Mutually unbiased phase states, phase uncertainties, and Gauss sums

M. Planat[1,a] and H. Rosu[2]

[1] Institut FEMTO-ST, Departement LPMO, 32 avenue de l'Observatoire, 25044 Besançon Cedex, France
[2] IPICyT, Apdo Postal 3-74, Tangamanga, San Luis Potosí, Mexico

Abstract. Mutually unbiased bases (MUBs), which are such that the inner product between two vectors in different orthogonal bases is a constant equal to $1/\sqrt{d}$, with d the dimension of the finite Hilbert space, are becoming more and more studied for applications such as quantum tomography and cryptography, and in relation to entangled states and to the Heisenberg-Weil group of quantum optics. Complete sets of MUBs of cardinality $d+1$ have been derived for prime power dimensions $d = p^m$ using the tools of abstract algebra. Presumably, for non prime dimensions the cardinality is much less. Here we reinterpret MUBs as quantum phase states, i.e. as eigenvectors of Hermitian phase operators generalizing those introduced by Pegg and Barnett in 1989. We relate MUB states to additive characters of Galois fields (in odd characteristic p) and to Galois rings (in characteristic 2). Quantum Fourier transforms of the components in vectors of the bases define a more general class of MUBs with multiplicative characters and additive ones altogether. We investigate the complementary properties of the above phase operator with respect to the number operator. We also study the phase probability distribution and variance for general pure quantum electromagnetic states and find them to be related to the Gauss sums, which are sums over all elements of the field (or of the ring) of the product of multiplicative and additive characters. Finally, we relate the concepts of mutual unbiasedness and maximal entanglement. This allows to use well studied algebraic concepts as efficient tools in the study of entanglement and its information aspects.

PACS. 02.10.De Algebraic structures and number theory – 03.65.Ud Entanglement and quantum nonlocality (e.g. EPR paradox, Bell's inequalities, GHZ states, etc.) – 03.65.Fd Algebraic methods

1 Introduction

In quantum mechanics, orthogonal bases of a Hilbert space $\mathcal{H}_q$ of finite dimension q are mutually unbiased if inner products between all possible pairs of vectors of distinct bases are all equal to $1/\sqrt{q}$. Eigenvectors of ordinary Pauli spin matrices (i.e. in dimension $q = 2$) provide the best known example. It has been shown that in dimension $q = p^m$ which is the power of a prime p, the complete sets of mutually unbiased bases (MUBs) result from Fourier analysis over a Galois field F_q (in odd characteristic p) [1] or of Galois ring R_{4^m} (in even characteristic 2) [2]. In [3,4], the reader can find an exhaustive literature on MUBs. Complete sets of MUBs have an intrinsic geometrical interpretation, and were related to discrete phase spaces [3,5,6], finite projective planes [7,8], convex polytopes [9], and complex projective 2-designs [10,11]. There are hints on the relation to symmetric informationally complete positive operator measures (SIC-POVMs) [12–15], and to Latin squares [16].

There are strong motivations to embark on detailed studies of MUBs. First, they enter rigorous treatments of Bohr's principle of complementarity that distinguishes between quantum and classical systems at the practical level of measurements. This fundamental quantum principle introduces the idea of complementary pairs of observables in the sense that precise measurement of one of them implies that possible outcomes of the other (when measured) are equally probable. In the nondegenerate case, if an observable O represented by a q times q Hermitian matrix is measured in a quantum system prepared in the eigenbase of its complementary counterpart O_c, then the probability to find the system in one of the eigenstates of O is just $1/q$ as corresponding to mutually unbiased inner products. Another domain of applications where MUBs have been found to play an important role is the field of secure quantum key exchange (quantum cryptography). In the area of quantum state tomography, one should use MUBs for a complete reconstruction of an unknown quantum state [17].

In this paper we approach the MUBs theory from the point of view of the theory of additive and multiplicative

a e-mail: `planat@lpmo.edu`

characters in Galois number field theory. The multiplicative characters $\psi_k(n) = \exp(2i\pi nk/(q-1))$, $k = 0...q-2$, are well known since they constitute the basis for the ordinary discrete Fourier transform. But in order to construct MUBs, the additive characters introduced below are the ones which are useful. This construction is implicit in some previous papers [1,2,4], and is now being fully recognized [18,19],

An interesting consequence is the following: the discrete Fourier transform in $\mathcal{Z}_q$ has been used by Pegg and Burnett [20] as a definition of phase states $|\theta_k\rangle$, $k = 0...q-1$, in $\mathcal{H}_q$. The phase states $|\theta_k\rangle$ could be considered as eigenvectors of a properly defined Hermitian phase operator Θ_{PB}. Phase properties and phase fluctuations attached to particular field states were extensively described. In particular the classical phase variance $\pi^2/3$ could be recovered.

We construct here a phase operator Θ_{Gal} having phase MUBs as eigenvectors. In contrast to the case of Θ_{PB}, we find that the phase fluctuations of Θ_{Gal} can be expressed in terms of Gauss sums over the finite number field F_q, and could be in principle smaller than those due to Θ_{PB}. This points to the fact that the phase MUBs may be of interest for quantum signal processing. Character sums and Gauss sums which are useful for optimal bases of m-qudits (p odd) are also generalized to optimal bases of m-qubits ($p = 2$).

2 Phase MUBs in odd prime characteristic

2.1 Mathematical preliminaries

The key relation between Galois fields F_q and MUBs is the theory of characters. This has not been recognized before and here we use the standpoint of characters as the most general way of considering previous results and also as a better criterium for elaborating on future results.

A Galois field is a finite set structure endowed with two group operations, the addition "+" and the multiplication "·". The field F_q can be represented as classes of polynomials obtained by computing modulo an irreducible polynomial over the ground field $F_p = \mathcal{Z}_p$, the integers modulo p [21]. A Galois field exists if and only if $q = p^m$. We also recall that $F_q[x]$ is the standard notation for the set of polynomials in x with coefficients in F_q.

A character $\kappa(g)$ over an Abelian group G is a (continuous) map from G to the field of complex numbers $\mathcal{C}$ of unit modulus, i.e. such that $|\kappa(g)| = 1$, $g \in G$.

We start with a map from the extended field F_q to the ground field F_p which is called the trace function

$$\mathrm{tr}(x) = x + x^p + ... + x^{p^{m-1}} \in F_p, \quad \forall \ x \in F_q. \quad (1)$$

Using (1), an additive character over F_q is defined as

$$\kappa(x) = \omega_p^{\mathrm{tr}(x)}, \quad \omega_p = \exp\left(\frac{2i\pi}{p}\right), \quad x \in F_q. \quad (2)$$

The main property is that it satisfies $\kappa(x + y) = \kappa(x)\kappa(y)$, $x, y \in F_q$.

On the other hand, the multiplicative characters are of the form

$$\psi_k(n) = \omega_{q-1}^{nk}, \quad k = 0...q-2, n = 0...q-2. \quad (3)$$

In the present research, the construction of Galois phase MUBs will be related to character sums with polynomial arguments $f(x)$ also called Weil sums [2]

$$W_f = \sum_{x \in F_q} \kappa(f(x)). \quad (4)$$

In particular, (theorem 5.38 in [21]), for a polynomial $f_d(x) \in F_q[x]$ of degree $d \geq 1$, with $gcd(d,q) = 1$, one gets $W_{f_d} \leq (d-1)q^{1/2}$.

The quantum fluctuations arising from the phase MUBs will be found to be related to Gauss sums of the form

$$G(\psi, \kappa) = \sum_{x \in F_q^*} \psi(x)\kappa(x) , \quad (5)$$

where $F_q^* = F_q - \{0\}$. Using the notation ψ_0 for a trivial multiplicative character $\psi = 1$, and κ_0 for a trivial additive character $\kappa = 1$ the Gaussian sums (5) satisfy $G(\psi_0, \kappa_0) = q - 1$; $G(\psi_0, \kappa) = -1$; $G(\psi, \kappa_0) = 0$ and $|G(\psi, \kappa)| = q^{1/2}$ for nontrivial characters κ and ψ.

2.2 Galois quantum phase states

We now introduce a class of quantum phase states as a "Galois" discrete quantum Fourier transform of the Galois number kets

$$|\theta^{(y)}\rangle = \frac{1}{\sqrt{q}} \sum_{n \in F_q} \psi_k(n)\kappa(yn)|n\rangle, \quad y \in F_q \quad (6)$$

in which the coefficient in the computational base $\{|0\rangle, |1\rangle, ..., |q-1\rangle\}$ represents the product of an arbitrary multiplicative character $\psi_k(n)$ by an arbitrary additive character $\kappa(yn)$.

It is easy to show that previous basic results in this area can be obtained as particular cases of (6). Indeed:

- **Pegg and Barnett (1989)**: for $\kappa = \kappa_0$ and $\psi \equiv \psi_k(n)$, one recovers the ordinary quantum Fourier transform over $\mathcal{Z}_q$. It has been shown [20] that the corresponding states

$$|\theta_k\rangle = \frac{1}{\sqrt{q}} \sum_{n \in \mathcal{Z}_q} \psi_k(n)|n\rangle, \quad (7)$$

are eigenstates of the Hermitian phase operator

$$\Theta_{PB} = \sum_{k \in \mathcal{Z}_q} \theta_k |\theta_k\rangle\langle\theta_k|, \quad (8)$$

with eigenvalues $\theta_k = \theta_o + 2\pi k/q$, θ_0 an arbitrary initial phase;

- **Wootters and Fields (1989)**: we recover the result of Wootters and Fields in a more general form by employing the Euclidean division theorem (see theorem 11.19 in [22]) for the field F_q, which says that given any two polynomials y and n in F_q, there exists a uniquely determined pair $(a, b) \in F_q \times F_q$, such that $y = an + b$, $\deg(b) < \deg(a)$. Using the decomposition of the exponent in (6), we obtain

$$|\theta_b^a\rangle = \frac{1}{\sqrt{q}} \sum_{n \in F_q} \psi_k(n)\kappa(an^2 + bn)|n\rangle, \quad a, b \in F_q. \quad (9)$$

(The result of Wootters and Fields corresponds to the trivial multiplicative character $\psi_0 = 1$.) Equation (9) defines a set of q bases (with index a) of q vectors (with index b). Using Weil sums (4) it is easily shown that, for q odd, so that $gcd(2, q) = 1$, the bases are orthogonal and mutually unbiased to each other and to the computational base

$$|\langle \theta_b^a | \theta_d^c \rangle| = \left| \frac{1}{q} \sum_{n \in F_q} \omega_p^{\mathrm{tr}((c-a)n^2 + (d-b)n)} \right|$$
$$= \begin{cases} \delta_{bd} & \text{if } c = a \text{ (orthogonality)} \\ 1/\sqrt{q} & \text{if } c \neq a \text{ (unbiasedness)}. \end{cases} \quad (10)$$

3 Quantum fluctuations of phase MUBs in odd prime characteristic

Following Pegg and Barnett, a good procedure to examine the phase properties of a quantized electromagnetic field state is by introducing a phase operator and this was one of the reasons that led them to introduce their famous Hermitian phase operator Θ_{PB}. In Section 6 of their seminal paper they showed "for future reference" how their phase operator could be employed to achieve this goal. In this section we proceed along the same lines using the phase form of the Wootters-Field MUBs.

3.1 The Galois phase operator

On the other hand, the phase MUBs as given in (9) are eigenstates of a "Galois" quantum phase operator

$$\Theta_{\mathrm{Gal}} = \sum_{b \in F_q} \theta_b |\theta_b^a\rangle\langle\theta_b^a|, \quad a, b \in F_q. \quad (11)$$

with eigenvalues $\theta_b = 2\pi b/q$. We use this fact to perform several calculations of quantum phase expectation values and phase variances for these MUBs.

Using (9) in (11) and the properties of the field theoretical trace the Galois quantum phase operator reads

$$\Theta_{\mathrm{Gal}} = \frac{2\pi}{q^2} \sum_{m,n \in F_q} \psi_k(n - m)\omega_p^{\mathrm{tr}[a(n^2 - m^2)]} S(n, m)|n\rangle\langle m|,$$
$$\text{with } S(n, m) = \sum_{b \in F_q} b\omega_p^{\mathrm{tr}[b(n-m)]}. \quad (12)$$

In the diagonal matrix elements, we have the partial sums

$$S(n, n) = \frac{q(q-1)}{2}, \quad (13)$$

so that $\langle n|\Theta_{\mathrm{Gal}}|n\rangle = \pi(q-1)/q$. In the non-diagonal matrix elements, the partial sums can be calculated from

$$\sum_{b \in F_q} bx^b = x(1 + 2x + 3x^2 + ... + qx^{q-1})$$
$$= x\left[\frac{1 - x^q}{(1-x)^2} - \frac{qx^q}{1-x}\right] = \frac{xq}{x-1}, \quad (14)$$

where we introduced $x = \omega_p^{\mathrm{tr}(n-m)}$ and we made use of the relation $x^q = 1$. Finally, we get

$$S(m, n) = \frac{q}{1 - \omega_p^{\mathrm{tr}(m-n)}}. \quad (15)$$

3.2 The Galois phase-number commutator

Using (12) and the Galois number operator

$$N = \sum_{l \in F_q} l|l\rangle\langle l|, \quad (16)$$

the matrix elements of the phase-number commutator $[\Theta_{\mathrm{Gal}}, N]$ are calculated as

$$u_{\mathrm{Gal}}(n, m) =$$
$$\frac{2\pi}{q^2}(n - m)\psi_k(n - m)\omega_p^{\mathrm{tr}[a(n^2 - m^2)]} S(n, m). \quad (17)$$

The diagonal elements vanish, the corresponding matrix is anti-Hermitian since $u_{\mathrm{Gal}}(n, m) = -u_{\mathrm{Gal}}^\dagger(m, n)$, and the states are pseudo-classical since $\lim_{q\to\infty} u_{\mathrm{Gal}}(n, m) = 0$. These properties are similar to those of the Pegg and Barnett commutator.

3.3 Galois phase properties of a pure quantum electromagnetic state

For the evaluation of the phase properties of a general pure state of an electromagnetic field mode in the Galois number field we proceed similarly to Pegg and Barnett. Thus, we consider the pure state of the form

$$|f\rangle = \sum_{n \in F_q} u_n|n\rangle, \quad \text{with } u_n = \frac{1}{\sqrt{q}} \exp(in\beta), \quad (18)$$

where β is a real parameter, and we sketch the computation of the phase probability distribution $|\langle\theta_b|f\rangle|^2$, the phase expectation value $\langle\Theta_{\mathrm{Gal}}\rangle = \sum_{b \in F_q} \theta_b|\langle\theta_b|f\rangle|^2$ and the phase variance $\langle\Delta\Theta_{\mathrm{Gal}}^2\rangle = \sum_{b \in F_q}(\theta_b - \langle\Theta_{\mathrm{Gal}}\rangle)^2|\langle\theta_b|f\rangle|^2$, respectively (the upper index a for the base is implicit and we discard it for simplicity).

The two factors in the expression for the probability distribution

$$\frac{1}{q^2}\left[\sum_{n\in F_q}\psi_k(-n)\exp(in\beta)\kappa(-an^2-bn)\right]$$
$$\times\left[\sum_{m\in F_q}\psi_k(m)\exp(-im\beta)\kappa(am^2+bm)\right],\quad(19)$$

have absolute values bounded by the absolute value of generalized Gauss sums $G(\psi,\kappa)=\sum_{x\in F_q}\psi(g(x))\kappa(f(x))$, with $f,g\in F_q[x]$. Weil [23] showed that for $f(x)$ of degree d with $gcd(d,q)=1$ as in (4), under the constraint that for the multiplicative character ψ of order s, the polynomial $g(x)$ should not be a sth power in $F_q[x]$ and with ν distinct roots in the algebraic closure of F_q, the order of magnitude of the sums is $(d+\nu-1)\sqrt{q}$. For a trivial multiplicative character ψ_0, and $\beta=0$, the overall bound is $|\langle\theta_b|f\rangle|^2\leq 1/q$ and it follows that the absolute value of the Galois phase expectation value is bounded from above as expected for a common phase operator

$$|\langle\Theta_{\text{Gal}}\rangle|\leq\frac{2\pi}{q^2}\sum_{b\in F_q}b\leq\pi.\quad(20)$$

The exact formula for the phase expectation value reads

$$\langle\Theta_{\text{Gal}}\rangle=\frac{2\pi}{q^3}\sum_{m,n\in F_q}e^\beta(m,n)S(m,n),\quad(21)$$

where $e^\beta(m,n)=\psi_k(m-n)\exp[i(n-m)\beta]\chi[a(m^2-n^2)]$ and the sums $S(m,n)$ were defined in (13) and (15). The set of all the q diagonal terms $m=n$ in $\langle\Theta_{\text{Gal}}\rangle$ contributes an order of magnitude $(2\pi/q^3)qS(n,n)\simeq\pi$. The contribution from off-diagonal terms in (21) are not easy to evaluate analytically; we were able to show that for them one has $|S(m,n)|=(q/2)|\sin[(\pi/p)\text{tr}(n-m)]|^{-1}$.

The phase variance can be written as

$$\langle\Delta\Theta_{\text{Gal}}^2\rangle=\sum_{b\in F_q}(\theta_b^2-2\theta_b\langle\Theta_{\text{Gal}}\rangle)|\langle\theta_b|f\rangle|^2.\quad(22)$$

The term $\langle\Theta_{\text{Gal}}\rangle^2\sum_{b\in F_q}|\langle\theta_b|f\rangle|^2$ does not contribute since it is proportional to the Weil sum $\sum_{b\in F_q}\omega_p^{\text{tr}(b(n-m))}=0$. As a result a cancellation of the quantum phase fluctuations may occur in (22) from the two extra terms of opposite sign. But the calculation are again not easy to perform analytically. For the first term one gets $2(2\pi/q^2)^2\sum_{m,n\in F_q}e^\beta(m,n)|S(m,n)|^2$. The second term in (22) is $-2\sum_{b\in F_q}\theta_b\langle\Theta_{\text{Gal}}\rangle|\langle\theta_b|f\rangle|^2=-2\langle\Theta_{\text{Gal}}\rangle^2$. Partial cancellation occurs in the diagonal terms of (22) leading to the contribution $\approx-2\pi^2/3$ which is still twice (in absolute value) the amount of phase fluctuations in the classical regime. A closed form for the estimate of the non-diagonal terms is still an open problem.

4 Phase MUBs for m-qubits

4.1 Mathematical preliminaries

The Weil sums (4) which have been proved useful in the construction of MUBs in odd characteristic p (and odd dimension $q=p^m$), are not useful in characteristic $p=2$, since in this case the degree 2 of the polynomial $f_d(x)$ is such that $gcd(2,q)=2$.

An elegant method for constructing complete sets of MUBs of m-qubits was found by Klappenecker and Rötteler [2]. It makes use of objects belonging to the context of quaternary codes [24], the so-called Galois rings R_{4^m}; we refer the interested reader to their paper for more mathematical details. We present a brief sketch in the following.

Any element $y\in R_{4^m}$ can be uniquely determined in the form $y=a+2b$, where a and b belong to the so-called Teichmüller set $\mathcal{T}_m=(0,1,\xi,...,\xi^{2^m-2})$, where ξ is a nonzero element of the ring which is a root of the so-called basic primitive polynomial $h(x)$ [2]. Moreover, one finds that $a=y^{2^m}$. We can also define the trace to the base ring $\mathcal{Z}_4$ by the map

$$\tilde{\text{tr}}(y)=\sum_{k=0}^{m-1}\sigma^k(y),\quad(23)$$

where the summation runs over R_{4^m} and the Frobenius automorphism σ reads

$$\sigma(a+2b)=a^2+2b^2.\quad(24)$$

In the Galois ring of characteristic 4 the additive characters are

$$\tilde{\kappa}(x)=\omega_4^{\tilde{\text{tr}}(x)}=i^{\tilde{\text{tr}}(x)}.\quad(25)$$

The Weil sums (4) are replaced by the exponential sums [2]

$$\Gamma(y)=\sum_{u\in\mathcal{T}_m}\tilde{\kappa}(yu),\quad y\in R_{4^m}\quad(26)$$

which satisfy

$$|\Gamma(y)|=\begin{cases}0 & \text{if } y\in 2\mathcal{T}_m,\ y\neq 0\\2^m & \text{if } y=0\\\sqrt{2^m} & \text{otherwise.}\end{cases}\quad(27)$$

Gauss sums for Galois rings were constructed [26]

$$G_y(\tilde{\psi},\tilde{\kappa})=\sum_{x\in R_{4^m}}\tilde{\psi}(x)\tilde{\kappa}(yx),\quad y\in R_{4^m},\quad(28)$$

where the multiplicative character $\bar{\psi}(x)$ can be made explicit [26].

Using the notation $\tilde{\psi}_0$ for a trivial multiplicative character and $\tilde{\kappa}_0$ for a trivial additive character, the Gaussian sums (28) satisfy $G_y(\tilde{\psi}_0,\tilde{\kappa}_0)=4^m$; $G_y(\tilde{\psi},\tilde{\kappa}_0)=0$ and $|G_y(\tilde{\psi},\tilde{\kappa})|\leq 2^m$.

$$(|0\rangle, |1\rangle, |2\rangle, |3\rangle);$$
$$\tfrac{1}{2}[|0\rangle + |1\rangle + |2\rangle + |3\rangle, |0\rangle + |1\rangle - |2\rangle - |3\rangle, \ |0\rangle - |1\rangle - |2\rangle + |3\rangle, |0\rangle - |1\rangle + |2\rangle - |3\rangle]$$
$$\tfrac{1}{2}[|0\rangle - |1\rangle - i|2\rangle - i|3\rangle, |0\rangle - |1\rangle + i|2\rangle + i|3\rangle, \ |0\rangle + |1\rangle + i|2\rangle - i|3\rangle, |0\rangle + |1\rangle - i|2\rangle + i|3\rangle]$$
$$\tfrac{1}{2}[|0\rangle - i|1\rangle - i|2\rangle - |3\rangle, |0\rangle - i|1\rangle + i|2\rangle + |3\rangle, \ |0\rangle + i|1\rangle + i|2\rangle - |3\rangle, |0\rangle + i|1\rangle - i|2\rangle + |3\rangle]$$
$$\tfrac{1}{2}[|0\rangle - i|1\rangle - |2\rangle - i|3\rangle, |0\rangle - i|1\rangle + |2\rangle + i|3\rangle, \ |0\rangle + i|1\rangle + |2\rangle - i|3\rangle, |0\rangle + i|1\rangle - |2\rangle + i|3\rangle], \tag{31}$$

$$(|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle);$$
$$\tfrac{1}{4}[|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle, \ |0\rangle + |1\rangle - |2\rangle + |3\rangle - |4\rangle - |5\rangle - |6\rangle + |7\rangle,$$
$$|0\rangle - |1\rangle + |2\rangle - |3\rangle - |4\rangle - |5\rangle + |6\rangle - |7\rangle, \ |0\rangle + |1\rangle - |2\rangle - |3\rangle - |4\rangle + |5\rangle + |6\rangle - |7\rangle,$$
$$|0\rangle - |1\rangle - |2\rangle - |3\rangle + |4\rangle + |5\rangle - |6\rangle + |7\rangle, \ |0\rangle - |1\rangle - |2\rangle + |3\rangle + |4\rangle - |5\rangle + |6\rangle - |7\rangle,$$
$$|0\rangle - |1\rangle + |2\rangle + |3\rangle - |4\rangle + |5\rangle - |6\rangle - |7\rangle, \ |0\rangle + |1\rangle + |2\rangle - |3\rangle + |4\rangle - |5\rangle - |6\rangle - |7\rangle],$$
$$\ldots \tag{32}$$

4.2 Phase states for m-qubits

The quantum phase states for m-qubits can be found as the "Galois ring" Fourier transform

$$|\theta^{(y)}\rangle = \frac{1}{\sqrt{2^m}} \sum_{n \in \mathcal{T}_m} \tilde{\psi}_k(n) \tilde{\kappa}(yn)|n\rangle, \ \ y \in R_{4^m}. \tag{29}$$

Using the Teichmüller decomposition in the character function $\tilde{\kappa}$ one obtains

$$|\theta_b^a\rangle = \frac{1}{\sqrt{2^m}} \sum_{n \in \mathcal{T}_m} \tilde{\psi}_k(n) \tilde{\kappa}[(a + 2b)n]|n\rangle, \ \ a, b \in \mathcal{T}_m. \tag{30}$$

This defines a set of 2^m bases (with index a) of 2^m vectors (with index b). Using the exponential sums (26), it is easy to show that the bases are orthogonal and mutually unbiased to each other and to the computational base. The case $\bar{\psi} \equiv \bar{\psi}_0$ was obtained before [2].

4.3 Phase MUBs for m-qubits: m = 1, 2 and 3

For the special case of qubits, one uses $\tilde{\mathrm{tr}}(x) = x$ in (30) so that the three pairs of MUBs are given as

$$[|0\rangle, |1\rangle]; \ \ \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle, |0\rangle - |1\rangle]; \ \ \frac{1}{\sqrt{2}}[|0\rangle + i|1\rangle, |0\rangle - i|1\rangle].$$

For 2-qubits one gets a complete set of 5 bases as follows

see system (31) above

and for 3-qubits a complete set of 9 bases

see system (32) above

where only the first two bases have been written down for brevity reasons.

Quantum phase states of m-qubits (30) are eigenstates of a "Galois ring" quantum phase operator as in (11), and

calculations of the same type as to those performed in Section 3 can be done, since the $\tilde{\mathrm{tr}}$ operator (23) fulfills rules similar to the tr operator (1). By analogy to the case of qudits in dimension p^m, p an odd prime, phase properties for sets of m-qubits heavily rely on the Gauss sums (28). The calculations are tedious once again but can in principle be achieved in specific cases.

5 Mutual unbiasedness and maximal entanglement

Roughly speaking, entangled states in $\mathcal{H}_q$ cannot be factored into tensorial products of states in Hilbert spaces of lower dimension. We show now that there is an intrinsic relation between MUBs and maximal entanglement (see below).

We start with the familiar Bell states

$$(|\mathcal{B}_{0,0}\rangle, |\mathcal{B}_{0,1}\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle, |00\rangle - |11\rangle),$$

$$(|\mathcal{B}_{1,0}\rangle, |\mathcal{B}_{1,1}\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle, |01\rangle - |10\rangle),$$

where the compact notation $|00\rangle = |0\rangle \odot |0\rangle$, $|01\rangle = |0\rangle \odot |1\rangle$, ..., is employed for the tensorial products.

These states are both orthonormal and maximally entangled, i.e., such that $\mathrm{trace}_2|\mathcal{B}_{h,k}\rangle\langle\mathcal{B}_{h,k}| = I_2/2$, where trace_2 means the partial trace over the second qubit [27].

One can define more general Bell states using the multiplicative Fourier transform (7) applied to the tensorial products of two qudits [18,29],

$$|\mathcal{B}_{h,k}\rangle = \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} \omega_q^{kn}|n, n+h\rangle, \tag{33}$$

These states are both orthonormal, $\langle\mathcal{B}_{h,k}|\mathcal{B}_{h',k'}\rangle = \delta_{hh'}\delta_{kk'}$, and maximally entangled, $\mathrm{trace}_2|\mathcal{B}_{h,k}\rangle\langle\mathcal{B}_{h,k}| = I_q/q$.

$\{(|00\rangle + |11\rangle + |22\rangle + |33\rangle \quad |00\rangle + |11\rangle - |22\rangle - |33\rangle \quad |00\rangle - |11\rangle - |22\rangle + |33\rangle \quad |00\rangle - |11\rangle + |22\rangle - |33\rangle);$
$(|00\rangle - |11\rangle - i|22\rangle - i|33\rangle \quad |00\rangle - |11\rangle + i|22\rangle + i|33\rangle \quad |00\rangle + |11\rangle + i|22\rangle - i|33\rangle \quad |00\rangle + |11\rangle - i|22\rangle + i|33\rangle); ...\}$

$\{(|01\rangle + |12\rangle + |23\rangle + |30\rangle \quad |01\rangle + |12\rangle - |23\rangle - |30\rangle \quad |01\rangle - |12\rangle - |23\rangle + |30\rangle \quad |01\rangle - |12\rangle + |23\rangle - |30\rangle);$
$(|01\rangle - |12\rangle - i|23\rangle - i|30\rangle \quad |01\rangle - |12\rangle + i|23\rangle + i|30\rangle \quad |01\rangle + |12\rangle + i|23\rangle - i|30\rangle \quad |01\rangle + |12\rangle - i|23\rangle + i|30\rangle); ...\}$

$\{(|02\rangle + |13\rangle + |20\rangle + |31\rangle \quad |02\rangle + |13\rangle - |20\rangle - |31\rangle \quad |02\rangle - |13\rangle - |20\rangle + |31\rangle \quad |02\rangle - |13\rangle + |20\rangle - |31\rangle); ...\}$

$$\{(|03\rangle + |10\rangle + |21\rangle + |32\rangle \quad |03\rangle + |10\rangle - |21\rangle - |32\rangle \quad |03\rangle - |10\rangle - |21\rangle + |32\rangle \quad |03\rangle - |10\rangle + |21\rangle - |32\rangle); ...\}, \quad (37)$$

We define here an even more general class of maximally entangled states using the Fourier transform (9) over F_q as follows

$$|\mathcal{B}_{h,b}^a\rangle = \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} \omega_p^{\mathrm{tr}[(an+b)n]} |n, n+h\rangle . \quad (34)$$

The h we use here has nothing to do with the polynomial $h(x)$ of Section 2. A list of the generalized Bell states of qutrits for the base $a = 0$ can be found in [28] which is a work that relies on a coherent state formulation of entanglement. In general, for q a power of a prime, starting from (34) one obtains q^2 bases of q maximally entangled states. Each set of the q bases (with h fixed) has the property of mutual unbiasedness.

Similarly, for sets of maximally entangled m-qubits one uses the Fourier transform over Galois rings (30) so that

$$|\mathcal{B}_{h,b}^a\rangle = \frac{1}{\sqrt{2^m}} \sum_{n=0}^{2^m-1} i^{\mathrm{tr}[(a+2b)n]} |n, n+h\rangle. \quad (35)$$

For qubits ($m = 1$) one gets the following bases of maximally entangled states (in matrix form, up to the proportionality factor)

$$\begin{bmatrix} (|00\rangle + |11\rangle, |00\rangle - |11\rangle) & (|01\rangle + |10\rangle, |01\rangle - |10\rangle) \\ (|00\rangle + i|11\rangle, |00\rangle - i|11\rangle) & (|01\rangle + i|10\rangle, |01\rangle) - i|10\rangle) \end{bmatrix}. \quad (36)$$

Two bases in one column are mutually unbiased, while vectors in two bases on the same line are orthogonal to each other.

For two-particle sets of quartits, using equations (31) and (35), one gets 4 sets of $(|\mathcal{B}_{h,b}^a\rangle$, $h = 0, ..., 3)$, see them below, each entailing 4 MUBs ($a = 0, ..., 3$):

see system (37) above

where, for the sake of brevity, we omitted the normalization factor $(1/2)$. Within each set, the four bases are mutually unbiased, as in (31), while the vectors of the bases from different sets are orthogonal.

As a conclusion, the two related concepts of mutual unbiasedness and maximal entanglement derive from the study of lifts of the base field $\mathcal{Z}_p$ to Galois fields of prime characteristic $p > 2$ (in odd dimension), or of lifts of the base ring $\mathcal{Z}_4$ to Galois rings of characteristic 4 (in even dimension). One wonders if lifts to more general algebraic structures would play a role in the study of non maximal entanglement. We have first in mind the near-fields that are used for deriving efficient classical codes and which have a strong underlying geometry [30].

6 Conclusion

In this research, we approached the MUBs fundamental topic from the point of view of the additive and multiplicative characters over finite fields in number theory. We consider that this framework is the most general including previous results in the literature as particular cases. Since MUBs are essentially generalized discrete Fourier transforms over finite number field kets, we formulated a quantum phase interpretation and illustrated several calculations of the phase properties of pure quantum states of the electromagnetic field in this finite number field mathematical context. Various types of Gauss sums get involved in this type of calculations of the MUBs phase properties of a pure quantum state and the generalization to the mixed states, although straightforward through the usage of the density matrix formalism, could lead to even more complicated calculations involving such sums. We hope to evaluate them in future works. We also mentioned in the last section a possible application to phase MUBs states of Bell type. This could lead to finite number field measures of the degree of entanglement.

References

1. W.K. Wootters, B.D. Fields, Ann. Phys. **191**, 363 (1989)
2. A. Klappenecker, M. Rötteler, e-print arXiv:quant-ph/0309120 (2003)
3. K.S. Gibbons, M.J. Hoffman, W.K. Wootters, Phys. Rev. A **70**, 062101 (2004); e-print arXiv:quant-ph/0401155

4. M. Planat, H. Rosu, S. Perrine, M. Saniga, e-print `arXiv:quant-ph/0409081`
5. J. Paz, A.J. Roncaglia, M. Saraceno, e-print `arXiv:quant-ph/0410117`
6. A.O. Pittinger, M.H. Rubin, J. Phys. A **38** (2005, to appear), e-print `arXiv:quant-ph/0501104`
7. M. Saniga, M. Planat, H. Rosu, J. Opt. B: Quant. Semiclass. Opt **6**, L19 (2004), e-print `arXiv:math-ph/0403057`
8. M. Saniga, M. Planat, Chaos, Solitons, and Fractals **27** (2005, to appear), e-print `arXiv:quant-ph/0409184`
9. I. Bengtsson, A. Ericsson, Open Syst. Inform. Dyn. **11** (2005, to appear), e-print `arXiv:quant-ph/0410120`
10. H. Barnum, e-print `arXiv:quant-ph/0205155`
11. A. Klappenecker, M. Roetteler, e-print `arXiv:quant-ph/0502031`
12. W.K. Wootters, Found. Phys. (to appear), e-print `arXiv:quant-ph/0406032`
13. M. Grassl, *Proc. ERATO Conf. on Quant. Inf. Science (EQIS 2004)* pp. 60–61, e-print `arXiv:quant-ph/0406175`
14. D.M. Appleby, J. Math. Phys. **46**, 052107 (2005), e-print `arXiv:quant-ph/0412001`
15. A.Klappenecker, M. Roetteler, I.E. Shparlinski, A. Winterhof, e-print `arXiv:quant-ph/0503239`
16. P. Wocjan, T. Beth, e-print `arXiv:quant-ph/0407081`
17. Quiprocone webside, `http://www.imaph.tu-bs.de/qi/problems`
18. T. Durt, J. Phys. A **38** (2005, to appear), e-print `arXiv:quant-ph/0409090`
19. A.B. Klimov, L.L. Sanchez-Soto, H. de Guise, J. Phys. A **38**, 2747 (2005), e-print `arXiv:quant-ph/0410155`
20. D.T. Pegg, S.M. Barnett, Phys. Rev. A **15**, 1665 (1989)
21. R. Lidl, H. Niederreiter, *Finite Fields* (Addison-Wesley, Reading, Mass., 1983)
22. R. Lidl, G. Pilz, *Applied Abstract Algebra*, 2nd edn. (Springer Verlag, New York, 1998)
23. A. Weil, Proc. Nat. Acad. Sci. USA **34**, 204 (1948)
24. Z.X. Wan, *Quaternary Codes* (World Scientific, Singapore, 1997)
25. A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Sole, IEEE Trans. Inform. Theory **40**, 301 (1994)
26. Yunchang Oh, Heung-Joon Oh, Kangweon-Kyungki Math. J. **9**, 1 (2001)
27. M.A. Nielsen, I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000), p. 582
28. K. Fujii, e-print `arXiv:quant-ph/0105077` (2001)
29. N.J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002)
30. G. Piltz, *Near-Rings* (North-Holland, Amsterdam, 1977), Chap. 8