THE PROBLEM OF MUTUALLY UNBIASED BASES: A NEW APPROACH

MÁTÉ MATOLCSI AND COAUTHORS...

Abstract. We outline a new approach to the MUB-problem, based on a Fourier analytic method in additive combinatorics.

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

1. Introduction

We introduce a very promising approach to the MUB-problem. However, currently i am somewhat stuck. I will describe why.

Recall that two orthonormal bases of $\mathbb{C}^d$, $\mathcal{A} = \{\mathbf{e}_1, \dots, \mathbf{e}_d\}$ and $\mathcal{B} = \{\mathbf{f}_1, \dots, \mathbf{f}_d\}$ are said to be *unbiased* if, for every $1 \leq j, k \leq d$, $|\langle \mathbf{e}_j, \mathbf{f}_k \rangle| = \frac{1}{\sqrt{d}}$. A family $\mathcal{B}_0, \dots \mathcal{B}_m$ of orthonormal bases is said to be *(pairwise) mutually unbiased* if every two of them are unbiased. It is well-known (see e.g. [2, 5, 23]) that the number of mutually unbiased bases (MUBs) in $\mathbb{C}^d$ cannot exceed $d+1$. It is also known that $d+1$ such bases can be constructed if the dimension d is a prime or a prime power (*see e.g.* [2, 11, 12, 13, 15, 17, 23]). Such a set of $d+1$ MUBs in dimension d is called a *complete set*. 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. Thus, the first case where the largest number of mutually unbiased bases is unknown is $d = 6$:

Problem 1.1.
What is the maximal number of pairwise mutually unbiased bases in $\mathbb{C}^6$?

Although this famous open problem has received considerable attention over the past few years ([5, 7, 8, 16, 19, 21]), it remains wide open. Since $6 = 2 \times 3$, we know that there are at least 3 mutually unbiased bases in $\mathbb{C}^6$ (see also [24, 16] for *infinite families* of MUB-triplets), but

M. Matolcsi was supported by OTKA Grant No. K77748.

so far tentative numerical evidence [7, 8, 10, 24] suggests that there are no more than 3, a fact apparently first conjectured by Zauner [24].

Conjecture 1.2.
The maximal number of pairwise mutually unbiased bases in $\mathbb{C}^6$ *is 3.*

One reason for the slow progress is 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

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

i.e. the k-th row 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 linear in the first variable and conjugate-linear in the second. Note also that for convenience of computer programming we use the unconventional definition that the *rows* of the matrices correspond to the vectors of the bases.) 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 clear that the existence of a family of mutually unbiased bases $\mathcal{B}_0, \dots, \mathcal{B}_m$ is thus 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*.

In particular, the existence of 7 MUBs $\mathcal{B}_0, \mathcal{B}_1, \dots \mathcal{B}_6$ in dimension 6 is equivalent to the existence of 6 mutually unbiased Hadamard matrices $H_1, H_2, \dots H_6$ (we dropped the $'$ from the notation). Therefore, in an attempt to prove that no collection of 7 MUBs exist in dimension 6 it is enough to prove that no six mutually unbiased Hadamard matrices exist. This will be the core of our argument in this note.

A complete classification of complex Hadamard matrices, however, is only available up to dimension 5 (*see* [14]) which allows for a complete classification of MUBs (*see* [9]). The classification in dimension 6 is still out of reach despite recent efforts [3, 19, 21]. This is one of the reasons for Problem 1.1 to be difficult.

In this paper we outline a Fourier analytic approach, borrowed from additive combinatorics. We will include all the basic definitions and ideas as well as some preliminary results.

2. Notation

Assume by contradiction that a family $H_1, \dots H_6$ of 6 mutually unbiased complex Hadamard matrices exists. Then all entries of all matrices are of modulus 1, and the rows (and thus the columns) within a matrix are complex orthogonal, and we have the unbiased condition: for any two rows u, v coming from different matrices we have $|\langle u, v\rangle| = \sqrt{6}$. (Recall that for the purposes of this note the *rows* of the matrices correspond to the vectors of the bases.)

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 column of all other matrices are 1's (i.e. we assume that all appearing rows have first coordinate 1, and the first row in H_1 consists of 1's. This is just 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 row $(1, e^{2\pi i\rho_1}, \dots, e^{2\pi i\rho_5})$ the vector $(0, \rho_1, \dots, \rho_5) \in \mathbb{T}^6$, the real 6-dimensional torus, $\mathbb{T}^6 = [-1/2, 1/2)^6$. Also, note that the first coordinate always automatically becomes 0, because each complex row starts with coordinate 1. Therefore we make the more useful association that $\mathbf{r} = (1, e^{2\pi i\rho_1}, \dots, e^{2\pi i\rho_5})$ is represented by $\mathbf{u} = (\rho_1, \dots \rho_5) \in \mathbb{T}^5$, the 5-dimensional torus. There are altogether 36 row vectors in the Hadamard matrices $H_1, \dots H_6$, and we will denote the associated vectors in $\mathbb{T}^5$ by $b_1, \dots b_{36}$ (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 $b_1 = (0, 0, 0, 0, 0)$, corresponding to the first row of H_1.)

Two rows $\mathbf{r_1} = (1, e^{2\pi i\rho_1}, \dots, e^{2\pi i\rho_5})$ and $\mathbf{r_2} = (1, e^{2\pi i\mu_1}, \dots, e^{2\pi i\mu_5})$ are orthogonal if and only if $1 + \sum_{j=1}^{5} e^{2\pi i(\rho_j - \mu_j)} = 0$, and they are unbiased if and only if $|1 + \sum_{j=1}^{5} e^{2\pi i(\rho_j - \mu_j)}| = \sqrt{6}$. Therefore it is natural to introduce the following definitions.

Definition 2.1. *Let ORT denote the set of vectors* $(\alpha_1, \dots \alpha_5) \in \mathbb{T}^5$, *in the 5-dimensional torus, such that* $1 + \sum_{j=1}^{5} e^{2\pi i\alpha_j} = 0$. *Also, let UB denote the set of vectors* $(\alpha_1, \dots \alpha_5) \in \mathbb{T}^5$, *such that* $|1 + \sum_{j=1}^{5} e^{2\pi i\alpha_j}| = \sqrt{6}$. *Let us also define* $A = (ORT \cup UB)^c$.

Therefore we conclude that the vectors $b_1, \dots b_{36}$ 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 $\mathbb{T}^5$) lies in $A^c \cup \{0\}$.

This is a standard situation in additive combinatorics. There is a compact Abelian group G ($= \mathbb{T}^5$ in this case) and a symmetric 'forbidden' set $A \subset G$, and we want to find as many points $B = \{b_1, \dots b_m\}$ in G as possible, so that all the differences $b_j - b_k \in A^c \cup \{0\}$ (so that all differences avoid the forbidden set A). How many such points can we find??? If we prove that $m < 36$, then we have shown that a full set of 6 unbiased complex Hadamards (and correspondingly, 7 MUBs) cannot exist.

3. The Delsarte method

In this section we describe a general method to tackle such problems. It was first introduced by Delsarte in connection with binary codes with prescribed Hamming distance. But it works in a very general manner, too (i should look up some proper references as to where this method is described in general. If at all...).

As a preliminary remark we note that the dual group of $G = \mathbb{T}^5$ is $\hat{G} = \mathbb{Z}^5$. And the action of a character $\gamma \in \mathbb{Z}^5$ on a point $x \in \mathbb{T}^5$ 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 now turn to Delsarte's method. We are looking for a 'witness' function $h : G \to \mathbb{R}$ with the following properties.

– $h(x) = h(-x)$, and h is 'nice enough' (continuity, smoothness, etc., not much is needed; we will see that the point is that the inverse Fourier formula should work for h; see below).

- $h(x) \leq 0$ for all $x \in A^c$
- $\hat{h}(\gamma) \geq 0$ for all $\gamma \in \hat{G}$
- $\hat{h}(0) = 1$ (this is just normalization, which is not really important).

Given such a function h 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 $|B| \leq h(0)$. The reason is the following:

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) 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

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

And comparing the two estimates (2), (3) we get that $|B| \leq h(0)$.

Let us see whether we can find a good witness function in our situation. At first sight it looks gloomy because we have no understanding whatsoever of the geometry of the sets ORT and UB. However, it turns out that it's not such a big problem. Define

$$h(x) = |1 + \sum_{j=1}^{5} e^{2\pi i x_j}|^2 \left(|1 + \sum_{j=1}^{5} e^{2\pi i x_j}|^2 - 6 \right). \tag{4}$$

Exercise 3.1. *Check that h satisfies all requirements, except that h is not normalized. In fact $\hat{h}(0) = 30$ and $h(0) = 1080$, so that we conclude that $|B| \leq 36$. This works in all dimensions d and we always get $B \leq d^2$. This gives an elegant new proof of the fact that there are at most $d + 1$ MUBs in dimension d.*

Now, the question is: can we do better than this in dimension 6??? Can we cook up a better function than h above? For a while i thought we can, because the geometry of ORT and UB really depends on the dimension. So maybe there is something particular about them when $d = 6$ is not a prime power. However these hopes are dashed in the next section.

Remark 3.2. If we follow the proof, there is a glimmer of hope. If either of the two estimates (2), (3) are strict, than we are done, and we have proved that no maximal collection of MUBs can exist. Now, it is trivial to see that (3) automatically becomes an equality for the h above (because h is zero on ORT and UB). However, inequality (2) becomes an equality *only if* $|\hat{B}(\gamma)|^2\hat{h}(\gamma) = 0$ for all $\gamma \neq 0$. These are non-trivial conditions. It could be possible to complete the proof by

somehow showing that these values cannot be simultaneously zero in dimension 6. (Of course these non-trivial conditions also exist in other dimensions, and it is illuminating to see that they are indeed satisfied in prime-power dimensions, say $d = 2, 3, 4, 5$.)

4. A dual witness: h cannot be beaten

In this section i describe the bad news, and the reason why i feel stuck.

Let us check the proof above, and see when and why it works. It is easy to see that $|\hat{B}(\gamma)|^2 = \sum_{j,k} \gamma(b_j - b_k) = \sum_{j,k} e^{2\pi i \langle \gamma, (b_j - b_k) \rangle} = \sum_y \lambda_y e^{2\pi i \langle \gamma, y \rangle}$ has the following essential properties.

• it is a finite exponential sum $\sum_y \lambda_y e^{2\pi i \langle \gamma, y \rangle}$, which is nonnegative for all $\gamma \in \mathbb{Z}^5$, and the exponents $y \in A^c \cup \{0\} = ORT \cup UB \cup \{0\}$.

• the coefficient λ_y corresponding to a fixed exponent y is a nonnegative integer (it is the number of ways of writing y as a difference of two elements of B).

• the sum of the coefficients $\sum_y \lambda_y = |B|^2$.

• $\lambda_0 = |B|$.

Let us relax the second condition and require only that the coefficients are nonnegative. If a function $f : \mathbb{Z}^5 \to \mathbb{R}_+$, $f(\gamma) = \sum_y \lambda_y e^{2\pi i \langle \gamma, y \rangle}$ satisfies the first and second conditions (the second being relaxed) then we will call it a pseudo-MUB. It is trivial that equations (1), (2),(3) can be generalized if we use $f(\gamma) = \sum_y \lambda_y e^{2\pi i \langle \gamma, y \rangle}$ instead of $|\hat{B}(\gamma)|^2$. And the conclusion becomes

$$\frac{\sum_y \lambda_y}{\lambda_0} \leq \frac{h(0)}{\hat{h}(0)}. \tag{5}$$

In particular, if we find a 'dual-witness' $f(\gamma) = \sum_y \lambda_y e^{2\pi i \langle \gamma, y \rangle}$ such that $\lambda(0) = 36$ and $\sum_y \lambda_y = 36^2$ (just what the case is with a hypothetical complete set of MUBs B), then we can call it a pseudo-complete-MUB-system. Such a dual-witness f would also show that our witness h above is best possible.

And the bad news is that such functions f exist.

Exercise 4.1. *Take all the vectors in ORT and UB which contain 24th roots of unity only. Use these as exponents y, and construct a dual-witness f such that $\lambda_0 = 36$ and $\sum_y \lambda_y = 36^2$. Use linear programming, as all the conditions are linear. This is a somewhat tougher exercise...*

This means that there exists a pseudo-complete-MUB-system (in short let's call it pseudo-MUB-6), consisting of 24th roots of unity. And it also means that the Delsarte method *alone* cannot prove the non-existence of a complete system of MUBs in dimension 6 (let's call it simply a MUB-6).

What else? I tried to see how unique those pseudo-MUBs f are. They are not unique at all, there are plenty of them. Say i take the vectors in ORT and UB with 48th roots of unity, but remove all those which contain purely 24th roots. And i use only the remaining vectors as exponents in f. You would think that i have removed an essential part of the possible exponents this way. But, unfortunately, there still exist dual witnesses satisfying all the properties.

The only way forward seems to be to somehow exploit that in a proper MUB-6 the coefficients of $|\hat{B}(\gamma)|^2$ are nonnegative *integers*. I have tried to find dual-witnesses with integer coefficients and 24th roots in the exponent-vectors, but they seem not to exist (i cannot claim it for certain, because my computer never finishes the calculations... but it does not find anything). But even if we prove, say, that dual witnesses with integer coefficients and 24th roots of unity do not exist, we are nowhere near the solution. Because we should not restrict ourselves to 24th roots of unity. The exponents can be any vectors in ORT and UB.

Any ideas?

References

[1] Y. Aharonov & B.-G. Englert, *The mean king's problem: Spin 1.* Z. Naturforsch. **56a**, (2001) 16.

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

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

[4] H. Bechmann-Pasquinucci & W. Tittel, *Quantum cryptography using larger alphabets.* Phys. Rev. A, **61** (2000), no. 6, 062308, 6 pp.

[5] 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.

[6] C. H. Bennett & G. Brassard, *Quantum cryptography: Public key distribution and coin tossing.* In Proceedings of the IEEE Intl. Conf. Computers, Systems, and Signal Processing, pages 175–179. IEEE, 1984.
[7] S. Brierley & S. Weigert, *Maximal sets of mutually unbiased quantum states in dimension six.* arXiv:0808.1614 (quant-ph).
[8] S. Brierley & S. Weigert, *Constructing Mutually Unbiased Bases in Dimension Six.* arXiv:0901.4051 (2009)
[9] S. Brierley, S. Weigert & I. Bengtsson, *All Mutually Unbiased Bases in Dimensions Two to Five* arXiv:0907.4097 (2009)
[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] M. Combescure *The mutually unbiased bases revisited.* Adventures in mathematical physics, 29–43, Contemp. Math., **447**, Amer. Math. Soc., Providence, RI, 2007.
[12] M. Combescure *Circulant matrices, Gauss sums and mutually unbiased bases I. The prime number case.* Available at `Arxiv:0710.5642v1.`
[13] M. Combescure *Circulant matrices, Gauss sums and mutually unbiased bases II. The prime power case.* Available at `Arxiv:0710.5643v1.`
[14] 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.
[15] I. D. Ivanovic, *Geometrical description of quantal state determination.* J. Phys. A **14** (1981), 3241.
[16] Ph. 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.
[17] A. Klappenecker & M. Rötteler *Constructions of Mutually Unbiased Bases.* Finite fields and applications, 137–144, Lecture Notes in Comput. Sci., **2948**, Springer, Berlin, 2004.
[18] C.W.H. Lam, L. H. Thiel & S. Swiercz, *The non-existence of finite projective planes of order 10.* Can. J. Math., Vol: XLI, (1989) 1117-1123.
[19] M. Matolcsi, F. Szöllősi, *Towards a classification of 6x6 complex Hadamard matrices.* Open Systems & Information Dynamics, **15**, Issue:2, (June 2008), 93-108.
[20] J. M. Renes, *Equiangular spherical codes in quantum cryptography.* Quantum Inf. Comput. **5** (2005), 81–92.
[21] A. J. Skinner, V. A. Newell, R. Sanchez, *Unbiased bases (Hadamards) for 6-level systems: Four ways from Fourier.* arXiv:0810.1761 (2008)
[22] R. F. Werner, *All teleportation and dense coding schemes. Quantum information and computation.* J. Phys. A, **34** (2001), 7081–7094.
[23] W. K. Wootters & B. D. Fields, *Optimal state-determination by mutually unbiased measurements.* Ann. Physics **191** (1989), 363–381.
[24] G. Zauner, *Quantendesigns Grundzüge einer nichtkommutativen Designtheorie.* PhD thesis, Universität Wien, 1999. (available at http://www.mat.univie.ac.at/∼neum/ms/zauner.pdf)
[25] Documentation of the results of [16]: http://www.math.bme.hu/∼matolcsi/angpubl.html

M. M.: Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences POB 127 H-1364 Budapest, Hungary Tel: (+361) 483-8302, Fax: (+361) 483-8333

E-mail address: matomate@renyi.hu