Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/100609

New Approach to Finding the Maximum Number of Mutually Unbiased Bases in $\mathbb{C}^6$

J. Batle[1,*], *Ahmed Farouk*[2], *Mosayeb Naseri*[3] *and Mohamed Elhoseny*[4]

[1] Departament de Física, Universitat de les Illes Balears, 07122 Palma de Mallorca, Balearic Islands, Spain
[2] Information Technology Department , Al-Zahra College for Women, P.O.Box 3365. Muscat, Oman
[3] Department of Physics, Kermanshah Branch, Islamic Azad University, Kermanshah, Iran
[4] Faculty of Computer and Information Sciences, Mansoura University, Egypt

Received: 10 May 2016, Revised: 9 Sep. 2016, Accepted: 17 Sep. 2016
Published online: 1 Nov. 2016

Abstract: We introduce a new approach to the problem of finding sets of m mutually unbiased bases which are compatible with a given space $\mathbb{C}^d$, by translating it into an optimization procedure for a given pair (m,d). In addition, our procedure leads to new sets of basis such that they may approach those hypothetical ones for $m=4$.

Keywords: Mutually Unbiased Bases, Quantum Information Theory, Optimization

1 Introduction

The paradigm of physical observables defined on an infinite Hilbert space being mutually incompatible in quantum mechanics is provided by the Heisenberg commutation relations for the position and momentum operators. The associated Heisenberg group –in connection with the corresponding Weyl algebra– of phase-space translations is still relevant for systems with a finite number of orthogonal states, providing a basis of the space $\mathbb{C}^d$. As first studied by Schwinger, for each dimension $d \geq 2$ there is a set of unitary operators which give rise to a discrete equivalent of the Heisenberg-Weyl group [1].

We may somehow expect that the evolution of composite quantum systems will be dependent on the dimensions of their building blocks. In other words, that composite systems (being the tensor product of two different Hilbert spaces that differ only in the corresponding dimensions) will undergo a similar evolution for they are structurally identical. Mathematically, the previous fact would imply the state spaces $\mathbb{C}^d$ to possess an identical structure, at least regarding properties closely related to the Heisenberg-Weyl group.

However, it is surprising that the aforementioned group allows one to construct $(d+1)$ so-called mutually unbiased (MU) bases of the space $\mathbb{C}^d$ if d is the power of a prime number [2,3], whereas the construction fails in all other dimensions. In point of fact, no other method is known to construct $(d+1)$ MU bases in arbitrary dimensions [4,5].

The definition of MU bases is provided as follows. Given $m=d+1$ orthonormal bases in the space $\mathbb{C}^d$, they are *mutually unbiased* if the moduli of the scalar products among the $d(d+1)$ basis vectors take these values:

$$\left|\langle \psi_j^b | \psi_{j'}^{b'} \rangle\right| = \begin{cases} \delta_{jj'} & \text{if } b=b', \\ \frac{1}{\sqrt{d}} & \text{if } b\neq b', \end{cases} \qquad (1)$$

where $b,b' = 0,1,\ldots,d$. MU bases have useful applications in many quantum information processing. Such (complete) sets of MU bases are ideally suited to reconstruct quantum states [3] while sets of up to $(d+1)$ MU bases have applications in quantum cryptography [6, **?**] and in the solution of the mean king's problem [8]. Even for $d=6$, we do not know whether there exist four MU bases or not [9,10,11,12]. Hence the research on the maximum number of bases for $d=6$ and construction of MU bases in $\mathbb{C}^6$ is of great importance. The issue of MU bases constitutes another part in the field of quantum information theory that is involved in pure mathematics, such as number theory, abstract algebra and projective algebra.

* Corresponding author e-mail: jbv276@uib.es

The methods to construct complete sets of MU bases typically deal with all prime or prime-power dimensions. They are constructive methods and effectively lead to the same bases. Two (or more) MU bases thus correspond to two (or more) unitary matrices, one of which can always be mapped to the identity I of the space $\mathbb{C}^d$, using an overall unitary transformation. It then follows from the conditions (1) that the remaining unitary matrices must be complex Hadamard matrices: the moduli of all their matrix elements equal $1/\sqrt{d}$. This representation of MU bases links their classification to the classification of complex Hadamard matrices [13].

In this paper, we choose a different method to study MU bases in dimension six or any other dimension d. We will approach the problem by directly exploring the unitary matrices – randomly distributed, but according to the Haar measure – whose columns vectors constitute the bases elements, which must fulfill a series of requirements concerning their concomitant bases being unbiased. The overall scenario reduces to a simple –though a bit involved– optimization procedure. In point of fact, we shall perform a two-fold search employing i) an amoeba optimization procedure, where the optimal value is obtained at the risk of falling into a local minimum and ii) the so called simulated annealing [14] well-known search method, a Monte Carlo method, inspired by the cooling processes of molten metals. The advantage of this duplicity of computations is that we can be absolutely confident about the final result reached. Indeed, the second recipe contains a mechanism that allows a local search that eventually can escape from local optima.

Others methods have also explored numerically MU bases. Our approach is different in the sense that new MU basis, arbitrarily close to a given case, may occur. This new insight aims at finding them and, eventually, describing the ensuing MU basis.

This paper is organized as follows. In Section II we describe the generation of unitary matrices according to their natural Haar measure. Section III explains how the optimization is performed and the concomitant results are shown in Section IV. Finally, some conclusions are drawn in Section V.

2 The Haar measure and the concomitant generation of ensembles of random matrices

The applications that have appeared so far in quantum information theory, in the form of dense coding, teleportation, quantum cryptography and specially in algorithms for quantum computing (quantum error correction codes for instance), deal with finite numbers of qubits. A quantum gate which acts upon these qubits or even the evolution of that system is represented by a unitary matrix $U(N)$, with $N = 2^n$ being the dimension of the associated Hilbert space $\mathscr{H}_N$. The state ρ describing a system of n qubits is given by a hermitian, positive-semidefinite ($N \times N$) matrix, with unit trace. In view of these facts, it is natural to think that an interest has appeared in the *quantification* of certain properties of these systems, most of the times in the form of the characterization of a certain state ρ, described by $N \times N$ matrices of finite size. Natural applications arise when one tries to simulate certain processes through random matrices, whose probability distribution ought to be described accordingly.

This enterprise requires a quantitative measure μ on a given set of matrices. There is one natural candidate measure, the **Haar measure** on the group $\mathscr{U}(N)$ of unitary matrices. In mathematical analysis, the Haar measure [15] is known to assign an "invariant volume" to what is known as subsets of locally compact topological groups. Here we present the formal definition [16]: given a locally compact topological group G (multiplication is the group operation), consider a σ-algebra Y generated by all compact subsets of G. If a is an element of G and S is a set in Y, then the set $aS = \{\, as : s \in S \,\}$ also belongs to Y. A measure μ on Y will be letf-invariant if $\mu(aS) = \mu(S)$ for all a and S. Such an invariant measure is the Haar measure μ on G (it happens to be both left and right invariant). In other words [17], the Haar measure defines the unique invariant integration measure for Lie groups. It implies that a volume element $\mathrm{d}\mu(g)$ is identified by defining the integral of a function f over G as $\int_G f(g)d\mu(g)$, being left and right invariant

$$\int_G f(g^{-1}x)d\mu(x) = \int_G f(xg^{-1})d\mu(x) = \int_G f(x)d\mu(x). \tag{2}$$

The invariance of the integral follows from the concomitant invariance of the volume element $\mathrm{d}\mu(g)$. It is plain, then, that once $\mathrm{d}\mu(g)$ is fixed at a given point, say the unit element $g = e$, we can move performing a left or right translation.

We do not gain much physical insight with these definitions of the Haar measure and its invariance, unless we identify G with the group of unitary matrices $\mathscr{U}(N)$, the element a with a unitary matrix U and S with subsets of the group of unitary matrices $\mathscr{U}(N)$, so that given a reference state $|\Psi_0\rangle$ and a unitary matrix $U \in \mathscr{U}(N)$, we can associate a state $|\Psi\rangle_0 = U|\Psi_0\rangle$ to $|\Psi_0\rangle$. Physically what is required is a probability measure μ invariant under unitary changes of basis in the space of pure states, that is,

$$P^{(N)}_{Haar}(U|\Psi\rangle) = P^{(N)}_{Haar}(|\Psi\rangle). \tag{3}$$

These requirements can only be met by the Haar measure, which is rotationally invariant.

Now that we have justified what measure we need, we should be able to generate random matrices according to such a measure in arbitrary dimensions. The theory of random matrices [18] specifies different *ensembles* of

matrices, classified according to their different properties. In particular, the Circular Unitary Ensemble (CUE) consists of all matrices with the (normalized) Haar measure on the unitary group $\mathscr{U}(N)$. The Circular Orthogonal Ensemble (COE) is described in similar terms using orthogonal matrices, and it was useful in order to describe the entanglement features of two-*rebits* systems. Given a $N \times N$ unitary matrix U, the minimum number of independent entries is N^2. This number should match those elements that need to describe the Haar measure on $\mathscr{U}(N)$. This is best seen from the following reasoning. Suppose that a matrix U is decomposed as a product of two (also unitary) matrices $U = XY$. In the vicinity of Y, we have [18] $U + dU = X(1 + idK)Y$, where dK is a hermitian matrix with elements $dK_{ij} = dK^R_{ij} + idK^I_{ij}$. Then the probability measure nearby dU is $P(dU) \sim \prod_{i\leq j} dK^R_{ij} \prod_{i<j} dK^I_{ij}$, which accounts for the number of independent variables. Such measure for CUE is invariant [18] and therefore proportional to the Haar measure.

Yet, the aforementioned description is not useful for practical purposes. We need to parameterize the unitary matrices according to the Haar measure. According to the parameterization for CUE dating back to Hurwitz [19] using Euler angles, the basic assumption is that an arbitrary unitary matrix can be decomposed into elementary two-dimensional transformations, denoted by $E^{i,j}(\phi, \psi, \chi)$:

$$\begin{aligned} E^{i,j}_{kk} &= 1 \qquad k = 1,..,N; \quad k \neq i,j \\ E^{i,j}_{ii} &= \cos\phi\, e^{i\psi} \\ E^{i,j}_{ij} &= \sin\phi\, e^{i\chi} \\ E^{i,j}_{ji} &= -\sin\phi\, e^{-i\chi} \\ E^{i,j}_{jj} &= \cos\phi\, e^{-i\psi}. \end{aligned} \tag{4}$$

Using these elementary rotations we define the composite transformations

$$\begin{aligned} E_1 &= E^{N-1,N}(\phi_{01}, \psi_{01}, \chi_1) \\ E_2 &= E^{N-2,N-1}(\phi_{12}, \psi_{12}, 0) E^{N-1,N}(\phi_{02}, \psi_{02}, \chi_2) \\ E_3 &= E^{N-3,N-2}(\phi_{23}, \psi_{23}, 0) E^{N-2,N-1}(\phi_{13}, \psi_{13}, 0) \\ &\quad E^{N-1,N}(\phi_{03}, \psi_{03}, \chi_3) \\ ... &= ... \\ E_{N-1} &= E^{1,2}(\phi_{N-2,N-1}, \psi_{N-2,N-1}, 0) \\ &\quad E^{2,3}(\phi_{N-3,N-1}, \psi_{N-3,N-1}, 0)... \\ &\quad E^{N-1,N}(\phi_{0,N-1}, \psi_{0,N-1}, \chi_{N-1}), \end{aligned} \tag{5}$$

we finally form the matrix

$$U = e^{i\alpha} E_1 E_2 E_3 ... E_{N-1} \tag{6}$$

with the angles parameterizing the rotations

$$0 \leq \phi_{rs} \leq \frac{\pi}{2} \;\; 0 \leq \psi_{rs} < 2\pi \;\; 0 \leq \chi_{1s} < 2\pi \;\; 0 \leq \alpha < 2\pi. \tag{7}$$

The ensuing (normalized) Haar measure [20]

$$\begin{aligned} P_{Haar}(dU) = &\sqrt{N! 2^{N(N-1)}} d\alpha \\ &\prod_{1\leq r<s\leq N} \frac{1}{2r} d[(\sin\phi_{rs})^{2r}] d\psi_{rs} \\ &\prod_{1<s\leq N} d\chi_{1s} \end{aligned} \tag{8}$$

provides us with a random matrix belonging to CUE. Finally, we randomly generate the angles (7) *uniformly* and obtain the desired random matrix U (6).

3 Description of the optimization procedure

Let us formulate the problem of having m orthonormal bases $B_i, i = 1..m$ in terms of the elements of a unitary matrix. All basis elements or vectors are obtained from a unitary matrix by identifying them with the corresponding columns. Unitarity guarantees that all vectors will therefore be orthonormal. Now we have to cope with the bases being unbiased amidst them. Since each basis is represented by a unitary matrix, we then have $B_i, i = 1..m \rightarrow U_i, i = 1..m$. This condition can be addressed by imposing that matrix elements

$$\left(U_i \cdot U_j\right)_{lm}, \tag{9}$$

where $i = 1 < j \leq m$, have to be equal to $1/\sqrt{d}$. In other words, $U_i \cdot U_j$ has to be proportional to a Hadamard-like matrix. The aforementioned conditions has to be applied to all possible $m(m-1)/2$ bipartite combinations of bases B_i.

Let us define the following quantities as the *residuals*

$$\rho_{l,m,i,j} \equiv \left(\left| \left(U_i \cdot U_j\right)_{l,m} \right|^2 - 1/d \right)^2. \tag{10}$$

Thus, the problem of finding a set of unbiased orthonormal bases is translated into the optimization procedure of finding the minimum of $\sum_{l,m,i,j} \rho_{l,m,i,j}$ being equal to zero. If the minimum is different from zero, given d and m, we definitely do not have a set of unbiased bases. In addition, our function resembles very much the quantity used in [21] to define the notion of "unbiasedness" between two orthonormal bases. To whether or not the aforementioned quantity represents a metric is something not checked.

Now that the we have translated the problem of finding MU bases into an operational one, one has to be able to explore all possible bases. This fact means that we have to be able to survey the set space of unitary matrices. Since we described in the previous section how to generate random unitary matrices properly, we will have to numerically explore all unitary matrices. The way to pursue that is to consider the angles (7) –given d and m– in all cases in (9) as the variables of the function

$\sum_{l,m,i,j} \rho_{l,m,i,j}$ to be minimized. Provided the concomitant optimal value (the sum of all residuals $\rho_{l,m,i,j}$) is equal to zero, we may then have found a set of MU bases. Otherwise, that may not be possible given the constraints on d and m.

4 Results

Now that we have the tools to perform a numerical survey over the set of unitary matrices, we carry out the optimization described in the previous section.

4.1 d=6, m=3

The $\mathbb{C}^6$ case with three bases is know to exist, so our numerical procedure must return a minimal value of zero. The results are depicted in Fig. (**??**). As can be appreciated, convergence is reached very fast after each Monte Carlo step (formed by 15000 different configurations each). Therefore, we are quite confident that we have found a set of MU bases in the $(d=6, m=3)-$case.

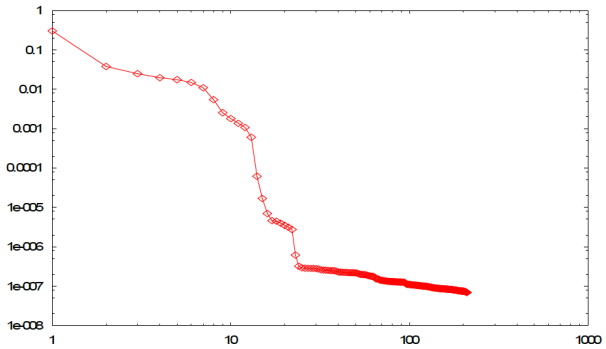

Fig. 1: Plot of the evolution of the sum of residuals –the figure of merit in the optimization– for the $d=6$ case with three basis vs. the number of Monte Carlo steps. As can be clearly appreciated, a global zero minimum is reached. See text for details.

However, we must bear in mind an important issue regarding numerical surveys. Not all our simulations lead to a zero minimum, so the lack of convergence is in favor of the argument that some sets of MU bases cannot be extended to further number of bases. In $d=6$ there are some sets of 2 MU bases that cannot be extended to 3 MU bases (see Ref. [22] and references therein). From numerical simulations it is knows that null measure sets cannot be reached. In [22], a subset of the Karlson's family of complex Hadamard matrices cannot be extended to 3 MU bases. Additionally, the Karlson's family has dimension 2 and the maximal set of complex Hadamard matrices in dimension 6 has dimension 4, so it is a null measure set. Therefore, one could never achieve a unitary matrix from random simulations such that it belongs to the Karlsson's family. Moreover, there are 1 dimensional families and even more, isolated complex Hadamard matrices in dimension six.

When considering the extension of the number of MU bases $\{I, H_i\}$, H_i being a Hadamard matrix, provided by a certain number, we then know that that function lacks the property of continuity [23]. The absence of continuity together with an incomplete knowledge about the number discontinuities in the number of MU bases makes the overall problem a difficult one. However, in our approach, we succeed in finding at least a few cases where $(m=3, d=6)$ holds.

The study of the case with three bases confirms that our approach to the problem is a good one. As a matter of fact, we could study the problem for any $(d,m)-$case, but the overall optimization procedure –as it is indeed the case for any simulation of a quantum system– becomes intractable at some point. With the numerical tools being a valid one, we can now tackle the problem of whether $\mathbb{C}^6$ can sustain $m=4$ MU bases.

4.2 d=6, m=4

Now that we have implemented the tools for performing a search in the space of unitary matrices of a given dimension $N \times N$, we are in a position a bit closer to ascertain whether it is possible to have four MU bases in the $d=6-$case. We start the numerical search and the outcome of if is shown in Fig. (**??**). The evolution is such that the total function to be minimized rapidly decreases, and attains a value that is not zero. Several repetitions of the same optimization procedure lead to the same conclusion: the value which is optimized is of $O(1)$. Thus, we have more evidence that four mutually unbiased bases cannot occur in $\mathbb{C}^6$. However, in the light of the previous discussion on continuity, it still remains doubts that our numerical procedure may not arrive at the minimum of 0 because we are trying to explore a set of zero measure. This fact implies that our numerical approach to the problem may have (still) some loopholes as far as reaching a conclusive answer. All facts points towards that $m=4$ is incompatible with $d=6$, but we have no theorem that ascertains whether the function which is optimized reaches may ever reach a minimum of zero.

In addition, we are left with an intriguing question: what is the meaning of having a set of four almost MU bases? (let us call them $\varepsilon-$MU bases from now on). Definitely, if we have found one such $\varepsilon-$MU bases set, it may not be unique. In point of fact, there may exist as many as different vales for the function to be optimized are reached. However, what is the physics that entails that one family of these $\varepsilon-$MU bases reaches a minimum minimorum? In operational terms, what role could these

$\varepsilon-$MU bases play in practice? It may be the case, for instance, that a subset of the four bases is mutually unbiased.

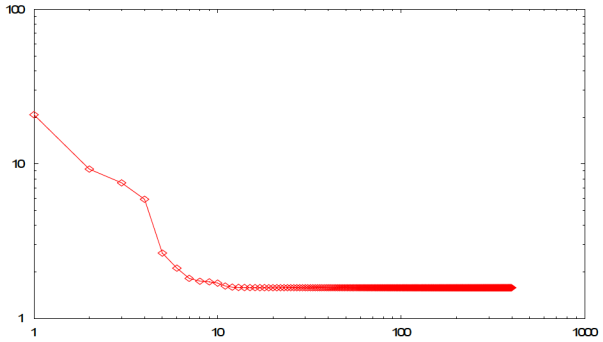

Fig. 2: Plot of the evolution of the sum of residuals for the $d = 6$ case with four basis vs. the number of Monte Carlo steps. This typical evolution of the function to be optimized –the sum of residuals in our case– does not reach a minimum of zero. It approaches zero but the corresponding value is always of $O(1)$. See text for details.

5 Conclusions

We have translated the problem of the existence of $m = 4-$bases in $\mathbb{C}^6$ into an optimization procedure. As expected, the concomitant numerical optimization has provided a satisfactory answer for known cases such as $m = 3$ in $\mathbb{C}^6$. This new approach to the problem of to whether or not there exist a set of $m = 4$ MU bases for $d = 6$ has provided more evidence in favor that this is not case, although no theorem guarantees this argument.

In addition, we are left with the interesting question on the limitations that pose the use of sets of imperfect MU bases in quantum information tasks, an issue that is certainly of interest for in experiments one has to deal with imperfections. Also, our procedure is capable to explore more dimensions and bases in a straightforward manner, although taking into account that a computational limitation is reached, and therefore opens the door to similar studies in the future, where the concomitant MU basis can be described systematically [24].

Acknowledgement

J. Batle acknowledges fruitful discussions with D. Goyeneche, J. Rosselló, Maria del Mar Batle and Regina Batle.

References

[1] J. Schwinger, Proc. Nat. Acad. Sci. U.S.A., **46**, 560, (1960)
[2] I. D. Ivanović, J. Phys. A, **14**, 3241, (1981)
[3] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.), **191**, 363 (1989)
[4] C. Archer, J. Math. Phys. **46**, 022106 (2005)
[5] M. Planat, H. Rosu, and S. Perrine, Found. Phys. **36**, 1662 (2006)
[6] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin: Phys. Rev. Lett. **88**, 127902 (2002)
[7] S. Brierley: *Quantum key distribution highly sensitive to eavesdropping*, arXiv:0910.2578
[8] Y. Aharonov and B. G. Englert, Z. Naturforsch A: Phys. Sci. **56**, 16 (2001)
[9] S. Brierley and S. Weigert, Phys. Rev. A **78**, 042312 (2008)
[10] S. Brierley and S. Weigert, Phys. Rev. A **79**, 052316 (2009)
[11] P. Raynal, X. Lü, and B.-G. Englert, Phys. Rev. A **83**, 062303 (2011)
[12] D. McNulty and S. Weigert, J. Phys. A: Math. Theor. **45**, 102001 (2012)
[13] W. Tadej and K. Zyczkowski, Open Sys. & Information Dyn. **13**, 133 (2006)
[14] S. Kirkpatrick, C. D. Gelatt Jr and M. P. Vecchi, Science **220** (4598), 671 (1983)
[15] A. Haar, Ann. Math. **34**, 147 (1933).
[16] J. Conway, *Course in Functional Analysis* (Springer-Verlag, New York, 1990)
[17] M. Chaichian and R. Hagedorn, *Symmetries in quantum mechanics*, (Inst. of Phys. Publ., Bristol)
[18] M. L. Mehta, *Random Matrices* (Academic, New York, 1990)
[19] A. Hurwitz, Nachr. Ges. Wiss. Gött. Math.-Phys. Kl. **71** (1887)
[20] V. L. Girko, *Theory of Random Determinants* (Kluwer, Dordrecht, 1990)
[21] T. Durt et al., Int. J. Quantum Information **8**, 535 (2010)
[22] D. Goyeneche, J. Phys. A: Math. Theor. **46**, 105301 (2013)
[23] P. Jaming et al, J. Phys. A: Math. Theor. **42**, 245305 (2009)
[24] J. Batle et al. Under preparation (2016)

J. Batle has been a Research Associate at the Universitat de les Illes Balears, Spain. He has been Assistant Professor in Kuwait, as well. His research interests are in quantum information, information theory, thermostatistics, and general quantum mechanics.

Ahmed Farouk is Assistant Professor at Al-Zahra College for Women, Oman. He obtained his PhD in Computer Sciences in 2015. His interests are Quantum Communication, Optical Technologies, Wireless Technologies, Quantum Cryptography and Satellite Communication.

Mosayeb Naseri obtained his PhD degree in theoretical physics from Razi University of Kermanshah, IRAN in 2007. He is associated professor of physics at Kermanshah branch, Islamic Azad University, Kermanshah, IRAN. His research interests are in Quantum Information and Computation, specially quantum communication and quantum image processing.

Mohamed Elhoseny is a lecturer in the Faculty of Computers and Information Sciences at Mansoura University, Mansoura, Egypt. He got his PhD in Computer and information Sciences after joint supervision between (Faculty of Computer and Information Sciences, Mansoura University, Egypt) and (Department of Computer Science and Engineering, University of North Texas, USA). His research interests include intelligent information systems, artificial intelligence, wireless sensor network, data security and big data.