International Journal of Modern Physics B
© World Scientific Publishing Company

MULTIPARTITE QUANTUM SYSTEMS: PHASES DO MATTER AFTER ALL

LUIS L. SÁNCHEZ-SOTO

Departamento de Óptica, Facultad de Física, Universidad Complutense, 28040 Madrid, Spain
lsanchez@fis.ucm.es

ANDREI B. KLIMOV

Departamento de Física, Universidad de Guadalajara, 44420 Guadalajara, Jalisco, Mexico
klimov@cencar.udg.mx

HUBERT de GUISE

Department of Physics, Lakehead University, Thunder Bay, Ontario P7B 5E1, Canada
hubert.deguise@lakehead.ca

Received September 27, 2005

A comprehensive theory of phase for finite-dimensional quantum systems is developed. The only physical requirement imposed is that phase is complementary to amplitude. This complementarity is implemented by resorting to the notion of mutually unbiased bases. For a d-dimensional system, where d is a power of a prime, we explicitly construct $d+1$ classes of maximally commuting operators, each one consisting of $d-1$ operators. One of this class consists of diagonal operators that represent amplitudes and, by the finite Fourier transform, operators in this class are mapped to off-diagonal operators that can be appropriately interpreted as phases. The relevant example of a system of qubits is examined in detail.

Keywords: Quantum Phase; Mutually Unbiased Bases; Complementarity.

1. Introduction

The problem of measuring phase has a very long history in quantum mechanics. Since the first attempts of London[1] and Dirac,[2] most efforts have been devoted to elucidate this question for a single harmonic oscillator.[3]

The encoding of information into the phase of d-dimensional systems[4] (also known as qudits) is currently transpiring as an essential ingredient in quantum computation and communication.[5] However, in spite of being a primitive of the theory, the notion of phase for finite-dimensional systems is rather imprecise and, roughly speaking, three quite distinct conceptions can be discerned.

In the first, phase is considered as a parameter and the problem is reduced to the optimal estimation of the value of the phase shift undergone by the system under quantum operations.[6] Although very operational in style, it accommodates perfectly the practical requirements of typical applications in quantum information.

In the second, a semiclassical approach is adopted: the phase is assumed to be linked to the geometry of the state space. For a qubit this is the Poincaré sphere; the phase is identified with the angle between the sate representative and the Z axis.[7] This pictorial understanding of phase as an angle makes intuitive contact with the classical world, but once more merely considers the phase as a state parameter instead of a full quantum variable.

The third major concept emphasizes the idea that phase, as any physical property, must be associated with a selfadjoint operator (or at least with a family of positive operator-valued measures). In this vein, phase operators have been constructed via a polar decomposition for qubits and qutrits.[8]

We wish to look at this fundamental problem from quite a different perspective. On closer examination, one immediately discovers that the idea of complementarity is at the root of all the previous approaches: phase is complementary to amplitude, by which we loosely mean that the precise knowledge of one implies that all possible outcomes of the other are equally probable.[9] This idea of *unbiasedness* leads directly to introduce mutually unbiased bases (MUBs),[10] which have recently been considered with increasing interest because of the central role they play not only in understanding complementarity,[11] but also in specific quantum information tasks, such as protocols of quantum cryptography,[12] Wigner functions in discrete phase spaces,[13] or the so-called mean king problem.[14]

It is known that the maximum number of such bases cannot be greater than $d+1$ and that this limit is certainly reached if d is prime or power of prime.[15] It is not known if there are nonprime-power values of d for which this bound is attained. In any case, we shall be not concerned with this problem in this paper, and assume that we are always working in a power of prime dimension, since this is the interesting case when dealing e.g. with systems of qubits or qutrits.

Quite recently, a number of papers have addressed the explicit construction of MUBs for dimensions that are power of a prime.[16] Here, we revisit a recent construction that resorts to elementary notions of finite field theory and has the advantage of obtaining in a systematic way $d+1$ disjoint classes of maximally commuting unitary matrices (each set having $d-1$ operators).[17] Additionally, the final expression for these MUBs is compact and can be expressed in different bases, in some of which they appear as tensor products of generalized Pauli matrices.

In this paper, we go one step further by noting that one of these classes consists solely of diagonal operators (i.e., amplitudes) that can be mapped, using the finite Fourier transform, to operators acting cyclically on basis states (which we interpret as phases). In this way, we provide a simple and unified picture of what phase is for these composite finite systems.

2. Constructing multicomplementary operators

We begin by considering a system living in a Hilbert space $\mathcal{H}_d$, whose dimension d is a prime number. It is useful to choose a computational basis $|n\rangle$ (where $n = 0, \ldots, d-1$) in $\mathcal{H}_d$ and introduce the basic operators

$$\begin{aligned} X|n\rangle &= |n+1\rangle, \\ Z|n\rangle &= \omega^n |n\rangle, \end{aligned} \tag{1}$$

where $\omega = \exp(2\pi i/d)$ is a dth root of the unity and addition and multiplication must be understood modulo d. These operators are generalizations of the Pauli matrices[18] and generate under multiplication a group known as the generalized Pauli group. They obey

$$ZX = \omega XZ, \tag{2}$$

which is the finite-dimensional version of the Weyl form of the commutation relations.

As anticipated in the Introduction, we can find $d+1$ disjoint classes (each one having $d-1$ commuting operators) such that the corresponding eigenstates form sets of MUBs. The explicit construction starts with the following sets of operators:

$$\{Z^k\}, \qquad \{(XZ^m)^k\}, \qquad k = 1, \ldots, d-1, \quad m = 0, \ldots, d-1. \tag{3}$$

One can easily check that

$$\begin{aligned} \mathrm{Tr}(Z^k Z^{k' \dagger}) = d\, \delta_{kk'}, \qquad \mathrm{Tr}(X^k X^{k' \dagger}) = d\, \delta_{kk'}, \\ \mathrm{Tr}[(XZ^m)^k (XZ^{m'})^{k' \dagger}] = d\, \delta_{kk'} \delta_{mm'}. \end{aligned} \tag{4}$$

These pairwise orthogonality relations indicate that, for every value of m, we generate a maximal set of $d-1$ commuting operators and that all these classes are disjoint. In addition, the common eigenstates of each class m form disjoint sets of unbiased bases. We shall refer to these classes as multicomplementary.

However, for all its simplicity, this construction fails if the dimension of the system is a power of a prime $d = p^n$ (where p is a prime and n is an integer) and operators constructed following (3) no longer form disjoint sets. The root of this failure can be traced to the fact that $\mathbb{Z}_{p^n}$, does not form an algebraic field. We know there exists (up to isomorphisms) exactly one field, written as $\mathbb{F}_d$, with d elements when $d = p^n$.[19] $\mathbb{F}_{p^n}$ can be represented as the field of equivalence classes of polynomials whose coefficients belong to $\mathbb{Z}_p$. The product in the multiplicative group $\mathbb{F}_{p^n}^*$ (i. e, excluding the zero) is defined as the product of the corresponding polynomials modulo a primitive polynomial of degree n irreducible in $\mathbb{Z}_p$. In fact, $\mathbb{F}_{p^n}^*$ is a cyclic group generated by powers of a primitive element α, which is a monic irreducible polynomial of degree n. This establishes a natural order for the field elements, and we use this order to label the elements of a basis in $\mathcal{H}_d$ as follows:

$$\{|0\rangle, |\alpha\rangle, |\alpha^2\rangle, \ldots, |\alpha^{d-1}\rangle\}. \tag{5}$$

Our solution to the problem of MUBs in composite dimension consists in using elements of $\mathbb{F}_d$, instead of natural numbers, to label the classes of complementary operators.

To proceed, we observe that elements of F_{p^n} form an additive group, for which we can introduce additive characters as a map that fulfills

$$\chi(\theta_1)\chi(\theta_2) = \chi(\theta_1 + \theta_2), \qquad \theta_1, \theta_2 \in \mathbb{F}_{p^n}. \tag{6}$$

All of these additive characters have the form

$$\chi(\theta) = \exp\left[\frac{2\pi i}{p}\,\mathrm{tr}(\theta)\right], \tag{7}$$

where the trace of a field element $\theta \in \mathbb{F}_{p^n}$ is

$$\mathrm{tr}(\theta) = \theta + \theta^p + \theta^{p^2} + \ldots + \theta^{p^{n-1}}. \tag{8}$$

Note that we distinguish the trace over field elements from the more common trace of matrices, by using the lower case "tr" for the former. The trace has remarkably simple properties, the most important for us being that it is linear and that it is always an element of the prime field $\mathbb{Z}_p$.

Next, we introduce the following operators with respect to the basis (5):

$$\begin{aligned} Z_q &= |0\rangle\langle 0| + \sum_{k=1}^{d-1} \chi(\alpha^{q+k})\, |\alpha^k\rangle\langle\alpha^k|, \\ X_r &= |\alpha^r\rangle\langle 0| + \sum_{k=1}^{d-1} |\alpha^k + \alpha^r\rangle\langle\alpha^k|, \end{aligned} \tag{9}$$

with $q, r = 0, \ldots, d-2$, which implies

$$\begin{aligned} Z_q|\alpha^k\rangle &= \chi(\alpha^{q+k})|\alpha^k\rangle, \\ X_r|\alpha^k\rangle &= |\alpha^k + \alpha^r\rangle. \end{aligned} \tag{10}$$

These operators inherit properties that naturally generalize the properties of matrices in Eq. (3). In fully analogy with the sets in (3), we can generate operators from X_q and Z_q; they will be of the form $X_q Z_r$. Linear independence and orthogonality are guaranteed, in the sense that [compare equation (4)]

$$\begin{aligned} \mathrm{Tr}(Z_q Z_{q'}^\dagger) = d\,\delta_{qq'}, &\qquad \mathrm{Tr}(X_q X_{q'}^\dagger) = d\,\delta_{qq'}, \\ \mathrm{Tr}[(X_q Z_r)(X_{q'} Z_{r'})^\dagger] &= d\,\delta_{qq'}\delta_{rr'}. \end{aligned} \tag{11}$$

It is clear from (11) that the sets [compare Eq. (3)]

$$\{Z_q\}, \qquad \{X_q Z_{q+r}\}, \qquad q, r = 0, \ldots, d-2, \tag{12}$$

are disjoint and that every element of a set with a fixed value r commutes with every other element in the same set: they define multicomplementary operators.

3. Complementary sets and finite Fourier transform

In the prime-dimensional case, we make the very important observation that, starting from Z, it is possible to obtain any element of the form $(XZ^m)^k$ by using a combination of only two operators F and V defined as follows: F is the finite Fourier transform[4]

$$F = \frac{1}{\sqrt{d}} \sum_{n,n'=0}^{d-1} \omega^{nn'} \, |n\rangle\langle n'|, \tag{13}$$

and V is the diagonal transformation (assuming d is odd)

$$V = \sum_{n=0}^{d-1} \omega^{-(n^2-n)(d+1)/2} \, |n\rangle\langle n|. \tag{14}$$

Indeed this is the case, since one easily verifies that

$$X = F^\dagger \, Z \, F, \tag{15}$$

much in the spirit of the standard way of looking at complementary variables in the infinite-dimensional Hilbert space: the position and momentum eigenstates are Fourier transform one of the other. On the other hand, the diagonal transformation V acts as a Z-right shift[a]:

$$XZ^m = V^{\dagger m} \, X \, V^m. \tag{16}$$

This is quite remarkable, since this prescription determines without ambiguity (except for a trivial phase) the complementary operators to the amplitude Z, which can be appropriately called phases.

For composite systems, we can easily translate the previous discussion: the finite Fourier transform F, when expressed in the basis $|\alpha^k\rangle$, takes the form

$$F = \frac{1}{\sqrt{d}} \left[|0\rangle\langle 0| + \sum_{k,k'=1}^{d-1} \chi(\alpha^{k'+k}) |\alpha^{k'}\rangle\langle\alpha^k| + \sum_{k=1}^{d-1} \big(|0\rangle\langle\alpha^k| + |\alpha^k\rangle\langle 0| \big) \right], \tag{17}$$

[a] The case $d = 2$ needs minor modifications. In fact, it turns out that one cannot find a diagonal unitary transformation V such that $X \rightarrow XZ$. For this reason, instead of XY the matrix Y is defined as iXZ, so that $Y = V^\dagger \, X \, V$, where V is

$$V = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}.$$

in such a way that F is set up to transform the operators Z_q into X_q:

$$X_q = F^\dagger \, Z_q \, F. \tag{18}$$

Finally, the diagonal operators similar to (16) transforming X_q to $X_q Z_r$ can be written as

$$V_q^{(r)} = |0\rangle\langle 0| + \sum_{k=1}^{d-1} \bar{\chi}(2^{-1}\alpha^{r+2k-q}) |\alpha^k\rangle\langle\alpha^k|, \tag{19}$$

where $\bar{\chi}$ means conjugate character and 2^{-1} is an element of $\mathbb{Z}_p$; in particular, if $p = 2N+1$ we have $2^{-1} = N+1$.

4. Application: systems of qubits

We begin with the simplest example of a quantum system of composite dimension: two qubits described in a four-dimensional Hilbert space $\mathcal{H}_4$. To construct multi-complementary operators, we start from the field $\mathbb{F}_4$ containing four elements. The polynomial

$$\theta^2 + \theta + 1 = 0 \tag{20}$$

is irreducible in $\mathbb{Z}_2$ and the primitive element α is defined as a root of (20). In consequence, the four elements of $\mathbb{F}_4$ as in Eq. (5) can be written as

$$\{0, 1, \alpha, \alpha+1\}, \tag{21}$$

where we have taken into account arithmetic modulo 2 and the fact that if α satisfies Eq. (20), then we have the relations

$$\alpha^2 = \alpha + 1, \qquad \alpha^3 = 1. \tag{22}$$

A direct application of the definition (7) gives

$$\chi(0) = 1, \quad \chi(\alpha) = -1, \quad \chi(\alpha^2) = -1, \quad \chi(\alpha^3) = 1. \tag{23}$$

Without going into technical details, one can always chose a basis such that

$$\begin{aligned} Z_0 &\mapsto \sigma_z\sigma_z, & X_0 &\mapsto \sigma_x\sigma_x, \\ Z_1 &\mapsto \sigma_z\mathbb{1}, & X_1 &\mapsto \sigma_x\mathbb{1}, \\ Z_2 &\mapsto \mathbb{1}\sigma_z, & X_2 &\mapsto \mathbb{1}\sigma_z. \end{aligned} \tag{24}$$

Here σ_x, σ_y, and σ_z denote the Pauli matrices and we have suppressed the tensor multiplication sign.

The set (X_0, X_1, X_2) constitutes the phase operators for the problem at hand.[20] If we take a maximally entangled state such as

$$|\Phi\rangle = \frac{1}{\sqrt{2}}[|00\rangle + e^{i\varphi}|11\rangle], \tag{25}$$

we get

$$\langle\sigma_x\sigma_x\rangle = \cos\varphi, \quad \langle\sigma_x\mathbb{1}\rangle = 0, \quad \langle\mathbb{1}\sigma_x\rangle = 0. \tag{26}$$

This interesting result holds true also for a system of N qubits: we can always factorize our phase operators in the form $(\mathbb{1}\mathbb{1}\ldots\mathbb{1}\sigma_x, \mathbb{1}\mathbb{1}\ldots\sigma_x\mathbb{1}\sigma_x, \ldots\mathbb{1}\mathbb{1}\ldots\sigma_x\sigma_x, \ldots\sigma_x\sigma_x\ldots\sigma_x\sigma_x)$. For maximally entangled states only $\langle\sigma_x\sigma_x\ldots\sigma_x\sigma_x\rangle$ is nonzero, all the other average values are zero. The result is obviously independent of the factorization. The rich consequences of this approach lie out of the scope of this paper and will be presented elsewhere.

5. Concluding remarks

In summary, we have used an elegant construction of MUBs to provide phase operators for composite finite systems that are devoid of any ambiguity associated with the nonuniqueness of polar decomposition of ladder operators. Phase and amplitudes are elegantly related by a finite Fourier transform, much like positions and momenta are related by an ordinary Fourier transform in infinite-dimensional systems. This provides an appealing way of treating a concept as central as phases.

References

1. F. London, *Z. Phys.* **37**, 915 (1926).
2. P. A. M. Dirac, *Proc. R. Soc. London Ser. A* **114**, 243 (1927).
3. W. P. Schleich and S. M. Barnett (eds) *Phys. Scr.* **T48** (1993) (special issue on *Quantum Phase and Phase Dependent Measurements*); R. Lynch, *Phys. Rep.* **256**, 367 (1995); R. Tanaś, A. Miranowicz and T. Gantsog, *Prog. Opt.* **36**, 161 (1996); V. Peřinová, A. Lukš and J. Peřina, *Phase in Optics* (World Scientific, Singapore, 1998); A. Luis and L. L. Sánchez-Soto, *Prog. Opt.* **41**, 421 (2000).
4. A. Vourdas, *Rep. Prog. Phys.* **67**, 267 (2004).
5. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2001); A. Galindo and M. A. Martín-Delgado, *Rev. Mod. Phys.* **74**, 347 (2002); M. Keyl *Phys. Rep.* **369**, 431 (2002).
6. C. W. Helstrom, *Quantum Detection and Estimation Theory*, (Academic, New York, 1976); A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, (North-Holland, Amsterdam, 1982); D. Bruß M. Cinchetti, G. M. D' Ariano and C. Macchiavello, *Phys. Rev. A* **62**, 012302 (2000); J. Řeháček, Z. Hradil, M. Dušek, O. Haderka and M. Hendrych, *J. Opt. B* **2**, 237 (2000); C. Macchiavello, *Phys. Rev. A* **67**, 062302 (2003); A. I. Lvovsky, *J. Opt. B* **6**, S556 (2004).
7. C. Cohen-Tannoudji, B. Diu and F. Laloë, *Quantum Mechanics* (Addison, New York, 1992); P. K. Arvind, K. S. Mallesh and N. Mukunda, *J. Phys. A* **30**, 2417 (1997); A. B. Klimov, L. L. Sánchez-Soto, H. de Guise and G. Björk, *J. Phys. A* **37**, 4097 (2004).
8. J. M. Lévy-Leblond, *Rev. Mex. Fis.* **22**, 17 (1973); A. Vourdas, *Phys. Rev. A* **41**, 1653 (1990); D. Ellinas *J. Math. Phys.* **32**, 135 (1990); A. Luis L. L. Sánchez-Soto *Phys. Rev. A* **56**, 994 (1997); L. L. Sánchez-Soto, J. Delgado, A. B. Klimov and G. Björk *Phys. Rev. A* **66**, 042112 (2002).
9. J. A. Wheeler and W. H. Zurek (eds) *Quantum Theory and Measurement* (Princeton University Press, Princeton, 1983).
10. W. K. Wootters, *Ann. Phys. (N. Y.)* **176**, 1 (1987).
11. K. Kraus, *Phys. Rev. D* **35**, 3070 (1987); J. Lawrence, Č. Brukner and A. Zeilinger, *Phys. Rev. A* **65**, 032320 (2002); S. Chaturvedi *Phys. Rev. A* **65**, 044301 (2002).

12. H. Bechmann-Pasquinucci and A. Peres, *Phys. Rev. Lett.* **85**, 3313 (2000); N. J. Cerf, M. Bourennane, A. Karlsson and N. Gisin, *Phys. Rev. Lett.* **88**, 127902 (2000).
13. W. K. Wootters, *IBM J. Res. Dev.* **48** 99 (2004); K. S. Gibbons, M. J. Hoffman and W. K. Wootters, *Phys. Rev. A*, **70**, 062101 (2004).
14. L. Vaidman, Y. Aharonov and D. Z. Albert, *Phys. Rev. Lett.* **58**, 1385 (1987); B.-G. Englert and Y. Aharonov, *Phys. Lett. A* **284**, 1 (2001); P. K. Aravind, *Z. Naturforschung.* **26**, 350 (2003); O. Schulz, R. Steinhüubl, M. Weber, B.-G. Englert, C. Kurtsiefer and H. Weinfurter, *Phys. Rev. Lett.* **90**, 177901 (2003); J. P. Paz, A. J. Roncaglia, and M. Saraceno, *Phys. Rev. A* **72**, 012309 (2005).
15. I. D. Ivanovic, *J. Phys. A* **14**, 3241 (1981); A. R. Calderbank, J. Cameron, W. M. Kantor and J. J. Seidel, *Proc. London Math. Soc.* **75**, 436 (1997); W. K. Wootters and B. D. Fields, *Ann. Phys. (N. Y.)* **191**, 363 (1987).
16. S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury and F. Vatan, *Algorithmica* **34**, 512 (2002); A. Klappenecker and M. Rötteler, “Constructions of Mutually Unbiased Bases”, quant-ph/0309120; T. Durt, “A new expression for mutually unbiased bases in prime power dimensions”, quant-ph/0409090; A. O. Pittenger and M. H. Rubin, *Linear Algebra Appl.* **390**, 255 (2004); P. Wocjan and T. Beth, “New Construction of Mutually Unbiased Bases in Square Dimensions”, quant-ph/0407081; M. Planat, H. Rosu, S. Perrine and M. Saniga, “Finite Algebraic Geometrical Structures Underlying Mutually Unbiased Quantum Measurements”, quant-ph/0409081; C. Archer, *J. Math. Phys.* **46**, 22106 (2005); P. O. Boykin, M. Sitharam, P. H. Tiep and P. Wocjan, “Mutually Unbiased Bases and Orthogonal Decompositions of Lie Algebras”, quant-ph/0506089;
17. A. B. Klimov, L. L. Sánchez-Soto and H. de Guise, *J. Phys. A* **38**, 2747 (2005).
18. J. Patera and H. Zassenhaus *J. Math. Phys.* **29**, 665 (1988).
19. R. Lidl and H Niederreiter, *Introduction to Finite Fields and their Applications* (Cambridge University Press, Cambridge, 1986).
20. M. Planat and H. C. Rosu, “Mutually Unbiased Phase States, Phase Uncertainties, and Gauss Sums” quant-ph/0506128.