A RIGIDITY PROPERTY OF COMPLETE SYSTEMS OF MUTUALLY UNBIASED BASES

MÁTÉ MATOLCSI AND MIHÁLY WEINER

Abstract. Suppose that for some unit vectors \( b_1, \ldots, b_n \) in \( \mathbb{C}^d \) we have that for any \( j \neq k \) \( b_j \) is either orthogonal to \( b_k \) or \( |\langle b_j, b_k \rangle|^2 = 1/d \) (i.e. \( b_j \) and \( b_k \) are unbiased). We prove that if \( n = d(d+1) \), then these vectors necessarily form a complete system of mutually unbiased bases, that is, they can be arranged into \( d+1 \) orthonormal bases, all being mutually unbiased with respect to each other.

1. Introduction

The concept of mutually unbiased bases (MUBs) originates from quantum state tomography ([8]), and appears also in several protocols in quantum information theory ([12]). As such, the existence and explicit constructions of MUBs have been active areas of research in the past decades (see e.g. [7] for a recent comprehensive survey article).

Recall that two orthonormal bases in \( \mathbb{C}^d \), \( \mathcal{A} = \{ e_1, \ldots, e_d \} \) and \( \mathcal{B} = \{ f_1, \ldots, f_d \} \) are called unbiased if for every \( 1 \leq j, k \leq d \), \( |\langle e_j, f_k \rangle| = \frac{1}{\sqrt{d}} \).

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. If the dimension \( d \) is a prime-power, then the maximal number of MUBs is well-known to be \( d + 1 \) (see e.g. [8] [13] [1] [10]). It is also well-known that in any dimension \( d \) the maximal number of MUBs is at most \( d + 1 \) (see e.g. [13] [2] [11] [7]). For this reason, a set of \( d + 1 \) mutually unbiased bases is commonly called a complete system of MUBs. However, for any \( d \) which is not a prime-power, it is not known whether a complete system of MUBs exists (even for \( d = 6 \), despite considerable efforts [3] [1] [5] [9]).

M. Matolcsi was supported by NKFI grants K132097, K129335. M. Weiner was supported by the Bolyai Janos Fellowship of the Hungarian Academy of Sciences, the UNKP-20-5 New National Excellence Program of the Ministry for Innovation and Technology and by NKFI grants K132097, K124152 and KH129601.
In [2, Theorem 8] it is proved that unit vectors forming a complete system of MUBs, if they exist, must satisfy some extra algebraic relations. Furthermore, in [11, Theorem 2.2] the following result is proved: a collection of unit vectors in $\mathbb{C}^d$, all of which are orthogonal or unbiased to a fixed orthonormal basis, can consist of at most $d^2$ vectors. These two results raise the following very general and natural question: given a set of $d(d+1)$ unit vectors in $\mathbb{C}^d$ such that any two of them are either orthogonal or unbiased to each other, is it true that they necessarily form a complete system of MUBs? In this paper we answer this question in the affirmative, which can be viewed as a certain rigidity property of complete systems of MUB’s. This result is somewhat surprising, considering that as many as $(d-1)^2$ unit vectors in $\mathbb{C}^d$ can be given such that they are pairwise unbiased to each other. Indeed, consider a SIC-POVM (which conjecturally exists in any dimension) in $\mathbb{C}^{d-1}$, i.e. a collection of $(d-1)^2$ unit vectors in $\mathbb{C}^{d-1}$ such that any pair has inner product with absolute value $\frac{1}{\sqrt{d}}$. Append each vector with a coordinate 0 in the $d$th coordinate, and you obtain a collection of $(d-1)^2$ unit vectors in $\mathbb{C}^d$ which are pairwise unbiased to each other. One might expect that similar special constructions may yield $d(d+1)$ unit vectors in several different ways, such that they are all orthogonal or unbiased to each other, but Theorem 2.4 tells us that this is not the case.

2. FROM A SET OF VECTORS TO A COMPLETE SYSTEM OF MUBS

Suppose that $n = d(d+1)$ and $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{C}^d$ is a collection of unit vectors such that any two of them is either orthogonal or unbiased to each other, that is $|\langle \mathbf{b}_j, \mathbf{b}_k \rangle| = 0$ or $\frac{1}{\sqrt{d}}$ for any $j \neq k$. We will prove below (Theorem 2.4) that these vectors necessarily form a complete system of MUBs.

Consider the simple graph $G = (V, E)$ with vertex set $V = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ and edge set $E$ containing all (unordered) pairs of orthogonal vectors in $V$. In other words, we imagine that vectors $\mathbf{b}_j$ and $\mathbf{b}_k$ are connected by an edge if they are orthogonal to each other. Our aim is to prove that $G$ is a disjoint union of $d+1$ complete graphs, each containing $d$ vertices. This will prove that the vectors $\mathbf{b}_j$ can be grouped into $d+1$ orthonormal bases, all being mutually unbiased to each other. We shall begin by considering the number of edges in $G$. Note that if the vectors in $V$ form $d+1$ mutually unbiased bases, then the number of orthogonality relations (i.e. the number of edges in $G$) should be $(d+1)\binom{d}{2}$. 
The following is a well-known general fact, but we include it for the convenience of the reader.

**Lemma 2.1.** Suppose $A$ is a self-adjoint matrix of rank $r = \text{rk}(A)$. Then $(\text{Tr } A)^2 \leq r \text{Tr } (A^2)$ with equality holding if and only if $A$ is a multiple of a projection.

**Proof.** We may assume that the rank $r > 0$ (the case $r = 0$ implies $A = 0$, which is trivial). Let $P$ be the orthogonal projection onto the range space of $A$. Then $PA = A$ and $\text{Tr } (P^2) = \text{Tr } (P) = \text{rk}(P) = \text{rk}(A) = r$. Using the Cauchy-Schwarz inequality $|\text{Tr } (X^*Y)|^2 \leq \text{Tr } (X^*X)\text{Tr } (Y^*Y)$ we have

$$(\text{Tr } A)^2 = (\text{Tr } PA)^2 \leq \text{Tr } (P^2) \text{Tr } (A^2) = r \text{Tr } (A^2)$$

with equality holding if and only if $A$ and $P$ are parallel; i.e. when $A$ is a multiple of $P$. □

**Corollary 2.2.** The graph $G$ has at most $(d + 1)(\binom{d}{2})$ edges.

**Proof.** We will denote the number of edges by $|E|$. Consider the Gram matrix

$$K := (\langle b_j, b_k \rangle)_{\{j,k\}}$$

of the given vectors. The rank of $K$ is the dimension of the subspace spanned by the vectors $b_1, \ldots, b_n \in \mathbb{C}^d$ and hence $\text{rk}(K) \leq d$. Since these vectors are of unit length, the diagonal elements of $K$ are all equal to $1$ and thus $\text{Tr } (K) = n = d(d + 1)$. Moreover, as $K$ is self-adjoint (actually: positive semidefinite),

$$\text{Tr } (K^2) = \text{Tr } (K^*K) = \sum_{j,k} |K_{j,k}|^2 = \sum_{j,k} |\langle b_j, b_j \rangle|^2.$$  

In the above sum, we have 3 kind of terms. First, the ones with $j = k$, of which we have $n = d(d + 1)$ many. Second, the ones corresponding to orthogonal pairs of vectors; of these we have $2|E|$ – the factor of 2 needed because we considered $G$ to be undirected. Finally, we have the ones corresponding to unbiased pairs of vectors; of these we have $2 \left( \binom{n}{2} - |E| \right)$. So

$$\text{Tr } (K^2) = n \cdot 1 + 2|E| \cdot 0 + 2 \left( \binom{n}{2} - |E| \right) \cdot \frac{1}{d} = n + \frac{n(n-1)}{d} - \frac{2|E|}{d},$$

and hence by the previous lemma

$$n^2 \leq d \left( n + \frac{n(n-1)}{d} - \frac{2|E|}{d} \right).$$

Substituting $n = d(d + 1)$ and rearranging we get $|E| \leq \frac{d(d^2-1)}{2}$, which is the claimed bound. □
To completely determine $|E|$, we also need to bound it from below. This means bounding the number of non-orthogonal (i.e. unbiased) pairs from above. More concretely, we need to show that using the vectors $b_1, \ldots, b_n$, one can form at most \(\left(\frac{d+1}{2}\right)d^2\) unbiased pairs; i.e. exactly as many as we would have if these vectors were to form a complete system of MUBs.

To this end, for each $j \in \{1, \ldots, n\}$ consider $Q_j := |b_j\rangle\langle b_j|$, i.e. the orthogonal projection onto the one-dimensional subspace given by the vector $b_j$, and let $X_j = Q_j - \frac{1}{d}I$. Elementary computation shows that the Hilbert-Schmidt inner products satisfy

$$\langle X_j, X_k \rangle_{HS} = \text{Tr} \left( X_j^* X_k \right) = |\langle b_j, b_k \rangle|^2 - \frac{1}{d},$$

where $\langle \cdot, \cdot \rangle_{HS}$ denotes the usual Hilbert-Schmidt inner product on $M_d(\mathbb{C})$. We shall now apply the estimate of Lemma 2.1 to the Gram matrix $\tilde{K} := (\langle X_j, X_k \rangle_{HS})_{\{j,k\}}$

Note that $\tilde{K}$ has size $n \times n$.

**Lemma 2.3.** The graph $G$ has exactly $(d+1)\binom{d}{2}$ edges, and $\tilde{K}$ is an orthogonal projection of rank $d^2 - 1$.

**Proof.** Since $\text{Tr} \left( X_j \right) = \text{Tr} \left( Q_j - \frac{1}{d}I \right) = 1 - (d/d) = 0$ for all $j = 1, \ldots, n$, the span of $\{X_j | j = 1, \ldots, n\}$ is contained in the subspace of traceless $d \times d$ matrices; thus $\text{rk}(\tilde{K}) \leq d^2 - 1$. Moreover,

$$\text{Tr} \left( \tilde{K} \right) = \sum_j \left( |\langle b_j, b_j \rangle|^2 - \frac{1}{d} \right) = n \left( 1 - \frac{1}{d} \right)$$

and

$$\text{Tr} \left( \tilde{K}^2 \right) = \sum_{j,k} \left( |\langle b_j, b_k \rangle|^2 - \frac{1}{d} \right)^2 = n(1 - \frac{1}{d})^2 + 2|E|\frac{1}{d^2}$$

where we have used that by (1), the diagonal entries of $\tilde{K}$ are equal to $1 - 1/d$, the entries corresponding to orthogonal pairs are equal to $0 - 1/d = -1/d$ and the entries corresponding to unbiased pairs are equal to $1/d - 1/d = 0$. Taking into account $\text{rk}(\tilde{K}) \leq d^2 - 1$, the application of Lemma 2.1 to the Gram matrix $\tilde{K}$ gives

$$n^2(1 - \frac{1}{d})^2 \leq (d^2 - 1)(n(1 - \frac{1}{d})^2 + 2|E|\frac{1}{d^2}).$$

After substituting $n = d(d+1)$ and rearranging, we get $|E| \geq (d+1)\binom{d}{2}$. This, together with Corollary 2.2, proves that this inequality is
A RIGIDITY PROPERTY OF MUBS

actually an equality. Therefore, by the equality case of Lemma 2.1, the matrix $\tilde{K}$ is a multiple of a projection; $\tilde{K} = \lambda P$ for some scalar $\lambda$ and orthogonal projection $P$. Also, the inequality in (2) must also be an equality, which implies $\text{rk}(P) = \text{rk}(\tilde{K}) = d^2 - 1$. Therefore

$$n(1 - \frac{1}{d}) = \text{Tr}(\tilde{K}) = \text{Tr}(\lambda P) = \lambda(d^2 - 1),$$

implying that $\lambda = 1$ and hence that $\tilde{K} = P$. \hfill \Box$

Consider the $n \times n$ matrix $A := (d - 1)I - d \tilde{K}$. By what we know about the entries of $\tilde{K}$, it is easy to verify that

$$A_{j,k} = \begin{cases} 1, & \text{if } b_j \perp b_k, \\ 0, & \text{otherwise}; \end{cases}$$

i.e. $A$ is simply the adjacency matrix of $G$. Thus, by having established that $\tilde{K}$ is a rank $d^2 - 1$ projection, we can precisely determine the spectrum of the adjacency matrix $A$, or, as it is called in short, the spectrum of the graph $G$.

In general, the spectrum of a graph does not determine its isomorphism class. That is, there exist graphs which are not isomorphic, yet have the same spectrum (including multiplicities); a curious fact that was first noted more than half a century ago [6]. However, in this particular case, we can prove that $G$ must be a disjoint union of $(d + 1)$ complete graphs, each with $d$ vertices.

**Theorem 2.4.** Let $n = d(d + 1)$ and $b_1 \ldots b_n \in \mathbb{C}^d$ be a collection of unit vectors such that $|\langle b_j, b_k \rangle|^2$ is either 0 or $1/d$ for any $j \neq k$ (i.e. such that any two of them are either orthogonal or unbiased to each other). Then the vectors $b_1 \ldots b_n$ can be arranged into $d + 1$ orthogonal bases, all being mutually unbiased to each other.

**Proof.** The eigenvalues of the matrix $A = (d - 1)I - d \tilde{K}$, defined above, are $-1$ (with multiplicity $d^2 - 1$) and $d - 1$ (with multiplicity $n - d^2 + 1 = d + 1$). Let $1 \in \mathbb{C}^n$ denote the vector with entry 1 in each coordinate, and consider $h = \langle 1, A1 \rangle$. Due to the eigenvalues of $A$ we have $h \leq (d - 1)(1, 1) = (d - 1)d(d + 1)$, with equality only if $1$ is an eigenvector with eigenvalue $d - 1$. Furthermore, $h$ is the sum of entries in $A$, which equals to twice the number of edges in $G$ (each edge being counted twice by the symmetry of $A$). Therefore $h = |E| = (d - 1)d(d + 1)$. This implies that $1$ is an eigenvector with eigenvalue $d - 1$, which means that each vertex in $G$ has degree $d - 1$ (in other words, the graph $G$ is $d - 1$-regular).
It is also well-known that $\text{Tr} (A^3)$ equals to the number of (ordered) triangles present in $G$. By knowing the spectrum of $A$ we can calculate $\text{Tr} (A^3) = (-1)(d^2 - 1) + (d - 1)^3(d + 1) = (d^2 - 1)d(d - 2)$. We claim that this implies that $G$ can be broken up to the disjoint union of $d + 1$ complete graphs with $d$ vertices each. Indeed, the number of (ordered) triangles in a $d - 1$ regular graph on $n$ vertices is at most $n(d - 1)(d - 2)$, because from each vertex we can choose $(d - 1)(d - 2)$ ordered pairs of edges, and the maximum number of triangles occurs if each of these pairs can be completed by a further edge to make a triangle. This happens if and only if $G$ breaks up to a disjoint union of $d + 1$ complete graphs on $d$ vertices.

In turn, this is equivalent to the vectors $b_1, b_2, \ldots, b_n$ forming $d + 1$ orthonormal bases, all being pairwise unbiased with respect to each other. □

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, 5393, Mathematical Methods in Computer Science: Essays in Memory of Thomas Beth, Section: Quantum Computing, (2008), 50 – 69.

[3] I. Bengtsson, W. Bruzda, A. 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] L. Collatz, U. Sinogowitz: Spektren endlicher Grafen. Abh. Math. Sem. Univ. Hamburg 21 (1957), 63–77

[7] T. Durt, B. G. Englert, I. Bengtsson, K. Życzkowski, On mutually unbiased bases. International Journal of Quantum Information, 8, (2010), 535–640.

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

[9] 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.

[10] A. Klappenecker & M. Rötteler, Constructions of Mutually Unbiased Bases. Finite fields and applications, 137–144, Lecture Notes In Computer Science 2948, Springer, Berlin, 2004.
[11] M. Matolcsi, *A Fourier analytic approach to the problem of mutually unbiased bases*. Stud. Sci. Math. Hung., **49** (2012), 482–491.

[12] Planat, M., Rosu, H.C., Perrine, S. *A Survey of Finite Algebraic Geometrical Structures Underlying Mutually Unbiased Quantum Measurements*. Found. Phys. **36**, 1662–1680 (2006).

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

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)

*Email address*: matomate@renyi.hu

M.W.: Budapest University of Technology and Economics (BME), H-1111, Egry J. u. 1, Budapest, Hungary and MTA-BME Lendület Quantum Information Theory Research Group

*Email address*: mweiner@math.bme.hu