MUBs: From Finite Projective Geometry to Quantum Phase Enciphering

H.C. Rosu*, M. Planat† and M. Saniga**

*Department of Applied Mathematics, IPICyT, Apdo Postal 3-74 Tangamanga, San Luis Potosí, Mexico
†Institut FEMTO-ST, Département LPMO, CNRS, 32 Avenue de l'Observatoire, 25044 Besançon, France
**Astronomical Institute, Slovak Academy of Sciences, 05960 Tatranská Lomnica, Slovak Republic

Abstract. This short note highlights the most prominent mathematical problems and physical questions associated with the existence of the maximum sets of mutually unbiased bases (MUBs) in the Hilbert space of a given dimension.

INTRODUCTION

Technical problems in quantum information theory already connect such distinct disciplines as number theory, abstract algebra and projective geometry. For a partial list of open problems related to the development of quantum computing technologies, see `http://www.imaph.tu-bs.de/qi/problems`. In this stimulating research area the issue of the so-called mutually unbiased bases is an important one since it is related to the complete state determination of a quantum system.

DEFINITIONS AND BASIC FACTS

Two different orthonormal bases A and B of a d-dimensional Hilbert space are called *mutually unbiased* if and only if

$$|\langle a|b\rangle| = 1/\sqrt{d}\,, \tag{1}$$

for all $a \in A$ and all $b \in B$. An aggregate of MUBs is a set of orthonormal bases which are pairwise mutually unbiased. It has been found that the maximum number of such bases cannot be greater than $d+1$ in d-dimensional Hilbert space [1]. It is also known that this limit is reached if d is a power of a prime.

Yet, a still unanswered question is if there are non prime power values of d for which this bound is attained. Based on numerical calculations, it is generally agreed [2] that in the latter cases the lower bound on the maximum number of such bases is

$$N_{\max} = 1 + \min(p_i^{e_i}),$$

where $\min(p_i^{e_i})$ is the lowest factor in the prime number decomposition of $d = \prod_i p_i^{e_i}$.

Whether or not there exists a set of $d+1$ MUBs in a d-dimensional Hilbert space if d not a power of a prime could be intimately linked with the question of the existence of projective planes whose order is not a power of prime according to a conjecture that we published recently [3]. Another interesting recent result is that when the quantum measurements are performed in MUBs, a simple linear and universal relation exists between the post-measurement density matrix and the pre-measurement density matrix [4].

The main application of MUBs pertains to secure quantum key exchange (quantum cryptography). This is because any attempt by an eavesdropper (say Eve) to distinguish between two non-orthogonal quantum states shared by two remote parties (say Alice and Bob) will occur at the price of introducing a disturbance to the signal, thus revealing the attack, and allowing to reject the corrupted quantum data. Modern protocols, e.g., the original BB84 protocol, use only one qubit technologies implying dimension $d = 2$, usually the polarisation states of the photon. But the security against eavesdropping increases when all the three bases of qubits are used, or by using qudits, or entanglement-based protocols.

CP734, *Quantum Communication, Measurement and Computing*,
edited by S. M. Barnett et al.

Quantum state recovery and secure quantum key distribution can also be achieved using positive operator valued measures (POVMs) which are symmetric informationally complete (SIC-POVMs) [5]. These are sets of d^2 normalized vectors a and b such that

$$|\langle a|b\rangle| = 1/(d+1)^{1/2} \text{ when } a \neq b\,.$$

Unlike the MUBs, the SIC-POVMs could exist in all finite dimensions. Recently, SIC-POVMs have been constructed in dimension $d = 6$ [6].

MUB'S AND FINITE PROJECTIVE PLANES

As already mentioned, we have recently conjectured [3] that the existence of the maximum set of MUBs in a given dimension d and that of a projective plane of the same dimension may well represent two aspects of one and the same problem. Perhaps the most serious backing of our surmise is found in a recent paper by Wootters [7]. Associating a line in a finite geometry with a pure state in the quantum problem, the author shows that a complete set of MUBs is, in some respects, analogous to a finite *affine* plane, and another kind of quantum measurement, the SIC-POVM, is also analogous to the same configuration, but with the swapped roles of points and lines. It represents no difficulty to show that this "dual" view of quantum measurement is deeply rooted in our conjecture. To this end, it suffices to recall two facts [8]. First, any affine plane is a particular subplane (subgeometry) of a projective plane, viz. a plane which arises from the latter if one *line*, the so-called "line at infinity," is deleted. Second, in a projective plane, there is a perfect *duality* between points and lines; that means, to every projective plane, S_2, there exists a dual projective plane, Σ_2, whose points are the lines of S_2 and whose lines are the points of S_2 [9]. So, *affinizing* S_2 means deleting a *point* of Σ_2 and thus, in light of our conjecture, qualitatively recovering the results of Wootters, shedding also important light on some other of the most recent findings [4, 10]. The latter reference, in fact, gives several strong arguments that there are no more than three MUBs in dimension six, the latter being the smallest non-prime-power dimension.

MUB'S AND QUANTUM FOURIER TRANSFORMS (QFT'S)

There is a useful relationship between MUBs and QFTs. Consider a basis $\mathrm{B}_0 = (|0\rangle, |1\rangle, ..., |d-1\rangle)$ with indices n in the ring Z_d of integers modulo d. The dual basis defined by the quantum Fourier transform is

$$|\theta_k\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} \omega_d^{nk} |n\rangle\,, \qquad \omega_d = \exp\left(i\frac{2\pi}{d}\right).$$

In the particular case $d = 2$, $\omega_2 = -1$ and the θ basis acquires the form

$$|\theta_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,; \quad |\theta_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Note that the two orthogonal bases $\mathrm{B}_0 = (|0\rangle, |1\rangle)$ and $\mathrm{B}_1 = (|\theta_0\rangle, |\theta_1\rangle)$ are mutually unbiased. The third base $\mathrm{B}_2 = (|\psi_0\rangle, |\psi_1\rangle)$, mutually unbiased to them, is obtained from H (the Hadamard matrix) amended by the action to the right of a $\pi/2$ rotation S

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad \rightarrow \qquad HS = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$$

as applied to B_0.

The fact that the B bases for $d = 2$ are also the eigenvectors of the Pauli matrices σ_z, σ_x, and σ_y, respectively, has led to a method of MUBs' construction in dimension d in terms of the generalized Pauli operators

$$X_d|n\rangle = |n+1\rangle\,, \qquad Z_d|n\rangle = \omega_d^n|n\rangle,$$

known as shift and clock operators. For a prime dimension $d = p$, it can be shown [11] that the eigenvectors of the set of unitary operators $Z_p, X_p, X_pZ_p, ..., X_pZ_p^{p-1}$ generate the corresponding $d+1$ MUBs.

Can MUBs be obtained for any d and any (number) field by Fourier transforms as in the case of $d = 2$? In principle, the answer is yes. For this, one should employ such a quantum Fourier transform whose exponent ω now acts on a finite (Galois) field, $G = GF(p^m)$, having characteristic p and $d = p^m$ elements. Denote "$\oplus$" and "$\bullet$" the two operations in the field, corresponding to "+" and "·" in the field of real numbers. Then, the G-Fourier transform reads

$$|\theta_k\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} \omega_p^{n \bullet k} |n\rangle \, .$$

Given any two polynomials k and n in G, there exists a uniquely determined pair a and b in G such that

$$k = a \bullet n \oplus b,$$

where deg $a >$ deg b, so that the exponent in the G-quantum Fourier transform can be written in the form

$$E = n \bullet (a \bullet n \oplus b).$$

The last formula is valid for the case of a prime dimension $d = p$ for which E is an integer. Otherwise, it has to be replaced by the trace of $GF(p^m)$, i.e., a map down to $GF(p)$ defined as follows

$$tr(E) = E + E^p + ... + E^{p^{m-1}} \, , \quad E \in GF(p^m),$$

and so

$$|\theta_b^a\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} \omega_p^{tr[n \bullet (a \bullet n \oplus b)]} |n\rangle \, .$$

This general formula was first obtained by Wootters & Fields and further insights into it have recently been given [12]. In a Galois field of odd characteristic, the latter formula provides us with a set of d bases of index a for the base and index b for the vector in the base, mutually unbiased to each other as well as to the computational base B_0. It is worth noting that this strategy of constructing MUBs fails for characteristic two, since in this case

$$|\sum_{n=0}^{d-1} \omega_2^{tr[n \bullet (a \bullet n \oplus b)]} |n\rangle| = 0 \, ,$$

irrespectively of the values of a and b. In this case, one has to use Galois rings instead of Galois fields in order to find MUBs [12, 13].

Finally, we notice that the same formula provides an interesting relationship between MUBs and quantum phase operators [14]. Indeed, it is known that the Fourier basis $|\theta_k\rangle$ can be derived as the set of eigenvectors of a quantum phase operators $\Theta = \sum_{k=0}^{d-1} \theta_k |\theta_k\rangle\langle\theta_k|$. Thus, viceversa, each base of index a can be associated to a quantum phase operator of the form

$$\Theta^a = \sum_{b=0}^{d-1} \theta_b^a |\theta_b^a\rangle\langle\theta_b^a| \, .$$

The implementation of the MUB concept at the level of quantum phase kets and operators could have important technological consequences for defining generalized measurements of the quantum phase, which is a key feature in quantum computing processes.

CONCLUSION

This short note highlights only the most prominent mathematical problems and physical questions associated with the existence of the maximum sets of MUBs in the Hilbert space of a given dimension. Yet, it should give the reader a fairly good picture of the state of the art of the topic and why the latter entails steadily-increasing attention of both physicists and mathematicians.

REFERENCES

1. W.K. Wootters and B.D. Fields, Ann. Phys. **191**, 363 (1989); I.D. Ivanovic, J. Phys. A **14**, 3241 (1981).
2. G. Zauner, "Quantendesigns", Dissertation in German, Wien (1999).
3. M. Saniga, M. Planat, and H. Rosu, J. Opt. B: Quant. Semiclass. Opt. **6**, L19 (2004), *Preprint* math-ph/0403057.
4. C. Dhara and N.D. Hari Dass, A New Relation between Post and Pre-Optimal Measurement States, *Preprint* quant-ph/0406169.
5. J.M. Renes, R. Blume-Kohout, A.J. Scott, and C.M. Caves, J. Math. Phys. **45**, 2171 (2004).
6. M. Grassl, On SIC-POVMs and MUBs in Dimension 6, *Preprint* quant-ph/0406175.
7. W.K. Wootters, Quantum Measurements and Finite Geometry, *Preprint* quant-ph/0406032.
8. A. Beutelspacher and U. Rosenbaum, *Projective Geometry: From Foundations to Applications*, Cambridge University Press, Cambridge, 1998.
9. H. Levy, *Projective and Related Geometries*, Macmillan, New York, 1964, p. 108.
10. I. Bengtsson, MUBs, Polytopes, and Finite Geometries, *Preprint* quant-ph/0406174.
11. S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
12. A. Klappenecker and M. Rötteler, Lecture Notes in Computer Science **2948**, 137 (2004), *Preprint* quant-ph/0309120.
13. M. Planat, H. Rosu, S. Perrine, M. Saniga, Finite Algebraic Geometrical Structures Underlying Mutually Unbiased Quantum Mesurement, *Preprint* quant-ph/0409081, to be published.
14. D.T. Pegg & S.M. Barnett, Phys. Rev. A **39**, 1665 (1989); M. Planat & H.C. Rosu, Phys. Lett. A **315**, 1 (2003).