On the algorithmic solvability of mutually unbiased bases problem

Nikolay Nadirashvili

Abstract—**The concept of mutually unbiased bases is studied from the finite point of view and it is shown that the inexistence hypotheses can be verified by means of finite algorithms. The sketch of the algorithm is presented.**

Keywords— **algorithmic approach, mutually unbiased bases, quantum information theory.**

I. Introduction

The problem of mutually unbiased bases (MUBs) has been one of the central open problems in quantum information theory. Whereas having a clear physical interpretation the problem is solely algebraic. Here is the formal definition. Mutually unbiased bases (MUB) in Hilbert space $\mathbb{C}^d$ are two orthonormal bases $\{v_1, v_2, \ldots, v_d\}$ and $\{u_1, u_2, \ldots, u_d\}$ such that

$$|\langle v_i, u_j\rangle|^2 = \frac{1}{d} \ \forall i,j \in \{1,2,\ldots,d\}$$

Let $\mathfrak{M}(d)$ denote the maximal number of mutually unbiased bases in the d-dimensional Hilbert space. So it is an open question - how many mutually unbiased bases $\mathfrak{M}(d)$ do there exist in a Hilbert space $\mathbb{C}^d$. The physical interpretation is quite plain. Each orthonormal basis in a Hilbert space is associated with a quantum observable, in other words there exists a measurement of a particle in a d-dimensional quantum state in this basis resulting in the collapse of the state to one of the orthonormal vectors. Since a pure quantum state q is a unit vector in a Hilbert space $\mathbb{C}^d$ the probability of collapsing to the given vector v_i of the basis is $|\langle v_i, u_j\rangle|^2$. Therefore in case if a quantum system is prepared in a state belonging to one of the bases, then all outcomes of the measurement with respect to the other basis will occur with equal probabilities. All the information is erased. Heisenberg's uncertainty principle is closely associated with the infinite-dimensional MUBs problem with position and momentum measurements being quantum observables which are mutually unbiased. So getting back to the finite dimensions case, the question is: how many different quantum observables do there exist in a given dimension such that a measurement in any basis automatically "erases" the information about the outcomes of the others?

And the algebra leads to some physically unpredictable results. The problem has been solved for the prime power dimensions [4]

$\mathfrak{M}(p^n) = p^n + 1$ where p is a prime,

and there are numerical evidences that for composite numbers other than prime powers the answer is different. It is unknown even for the Hilbert space of complex dimension 6. There is a conjecture that $\mathfrak{M}(6) = 3$ [6]. Explicit constructions that have been proposed for Hilbert spaces of prime power dimensions use the fact that there exist algebraic fields of every prime power order. That is why such an approach seems pointless in other composite cases. So it appears that the physical properties of the system are in some inconceivable way dependent on the number-theoretical properties of the space dimension.

There have been many attempts to deal with the MUBs problem in the 6 dimensional case. 3 pairwise unbiased orthonormal bases can be easily constructed, but the problem of proving the non-existence of the 4th seems to be extremely difficult. In recent times there have been attempts to computationally deal with the problem [5] which were quite unsatisfactory, though resulting in some additional evidences supporting conjecture $\mathfrak{M}(6) = 3$.

This paper is partly inspired by this finite approach, and partly by complex Hadamard matrices approach. We will prove that hypotheses of the impossibility of constructing mutually unbiased orthonormal bases (when this is actually impossible) can be verified in the finite number of steps.

II. Algorithmic solvability

A. Notation

It would be convenient to use the following notation:
$\mathcal{M}_n$ - the algebra of square $(n * n)$ complex matrices.
$\mathcal{N}$ - the set of square $(n * n)$ complex matrices with unit columns.
$\mathcal{U}_n$ - the group of unitary matrices or rank n.
$\mathcal{H}_n$ - the set of complex Hadamard matrices of rank n.
$\mathcal{H}_n \neq \emptyset \, \forall n$ [1]

$\mathcal{NH}_n = \left\{A = \{a_{i,j}\} \mid A \in \mathcal{M}_n , |a_{i,j}| = \frac{1}{\sqrt{n}}, \forall i,j \right\}$

$\mathcal{UH}_n = \left\{\frac{1}{\sqrt{n}} A \mid A \in \mathcal{H}_n\right\}$

Let X be an arbitrary set, then denote $X^{\otimes k} = X \otimes X \otimes \ldots \otimes X - k$ times
Let $\|\cdot$ be a matrix norm such that for a given $\|B\|_1 = \sum_{i,j}^{n} |b_{i,j}|, \ B \in \mathcal{J}$

Manuscript received May 20, 2014.

N. Nadirashvili is with the Computational Mathematics and Cybernetics Faculty, Lomonosov Moscow State University (nick.quant@gmail.com).

B. The main part

Remark 2.1.

Each orthonormal basis $\{v_1, v_2, \dots, v_d\}$ in Hilbert space $\mathbb{C}^d$ is associated with the unitary matrix $V \in \mathcal{U}_d$, where each column represents the corresponding basis vector.

This is quite obvious for all the columns are pairwise orthogonal, and they also represent unit vectors. From now on we will sometimes use the notion of mutually unbiased unitary matrices, which means unitary matrices associated with the MUBs.

Lemma 2.1

$$\max_{A \in \mathcal{N}_d}(\|A\|_1) = d^{3/2}, argmax_{A \in \mathcal{N}_d}(\|A\|_1) = \{B \mid B \in \mathcal{NH}_d\}$$

Proof.

The first statement is easily deduced from the following fact

$$\max_{A \in \mathcal{N}_d}(\|A\|_1) = \sum_{i=1}^{d} \max_{\|a_i\|_2=1, a_i \in \mathbb{C}^d}(\|a_i\|_1)$$
$$= d \max_{\|a\|_2=1, a \in \mathbb{C}^d}(\|a\|_1)$$

Where a_i is the i-th column of the A matrix, and $\|\cdot\|_2$ is a simple Euclidian norm.

$$\max_{\|a\|_2=1, a \in \mathbb{C}^d}(\|a\|_1) = d^{1/2},$$

which is obvious, if we restate the problem as follows:

$$\begin{cases} \sum_{i=1}^{d} |a_i| \to max \\ \sum_{i=1}^{d} |a_i|^2 = 1 \end{cases} \Rightarrow |a_i| = \frac{1}{\sqrt{d}}, \forall i$$

This also proves the second part of the lemma, thus stating that the elements of the A matrix can only be modulus equal to $\frac{1}{\sqrt{d}}$.

Corollary 2.1

$$\max_{V \in \mathcal{U}_d}(\|V\|_1) = d^{\frac{3}{2}}, argmax_{V \in \mathcal{U}_d}(\|V\|_1) = \{B \mid B \in \mathcal{UH}_d\}$$

Lemma 2.2

$\|U_x^* U_y\|_1 = d^{3/2}$, $U_x, U_y \in U_d \Leftrightarrow$

bases associated with U_x and U_y are mutually unbiased.

Proof.

$(\Rightarrow)$

$$\|U_x^* U_y\|_1 = d^{\frac{3}{2}} \Rightarrow U_x^* U_y \in \mathcal{UH}_d \Rightarrow \forall i,j \ |\langle u_i^x, u_j^y \rangle| = \frac{1}{\sqrt{d}},$$

therefore U_x, U_y are mutually unbiased.

$(\Leftarrow)$

U_x, U_y are mutually unbiased, therefore

$\forall i,j \ |\langle u_i^x, u_j^y \rangle| = \frac{1}{\sqrt{d}} \Rightarrow U_x^* U_y \in \mathcal{UH}_d \Rightarrow \|U_x^* U_y\|_1 = d^{3/2}$.

Definition 2.1

$$MUB(d,k) = \{(U_1, U_2, \dots, U_k) \in \mathcal{U}_d^{\otimes k} \mid U_i^* U_j \in \mathcal{UH}_d, 1 \le i < j \le d\}$$

Which is equivalent to the following definition:

$$MUB(d,k) = \left\{ \begin{array}{c} (U_1, U_2, \dots, U_k) \in \mathcal{U}_d^{\otimes k} \mid \|U_i^* U_j\|_1 = d^{\frac{3}{2}}, \\ 1 \le i < j \le d \end{array} \right\}$$

The two definitions are equivalent due to the previous lemma. So $MUB(d,k)$ is a set of all k-element sets of mutually unbiased unitary matrices of rank d.

Definition 2.2

Let $\zeta_{d,k}: \mathcal{M}_d^{\otimes k} \to \mathbb{R}$, *such that*

$$\zeta_{d,k}(M_1, M_2, \dots, M_k) = \sum_{1 \le i < j \le d} \|M_i^* M_j\|_1$$

Lemma 2.3

$argmax_{\overline{U} \in \mathcal{U}_d^{\otimes k}} \zeta_{d,k}(\overline{U}) = MUB(d,k)$, *if there exist k mutually unbiased bases in Hilbert space dimension d. If so, then*

$$max_{\overline{U} \in \mathcal{U}_d^{\otimes k}} \zeta_{d,k}(\overline{U}) = \frac{k(k-1)d^{3/2}}{2} = \zeta_{d,k}^*$$

Proof.

If there exist k mutually unbiased bases ($\overline{U}$) in Hilbert space dimension d then

$$\forall i,j \mid 1 \le i < j \le k \ \|U_i^* U_j\|_1 = d^{3/2}$$
$$\zeta_{d,k}(\overline{U}) = \frac{k(k-1)d^{3/2}}{2}$$

This equation cannot hold for non mutually unbiased bases, because it would contradict Lemma 2.2.

Remark 2.2

The problem is that

$$max_{\overline{N} \in \mathcal{N}_d^{\otimes k}} \zeta_{d,k}(\overline{N}) = \frac{k(k-1)d^{\frac{3}{2}}}{2}$$
$$\nRightarrow argmax_{\overline{N} \in \mathcal{N}_d^{\otimes k}} \zeta_{d,k}(\overline{N}) = MUB(d,k)$$

So we cannot search throughout the $\mathcal{N}_d^{\otimes k}$ and expect that finding $\zeta_{d,k}^*$ will immediately give us the mutually unbiased matrices. The counterexample is not difficult to construct.

Definition 2.3

Let $\xi_{d,k}: \mathcal{M}_d^{\otimes k} \to \mathbb{R}$, *such that*

$$\xi_{d,k}(M_1, M_2, \dots, M_k) = \sum_{1 \le i < j \le d} \|M_i^* M_i\|_1$$

This $\xi_{d,k}$ function helps us overcome the problem stated in Remark 2.2 by introducing a kind of unitarity measure for the set of k d-rank matrices.

Lemma 2.4

$\xi_{d,k}(\overline{N}) \ge dk$ if $\overline{N} \in \mathcal{N}_d^{\otimes k}$

Proof.

This holds true, for $min_{A\in\mathcal{N}}(\|A^*A\|_1) = d$. The diagonal elements are always equal to $\frac{1}{\sqrt{d}}$, whereas the other elements add some non-strictly positive delta.

Lemma 2.5
$\xi_{d,k}(\overline{N}) = dk = \xi^*_{d,k} \Leftrightarrow \overline{N} \in \mathcal{U}_d^{\otimes k}$
Proof.
Continuing the reasoning of the previous lemma, we may notice that the non-strictly positive delta of the non-diagonal elements turn to zero $\forall i,j\ \langle u_i, u_j\rangle = 0$.
The next step is to combine the functions introduced earlier into a compound “MUBness” criteria.

Definition 2.4
Let $\eta_{d,k}: \mathcal{M}_d^{\otimes k} \to \mathbb{R}^2$, *such that*

$$\eta_{d,k}(\overline{M}) = \begin{pmatrix} \zeta_{d,k}(\overline{M}) \\ \xi_{d,k}(\overline{M}) \end{pmatrix}$$

The following theorem can now be said to be obvious.

Theorem 2.1
If $\overline{N} \in \mathcal{N}_d^{\otimes k}$ *then*

$$\eta_{d,k}(\overline{N}) = \begin{pmatrix} \zeta^*_{d,k} \\ \xi^*_{d,k} \end{pmatrix} = \eta^*_{d,k} \Leftrightarrow \overline{N} \in MUB(d,k)$$

Lemma 2.6
Let $(U_1, U_2, \dots, U_k) \in MUB(d,k)$, *then*
$\forall V \in \mathcal{U}_d \quad (VU_1, VU_2, \dots, VU_k) \in MUB(d,k)$
Proof.
This holds true for $(VU_i)^* VU_j = U_i^* V^* V U_j = U_i^* U_j$

Corollary 2.2
Let $(U_1, U_2, \dots, U_k) \in MUB(d,k)$, *then* $(I_d, U_1^* U_2, \dots, U_1^* U_k) \in MUB(d,k)$, *where* I_d *is an identity matrix. So constructing MUBs we can always assume the first basis to be computational and the set of all the other bases belongs to* $\mathcal{UH}_d^{\otimes(k-1)}$.

Definition 2.5
Let $\mathcal{IUH}_{d,k} = \{(I_d, \overline{U}), \overline{U} \in \mathcal{UH}_d^{\otimes(k-1)}\}$,
$\mathcal{INH}_{d,k} = \{(I_d, \overline{N}), \overline{N} \in \mathcal{NH}_d^{\otimes(k-1)}\}$
We introduce these definitions in order to easily declare enumerated sets of unitary matrices with the first matrix being the identity one.

Remark 2.3
$\mathcal{INH}_{d,k}$ *is a compact. Therefore every open cover in it has a finite subcover.*

Remark 2.4
$\mathcal{IUH}_{d,k} \subset \mathcal{INH}_{d,k}$. $\mathcal{INH}_{d,k}$ *is homeomorphic to* $(k-1)d^2$ *dimensional torus.*

Definition 2.6
Define function $\psi: \mathcal{NH}_d \times \mathcal{NH}_d \to \mathbb{R}$, *as*
$\psi(A_1, A_2) = \sum_{i,j} \min(|\alpha_{i,j} - \beta_{i,j}|, 2\pi - |\alpha_{i,j} - \beta_{i,j}|)$,
where $A_1 = \left\{\frac{e^{i\alpha_{k,l}}}{\sqrt{d}}\right\}$, $A_2 = \left\{\frac{e^{i\beta_{k,l}}}{\sqrt{d}}\right\}$,
$1 \le k \le d, 1 \le l \le d;\ \alpha, \beta \in [0; 2\pi)$ *is a metric.*

The metric properties can be easily checked.

Theorem 2.2

1. $\eta_{d,k}: \mathcal{INH}_{d,k} \to \mathbb{R}^2$ *is uniformly continuous.*
2. $\sigma_\varepsilon \eta_{d,k}(\overline{N}) \le \begin{pmatrix} \frac{d^2(k-1)(k-2)}{2} \min(\varepsilon, 2d) \\ d^2(k-1)\min(\varepsilon, 2d) \end{pmatrix}$

Where σ_ε *is the* ε*-neighbourhood variation (with respect to* ψ*-metric) of the function* $\eta_{d,k}$ *in the point* $\overline{N} \in I\mathcal{NH}_{d,k}$ *which is not dependent on* $\overline{N}$.
Proof.
The first statement follows from the facts that ζ and ξ functions are both uniformly continuous and they two precisely form the components of η. Now let’s deal with the second statement. First let’s evaluate the ε-neighborhood variation for the components of $\eta_{d,k}$. Let $Q = \{q_{i,j}\}, i,j < d \mid q_{i,j} = \frac{1}{\sqrt{d}}$.
And let $A \circ B$ be an element wise product of the two matrices (or vectors). Then

$$\|U^*V\|_1 - \|(U \circ E_1)^*(V \circ E_2)\|_1 =$$
$$\sum_{k,l} (|\langle u_k, v_l\rangle| - |\langle u_k \circ \varepsilon_k, v_l \circ \delta_l\rangle|) \le$$
$$\sum_{k,l} \left| \sum_i^d \bar{u}_i^k v_i^l - \sum_i^d \bar{u}_i^k \bar{\varepsilon}_i^k v_i^l \delta_i^l \right| \le$$
$$\sum_{k,l} \left| \sum_i^d \bar{u}_i^k v_i^l (1 - \bar{\varepsilon}_i^k \delta_i^l) \right| \le$$
$$\sum_{k,l} \left(\left(\sum_i^d |\bar{u}_i^k v_i^l| \right) \left(\sum_i^d |1 - \bar{\varepsilon}_i^k \delta_i^l| \right) \right) =$$
$$\sum_{k,l} \left(\left(\sum_i^d \frac{1}{d} \right) \left(\sum_i^d |1 - \bar{\varepsilon}_i^k \delta_i^l| \right) \right) =$$
$$\sum_{k,l} \sum_i^d |1 - \bar{\varepsilon}_i^k \delta_i^l| \le \sum_{k,l} d \left|1 - e^{\frac{i\varepsilon}{d}}\right| \le$$
$$\sum_{k,l} \min(\varepsilon, 2d) = d^2 \min(\varepsilon, 2d)$$

So that for a given ε,
$\psi(E_1, Q) + \psi(E_2, Q) < \varepsilon$, $E_1 = \{\varepsilon_{i,j}\}, E_2 = \{\delta_{i,j}\}$.
Now it is easy to show that $\sigma_\varepsilon \zeta_{d,k}(\overline{N}) \le \frac{d^2(k-1)(k-2)}{2} \min(\varepsilon, 2d)$.
Similarly $\sigma_\varepsilon \xi_{d,k}(\overline{N}) \le (k-1)d^2 \min(\varepsilon, 2d)$. Therefore the second statement of the theorem holds true.
This all leads us to the following:

Theorem 2.3 (Theorem of weak algorithmic solvability)

1. $MUB(d,k) = \emptyset \Rightarrow$ *there exists a finite open* ε*-cover* $(E_1, E_2, \dots, E_p)$ *of* $\mathcal{INH}_{d,k}$, *such that for a given* $E_i\ \forall x \in E_i$

$$|\eta_{d,k}(x) - \eta^*| = \begin{pmatrix} |\zeta_{d,k}(x) - \zeta^*| \\ |\xi_{d,k}(x) - \xi^*| \end{pmatrix} > \sigma_\varepsilon \eta_{d,k}$$

2. *If there exists a finite open ε-cover $(E_1, E_2, \dots, E_p)$ of $\mathcal{INH}_{d,k}$, such that $|\eta_{d,k}(x) - \eta^*| > \sigma_\varepsilon \eta_{d,k}$, then $MUB(d,k) = \emptyset$.*

Consequently the last theorem opens a way for the finite approach to the problem. Let's mention only one of them (which is quite naive) implemented to the Hilbert space $\mathbb{C}^d$.

1. Choose an arbitrary small enough ε.
2. Construct an ε-cover for $\mathcal{INH}_{d,k}$
3. For each element of the cover, choose an arbitrary point x on it and evaluate $\eta_{d,k}(x)$. If it meets the conditions of the last theorem (part 2), then there are no mutually unbiased bases in this element of the cover, so move to the next element of the cover. If the condition if fulfilled, then choose a smaller ε and repeat the step 3.

If all the elements of the cover meet the condition, then there are no k mutually unbiased bases in the Hilbert space dimension d.

III. Conclusion

We have shown that the mutually unbiased bases problem, which having a clear physical interpretation still remains purely algebraic, can be algorithmically solved in some cases (when the hypothesis of the inexistence of a set of MUBs of a given order is true). At the same time, while dealing with the opposite cases (when the hypothesis is false) this approach can help us "localize" these MUBs in the sense that we can construct the bases that act very much like mutually unbiased. The inequalities used in the proof of Theorem 2.2 are not optimally efficient for they can often be significantly improved by observing different cases. These improvements can serve as a strong basis for the further researches.

References

[1] Ferenc Szollozi, "Construction, classification and parametrization of complex Hadamard matrices " arXiv:1110.5590v1, 2011.

[2] Wojciech Tadej, Karol Zyczkowski, "A concise guide to complex Hadamard matrices", http://arxiv.org/abs/quant-ph/0512154v2, 2006.

[3] Stefan Weigert, Michael Wilkinson, "Mutually Unbiased Bases for Continuous Variables", arXiv:0802.0394v2, 2008.

[4] Ingemar Bengtsson, Wojciech Bruzda, Asa Ericsson, Jan-Ake Larsson, Wojciech Tadej, Karol Zyczkowski "Mutually unbiased bases and hadamard matrices of order", arXiv:quant-ph/0610161v3, 2007.

[5] Paul Butterley, and William Hall, "Numerical evidence for the maximum number of mutually unbiased bases in dimension six", arXiv:quant-ph/0701122v2, 2007.

[6] Thomas Durt, Berthold-Geord Englert, Ingemar Bengtsson, Karol Zyczkowski, "On mutually unbiased bases", International Journal of Quantum Information 8, 2010.