contradiction (maybe indirectly, as in Proposition 3.3). Therefore, we would be very interested to see a proof of Conjecture 2.3.

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] 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.

[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] D. Best & H. Kharaghani, *Unbiased complex Hadamard matrices and bases.* Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences, **2** (2010), 199–209.

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

[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] 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] 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

[10] U. Haagerup, *Orthogonal 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.

[11] W. Holzmann, H. Kharaghani & W. Orrick, *On the real unbiased Hadamard matrices.* Contemporary Mathematics, Combinatorics and Graphs, Volume **531** (2010), 243-250.

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

[13] 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.

[14] B. R. Karlsson, *H_2-reducible complex Hadamard matrices of order 6.* Linear Algebra and its Applications, Volume 434, Issue 1, 1 January 2011, Pages 239246.

[15] 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

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

[17] N. LeCompte, W. J. Martin & W. Owens, *On the equivalence between real mutually unbiased bases and a certain class of association schemes.* European Journal of Combinatorics, Volume **31**, Issue 6, August, (2010), 1499-1512.

[18] M. Matolcsi, *A Fourier analytic approach to the problem of mutually unbiased bases.* Stud. Sci. Math. Hung., to appear.

[19] P. Raynal, X. Lü, & B.-G. Englert, *Mutually unbiased bases in six dimensions: The four most distant bases.* Phys. Rev. A **83** (2011) 062303.

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

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

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

[23] P. Wocjan & T. Beth, *New construction of mutually unbiased bases in square dimensions.* Quantum Inf. Comput. **5** (2005), 93-101.
[24] W. K. Wootters & B. D. Fields, *Optimal state-determination by mutually unbiased measurements.* Ann. Physics **191** (1989), 363–381.
[25] 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

I.Z. R.: Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences POB 127 H-1364 Budapest, Hungary Tel: (+361) 483-8328, Fax: (+361) 483-8333
E-mail address: ruzsa@renyi.hu

M. W.: Budapest University of Technology and Economics (BME), H-1111, Egry J. u. 1, Budapest, Hungary Tel: (+361) 463-2324
E-mail address: mweiner@renyi.hu