Galois algebras of squeezed quantum phase states

Michel R. P. Planat, Metod Saniga

Galois algebras of squeezed quantum phase states

Michel Planat† § and Metod Saniga‡

† Institut FEMTO-ST, Dept LPMO,
32 Avenue de l'Observatoire, 25044 Besançon Cedex, France
‡ Astronomical Institute, Slovak Academy of Sciences
05960 Tatranská Lomnica, Slovak Republic

Abstract. Coding, transmission and recovery of quantum states with high security and efficiency, and with as low fluctuations as possible, is the main goal of quantum information protocols and their proper technical implementations. The paper deals with this promise focusing on the quantum states related to Galois algebras. We first review the constructions of complete sets of mutually unbiased bases in a Hilbert space of dimension $q = p^m$, with p being a prime and m a positive integer, employing the properties of Galois fields F_q (for $p > 2$) and/or Galois rings of characteristic four R_4^m (for $p = 2$). We then discuss the Gauss sums and their role in describing quantum phase fluctuations. Finally, we examine an intricate connection between the concepts of mutual unbiasedness and maximal entanglement.

PACS numbers: 03.67.-a, 05.40.Ca, 02.10.De, 02.30.Nw

§ To whom correspondence should be addressed (planat@lpmo.edu)

1. Introduction

It has been known for a long time that concepts belonging to the separate fields of quantum optics, quantum information, Galois algebra and geometry, or even group theory, are related. In the realm of quantum optics, problems arose in attempts to identify a suitable Hermitian operator for the quantum optical phase [1, 2]; they can now be solved by means of a properly defined quantum phase operator over a Galois field [3]. In the field of quantum information, the quantum theory of von Neumann measurements is being supplemented by more symmetric and efficient protocols based, for example, on mutually unbiased bases (MUBs)[4, 5, 6], or positive operator valued measures (POVMs) [7], which are optimally constructed thanks to a Galois algebra. The Galois fields and rings are being extensively used to weave the resources of quantum information, in most applications such as entanglement-assisted quantum cryptography, cloning, coding and computing [8, 9], as well as in relation to the group theoretical approach of coherent states [10, 11, 12, 13]. Finally, Galois fields can be used to coordinatize the projective planes [14, 15], or the discrete phase space [4, 16], which are geometrical concepts having an intrinsic relevance to complete sets of MUBs.

The physical motivations to embark on detailed studies of MUBs are as follows. First, MUBs enter rigorous treatments of Bohr's principle of complementarity that distinguishes between quantum and classical systems at the practical level of measurements. At the conceptual level, two observables are complementary if precise knowledge of one of them implies that all possible outcomes of measuring the other one are equally probable. The eigenstates of such complementary observables are non-orthogonal quantum states, and in any attempt to distinguish between them, information gain is only possible at the expense of introducing disturbance. This property was first implicitly exploited by Bennett and Brassard in 1984 to secure the quantum key exchange against eavesdropping. Most quantum cryptography protocols to-date, like the original BB84 one, use only one-qubit technologies, i.e. quantum states embedded in a Hilbert space of dimension 2, usually the polarisation states of a single photon. But it was found that the security against eavesdropping is heightened by using all the three mutually unbiased bases of qubits, going to higher dimensional Hilbert spaces (i.e. employing qudits), or by making use of entanglement-based protocols [17].

There is a mathematical implementation of the complementary principle which leads to this key notion of mutual unbiasedness. Let $\mathcal{O}$ be an observable in a Hilbert space of dimension q, $\mathcal{H}_q$, which is represented by a Hermitian $q \times q$ matrix. Let us assume that its real eigenvalues are multiplicity-free and its eigenvectors $|b\rangle$ belong to an orthonormal basis B. Let $\mathcal{O}'$ be a (prepared) complementary observable with eigenvectors $|b'\rangle$ in B'. If $\mathcal{O}$ is measured, then the probability to find the system in the state $|b\rangle \in B$ is given by $|\langle b|b'\rangle|^2 = 1/q$. We here recall that two orthonormal bases B and B' of $\mathcal{H}_q$ are mutually unbiased precisely when $|\langle b|b'\rangle|^2 = \frac{1}{q}$ for all $b \in B$ and $b' \in B'$. It can be shown that in order to fully recover the density matrix of a set of identical copies of a quantum state, we need at least $q + 1$ measurements performed on

complementary observables [7, 18].

A simple example is provided by the "complementary" Pauli spin matrices in the Hilbert space $\mathcal{H}_2$, e.g. $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ and $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, where $\sigma_y = i\sigma_x\sigma_z$. The eigenvectors of these three observables are respectively in the bases $B_0 = (|0\rangle, |1\rangle)$, $B_1 = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle, |0\rangle-|1\rangle)$, $B_2 = \frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle, |0\rangle-i|1\rangle)$. They constitute a complete set of three MUBs from which an arbitrary qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, can be recovered.

Recently, a search for complete, $(q+1)$-sets of MUBs in $\mathcal{H}_q$ triggered off a way of remarkable activity [19]. First, if the dimension $q = p$, p being an odd prime number, then using the discrete Fourier transform applied to the kets $|n\rangle$ in the computational basis $(|0\rangle, |1\rangle, \cdots, |p-1\rangle)$,

$$|\theta_k\rangle = \frac{1}{\sqrt{p}} \sum_{n=0}^{p-1} \exp\left(\frac{2i\pi kn}{p}\right) |n\rangle, \tag{1}$$

and replacing k in (1) by its unique decomposition $k = an + b$ in the set $\mathcal{Z}_p$ of integers modulo p, one gets

$$|\theta_b^a\rangle = \frac{1}{\sqrt{p}} \sum_{n=0}^{p-1} \exp\left(\frac{2i\pi(an+b)n}{p}\right) |n\rangle. \tag{2}$$

Eq. (2) defines a set of p bases (with the index $a = 0, \ldots, p-1$) of p vectors (with the index $b = 0, \ldots, p-1$). The p bases are mutually unbiased to each other and to the computational basis and thus form the expected $(p+1)$-set of MUBs. This procedure, however, fails for qubits, i.e. for $p = 2$, because the polynomial in the exponential factor of (2) has a degree which is not coprime to 2. This observation will be made clear below in relation to the property of the Weil sums. It is worthwhile to observe that the complete set of MUBs in this case can also be derived from the generalized Pauli spin matrices

$$\begin{aligned} X_q|n\rangle &= |n+1\rangle, \\ Z_q|n\rangle &= \exp\left(\frac{2i\pi n}{q}\right)|n\rangle; \end{aligned} \tag{3}$$

here, the eigenvectors of the unitary operators $(Z_p, X_p, X_pZ_p, \cdots, X_pZ_p^{p-1})$ generate the set of $p+1$ MUBs [20]. The task of finding a complete set of MUBs may also be related to the phase properties of the single-mode electromagnetic field in quantum optics [2]. A suitable procedure to examine the phase properties of a quantized electromagnetic field state is to introduce a Hermitian phase operator of the form

$$\Theta_{PB} = \sum_{k \in \mathcal{Z}_q} \theta_k |\theta_k\rangle\langle\theta_k|, \tag{4}$$

with eigenvalues $\theta_k = \theta_0 + \frac{2\pi k}{q}$, θ_0 being an arbitrary initial phase, and eigenvectors as in the discrete Fourier transform (1).‖

‖ Pegg and Barnett [2] used the same quantum phase operator for an arbitrary dimension q and thus failed to notice the connection of their problem to complete sets of MUBs. See [21] and [3] for a generalization of their work.

It has been said that with a complete set of $q+1$ mutually unbiased measurements one can ascertain the density matrix of an ensemble of unknown quantum q-states; hence, a natural question emerges as what mathematics can provide the construction. It is known that in dimensions $q = p^m$, p being a prime and m a positive integer, the complete sets of MUBs result from a Fourier analysis over the Galois fields F_q (p odd) [22] or the Galois rings R_{4^m} ($p = 2$) [24]. See also [25].

2. Quantum phase states in MUBs and their relation to additive characters in the Galois field F_q: m-qudits in odd characteristic p

2.1. Construction of finite fields

The key relation between finite (also called) Galois fields and MUBs is the theory of characters. A Galois field F_q, $q = p^m$, is a finite set structure endowed with two group operations, addition "+" and multiplication "$\cdot$". It can be represented as classes of polynomials obtained by computing modulo an irreducible polynomial over the ground field $F_p = \mathcal{Z}_p$ [26, 28].

Let us consider the ring of polynomials $F_p[x]$ defined over the field F_p

$$F_p[x] = \{a_0 + a_1 x + \cdots + a_n x^n\}, \quad a_i \in F_p. \tag{5}$$

For a polynomial $g \in F_p[x]$, the residue class ring $F_p[x]/(g)$, where (g) is the ideal class generated by g, is a field iff g is irreducible (cannot be factored) over F_p. For example, for $q = 2^2$ one can choose the polynomial $g(x) = x^2 + x + 1 \in F_2[x]$ which is irreducible over F_2. Contrary to $\mathcal{Z}_4$, which has zero divisors and is thus only a ring, the above construction defines indeed the field with four residue classes: $F_4 = \{0, 1, x, x+1\}$. For example $[x] + [x+1] = x + (g) + x + 1 + (g) = 2x + 1 + (g) + (g) = 1 + (g) = [1]$. Similarly $[x][x] = (x+(g))(x+(g)) = x^2+(g)(2x+1) = x^2+(g) = x^2-(x^2+x+1)+(g) = -(x+1)+(g) = (x+1)+(g) = [x+1]$.

It can be shown that a Galois field with q elements exists iff $q = p^m$, a power of a prime number p. Actually they are several representations of Galois fields. The first one is as a polynomial as in (5). The second one consists in identifying the Galois field F_q, with $q = p^m$ to the vector space F_p^m build from the coefficients of the polynomial. The third one uses the property that $F_q^* = F_q - \{0\}$ is a multiplicative cyclic group. One needs the concept of a primitive polynomial. A (monic) primitive polynomial, of degree m, in the field $F_q[x]$ is irreducible over F_q and has a root $\alpha \in F_{q^m}$ that generates the multiplicative group of F_{q^m}. A polynomial $g \in F_q[x]$ of degree m is primitive iff $g(0) \neq 0$ and divides $x^r - 1$, with $r = q^m - 1$.

For example F_8 can be build from $\mathcal{R} = F_2$ and $g = x^3+x+1$ which is primitive over F_2. One gets $F_8 = F_2[x]/(g) = \{0, 1, \alpha, \alpha^2, \alpha^3 = 1+\alpha, \alpha^4 = \alpha+\alpha^2, \alpha^5 = 1+\alpha+\alpha^2, \alpha^6 = 1+\alpha^2\}$ (see Table 1).

as powers of α	as polynomials	as 3-tuples in $\mathcal{Z}_2^3$
0	0	$(0,0,0)$
1	1	$(0,0,1)$
α	α	$(0,1,0)$
α^2	α^2	$(1,0,0)$
α^3	$1+\alpha$	$(0,1,1)$
α^4	$\alpha+\alpha^2$	$(1,1,0)$
α^5	$1+\alpha+\alpha^2$	$(1,1,1)$
α^6	$1+\alpha^2$	$(1,0,1)$

2.2. Characters of a finite field and Gauss sums

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 $|\kappa(g)| = 1$, $g \in G$. In a finite field F_q there are two finite abelian groups that are of significance–namely, the additive group and the multiplicative group of the field (Chapt. 5 in [26]). The characters pertaining to these two group structures are very different.

As far as the additive group is concerned one starts with a map from the extended field F_q to the ground field F_p which is called the trace function

$$tr(x) = x + x^p + \cdots + x^{p^{m-1}} \in F_p, \quad \forall\ x \in F_q. \tag{6}$$

In addition to its property of mapping an element of F_q into F_p, the trace function has other interesting properties [26]

$$\begin{aligned} &tr(x+y) = tr(x) + tr(y), \quad x, y \in F_q \\ &tr(ax) = atr(x), \quad x \in F_q,\ a \in F_p, \\ &tr(a) = ma, \quad a \in F_p, \\ &tr(x^q) = tr(x), \quad x \in F_q. \end{aligned} \tag{7}$$

Using (6), a canonical additive character over F_q is defined as

$$\kappa(x) = \omega_p^{tr(x)}, \quad \omega_p = \exp\left(\frac{2i\pi}{p}\right), \quad x \in F_q; \tag{8}$$

it is easy to check that $\kappa(x+y) = \kappa(x)\kappa(y),\ x, y \in F_q$.

Characters of the multiplicative group F_q^* are called multiplicative characters of F_q. Since F_q^* is a cyclic group of order $q-1$, its characters can easily be determined as [26, 29]

$$\psi_k(n) = \omega_{q-1}^{nk}, \quad k = 0...q-2,\ n = 0...q-2. \tag{9}$$

The construction of complete sets of MUBs is related to character sums with polynomial arguments $f(x)$, also called Weil sums [24], viz.

$$W_f = \sum_{x \in F_q} \kappa(f(x)). \tag{10}$$

In particular (Theorem 5.38 in [26]), for a polynomial $f_d(x) \in F_q[x]$ of degree $d \geq 1$ and $\gcd(d, q) = 1$, one finds $W_{f_d} \leq (d-1)q^{1/2}$. The quantum fluctuations arising from the phase MUBs are found to be related to Gauss sums which are of the form

$$G(\psi, \kappa) = \sum_{x \in F_q^*} \psi(x)\kappa(x), \tag{11}$$

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 (11) acquire the following values $G(\psi_0, \kappa_0) = q - 1$; $G(\psi_0, \kappa) = -1$; $G(\psi, \kappa_0) = 0$ and $|G(\psi, \kappa)| = q^{1/2}$ for any non-trivial characters κ and ψ.

2.3. Galois quantum phase states

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

$$|\theta^{(y)}\rangle = \frac{1}{\sqrt{q}} \sum_{n \in F_q} \psi_k(n)\kappa(yn)|n\rangle, \quad y \in F_q, \tag{12}$$

in which the coefficient in the computational basis $\{|0\rangle, |1\rangle, \cdots, |q-1\rangle\}$ represents the product of an arbitrary multiplicative character $\psi_k(n)$ with 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 (12). Indeed, as in [2], for $\kappa = \kappa_0$ and $\psi \equiv \psi_k(n)$ one recovers the ordinary quantum Fourier transform over $\mathcal{Z}_q$. As also shown in [2], the corresponding states

$$|\theta_k\rangle = \frac{1}{\sqrt{q}} \sum_{n \in \mathcal{Z}_q} \psi_k(n)|n\rangle \tag{13}$$

are eigenstates of the Hermitian phase operator

$$\Theta_{PB} = \sum_{k \in \mathcal{Z}_q} \theta_k |\theta_k\rangle\langle\theta_k| \tag{14}$$

with eigenvalues $\theta_k = \theta_0 + \frac{2\pi k}{q}$, θ_0 being an arbitrary initial phase. We also recover the result of Wootters & Fields [22] in a more general form by employing the Euclidean division theorem (see Theorem 11.19 in [27]) 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 this decomposition in the exponent of (12), we obtain

$$|\theta_b^a\rangle = \frac{1}{\sqrt{q}} \sum_{n \in F_q} \psi_k(n)\kappa(an^2 + bn)|n\rangle, \quad a, b \in F_q. \tag{15}$$

The result of [22] corresponds to the trivial multiplicative character $\psi_0 = 1$. Eq. (15) defines a set of q bases (with index a) of q vectors (with index b). Employing the Weil sums (10), it is easily shown that for q odd the bases are orthogonal and mutually unbiased to each other and to the computational basis as well [24, 3].

2.4. Quantum phase fluctuations

As already mentioned, following [2], a convenient 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 Pegg & Barnett to introduce their famous Hermitian phase operator Θ_{PB}. In this section we proceed along the same lines using the phase form of the Wootters-Field MUBs.

2.4.1. The Galois phase operator. The phase MUBs as given by (15) are eigenstates of a "Galois" quantum phase operator

$$\Theta_{\rm Gal} = \sum_{b\in F_q} \theta_b |\theta_b^a\rangle\langle\theta_b^a|, \quad a, b \in F_q, \tag{16}$$

with eigenvalues $\theta_b = \frac{2\pi b}{q}$. We use this fact to perform several calculations of quantum phase expectation values and phase variances for these MUBs. Inserting (15) in (16), and making use of the properties of the field theoretical trace, the Galois quantum phase operator can be brought into the form

$$\begin{aligned}\Theta_{\rm Gal} &= \frac{2\pi}{q^2} \sum_{m,n\in F_q} \psi_k(n-m)\omega_p^{tr[a(n^2-m^2)]} S(n,m)|n\rangle\langle m|,\\ S(n,m) &= \sum_{b\in F_q} b\omega_p^{tr[b(n-m)]}.\end{aligned} \tag{17}$$

In the diagonal matrix elements, we have the partial sums $S(n,n) = \frac{q(q-1)}{2}$ so that $\langle n|\Theta_{\rm Gal}|n\rangle = \frac{\pi(q-1)}{q}$. In the non-diagonal matrix elements, the partial sums can be calculated from $\sum_{b\in F_q} b\epsilon^b = \epsilon(1 + 2\epsilon + 3\epsilon^2 + \cdots + q\epsilon^{q-1}) = \epsilon[\frac{1-\epsilon^q}{(1-\epsilon)^2} - \frac{q\epsilon^q}{1-\epsilon}] = \frac{\epsilon q}{\epsilon-1}$, where we introduced $\epsilon = \omega_p^{tr(n-m)}$ and we made use of the relation $\epsilon^q = 1$. Hence,

$$S(m,n) = \frac{q}{1-\omega_p^{tr(m-n)}}. \tag{18}$$

2.4.2. 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 [2]. Thus, we consider the pure state of the form

$$|f\rangle = \sum_{n\in F_q} u_n|n\rangle, \quad u_n = \frac{1}{\sqrt{q}}\exp(in\beta), \tag{19}$$

where β is a real parameter, and sketch the computation of the phase probability distribution $|\langle\theta_b|f\rangle|^2$, the phase expectation value $\langle\Theta_{\rm Gal}\rangle = \sum_{b\in F_q}\theta_b|\langle\theta_b|f\rangle|^2$ and the phase variance $\langle\Delta\Theta^2_{\rm Gal}\rangle = \sum_{b\in F_q}(\theta_b - \langle\Theta_{\rm Gal}\rangle)^2|\langle\theta_b|f\rangle|^2$, respectively (the upper index a for the basis is implicit and we discard it for simplicity). The two factors in the expression for the probability distribution 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 [7] showed that for $f(x)$ of degree d with $\gcd(d,q) = 1$ as in (10), under the constraint that for the multiplicative character ψ of order s the polynomial $g(x)$ should not be an

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 $(d+\nu-1)\sqrt{q}$. The overall bound is $|\langle\theta_b|f\rangle|^2 \leq \frac{1}{q}$ and it follows that the absolute value of the Galois phase expectation value is bounded from above as expected for a common phase operator

$$|\langle\Theta_{\rm Gal}\rangle| \leq \frac{2\pi}{q^2}\sum_{b\in F_q} b \leq \pi. \tag{20}$$

The exact formula for the phase expectation value reads

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

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

The phase variance can be written as

$$\langle\Delta\Theta^2_{\rm Gal}\rangle = \sum_{b\in F_q}(\theta_b^2 - 2\theta_b\langle\Theta_{\rm Gal}\rangle)|\langle\theta_b|f\rangle|^2; \tag{22}$$

the term $\langle\Theta_{\rm Gal}\rangle^2\sum_{b\in F_q}|\langle\theta_b|f\rangle|^2$ does not contribute since it is proportional to the Weil sum $\sum_{b\in F_q}\omega_p^{tr(b(n-m)} = 0$. As a result, a cancellation of the quantum phase fluctuations may occur in (22) from the two extra terms of opposite signs. But the calculations 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 acquires the form $-2\sum_{b\in F_q}\theta_b\langle\Theta_{\rm Gal}\rangle|\langle\theta_b|f\rangle|^2 = -2\langle\Theta_{\rm Gal}\rangle^2$. Partial cancellation occurs in the diagonal terms, leading to the contribution $\approx -\frac{2\pi^2}{3}$, which is still (in the absolute value) twice the amount of phase fluctuations found in the classical regime. A closed form for the estimate of the non-diagonal terms is still an open problem. In odd prime dimension $q=p$ bounds on phase probability distribution, expectation value and variance can be established [23].

3. Quantum phase states in MUBs and their relation to additive characters in Galois rings R_{4^m}: m-qubits

The Weil sums (10), which have been proved useful in the construction of MUBs for odd p (and, so, odd dimensions $q=p^m$), are not useful for $p=2$, because in this case the degree of the polynomial $f_d(x)$ is such that $\gcd(2,q)=2$ — the characteristic of the relevant Galois fields.

3.1. The Galois rings R_{4^m}

An elegant method for constructing complete sets of MUBs of m-qubits was found by Klappenecker and Rötteler [24]¶. The method makes use of objects belonging to the

¶ Other, less explicit methods related to the discrete Fourier transform have also been proposed[9, 6].

context of quaternary codes [30], the so-called Galois rings R_{4^m}; we shall only give its brief sketch and refer the interested reader to [24] for more mathematical details.

In contrast to the Galois fields where the ground alphabet has p elements (p a prime number) in the field $F_p = \mathcal{Z}_p$, the ring R_{4^m} takes its ground alphabet in $\mathcal{Z}_4$. To construct it one uses the ideal class (h), where h is a (monic) basic irreducible polynomial of degree m i.e. such that its restriction to $\bar{h}(x) = h(x) \mathrm{mod}\, 2$ is irreducible over $\mathcal{Z}_2$. The Galois ring R_{4^m} is defined as the residue class ring $\mathcal{Z}_4[x]/(h)$. It has cardinality 4^m. We also needs the concept of a primitive polynomial. A (monic) primitive polynomial, of degree m, in the ring $F_q[x]$ is irreducible over F_q and has a root $\alpha \in F_{q^m}$ that generates the multiplicative group of F_{q^m}. A polynomial $f \in F_q[x]$ of degree m is primitive iff $f(0) \neq 0$ and divides $x^r - 1$, with $r = q^m - 1$. Similarly for Galois rings R_{4^m}, if $\bar{h}[x]$ is a primitive polynomial of degree m in $\mathcal{Z}_2[x]$, then there exists a unique basic primitive polynomial $h(x)$ of degree m in $\mathcal{Z}_4[x]$ (it divides $x^r - 1$, with $r = 2^m - 1$). It can be found as follows [31]. Let $\bar{h}(x) = e(x) - d(x)$, where $e(x)$ contains only even powers and $d(x)$ only odd powers; then $h(x^2) = \pm(e^2(x) - d^2(x))$. For $m = 2$, 3 and 4 one takes $\bar{h}(x) = x^2 + x + 1$, $\bar{h}(x) = x^3 + x + 1$ and $\bar{h}(x) = x^4 + x + 1$ and one gets $h(x) = x^2 + x + 1$, $x^3 + 2x^2 + x - 1$ and $x^4 + 2x^2 - x + 1$, respectively. Any element $y \in R_{4^m}$ can be uniquely expressed in the form $y = a + 2b$, where a and b belong to the so-called Teichmüller set $\mathcal{T}_m = (0, 1, \xi, \cdots, \xi^{2^m - 2})$, where ξ is a nonzero element of the ring which is a root of the basic primitive polynomial $h(x)$ [24]. Moreover, one finds that $a = y^{2^m}$. We can also define the trace to the base ring $\mathcal{Z}_4$ as the map

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

where σ is the so-called Frobenius automorphism, endowed with the following remarkable property

$$\sigma(a + 2b) = a^2 + 2b^2. \tag{24}$$

Let us apply this formula to the case $m = 2$ (which corresponds to 2-qubits). In $R_{4^2} = \mathcal{Z}_4[x]/(x^2 + x + 1)$ the Teichmüller set reads $\mathcal{T}_2 = (0, 1, x, 3 + 3x)$; the 16 elements $a + 2b$ with a and b in $\mathcal{T}_2$ are shown in the following matrix

$$\begin{bmatrix} 0 & 2 & 2x & 2 + 2x \\ 1 & 3 & 1 + 2x & 3 + 2x \\ x & 2 + x & 3x & 2 + 3x \\ 3 + 3x & 1 + 3x & 3 + x & 1 + x \end{bmatrix}. \tag{25}$$

For example the element in the second line of the fourth column equals $1 + 2(3 + 3x) = 3 + 2x$.

The case $m = 3$ (i.e. 3-qubits) can be examined in a similar fashion, with the ring $R_{4^3} = \mathcal{Z}_4[x]/(x^3 + 2x^2 + x - 1)$ and the Teichmüller set featuring the following eight elements: $\mathcal{T}_3 = \{0, 1, x, x^2, 1 + 3x + 2x^2, 2 + 3x + 3x^2, 3 + 3x + x^2, 1 + 2x + x^2\}$.

In a Galois ring of characteristic 4 the additive characters are

$$\tilde{\kappa}(x) = \omega_4^{\tilde{\mathrm{tr}}(x)} = i^{\tilde{\mathrm{tr}}(x)}. \tag{26}$$

The Weil sums (10) are replaced by the exponential sums [24]

$$\Gamma(y) = \sum_{u \in \mathcal{T}_m} \tilde{\kappa}(yu), \quad y \in R_{4^m} \tag{27}$$

which satisfy

$$|\Gamma(y)| = \begin{cases} 0 \ \text{ if } y \in 2\mathcal{T}_m, \ y \neq 0, \\ 2^m \ \text{ if } y = 0, \\ \sqrt{2^m} \ \text{ otherwise.} \end{cases} \tag{28}$$

Gauss sums for Galois rings were constructed in [32]

$$G_y(\tilde{\psi}, \tilde{\kappa}) = \sum_{x \in R_{4^m}} \tilde{\psi}(x)\tilde{\kappa}(yx), \quad y \in R_{4^m}, \tag{29}$$

where the multiplicative character $\bar{\psi}(x)$ can be made explicit. Using the notation $\bar{\psi}_0$ for a trivial multiplicative character and $\tilde{\kappa_0}$ for a trivial additive character, the Gaussian sums (29) satisfy $G_y(\tilde{\psi}_0, \tilde{\kappa_0}) = 4^m$; $G_y(\tilde{\psi}, \tilde{\kappa_0}) = 0$ and $|G_y(\tilde{\psi}, \tilde{\kappa})| \leq 2^m$.

3.2. Phase states for m-qubits

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

$$|\theta^{(y)}\rangle = \frac{1}{\sqrt{2^m}} \sum_{n \in \mathcal{T}_m} \tilde{\psi}_k(n)\tilde{\kappa}(yn)|n\rangle, \quad y \in R_{4^m}. \tag{30}$$

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

$$|\theta_b^a\rangle = \frac{1}{\sqrt{2^m}} \sum_{n \in \mathcal{T}_m} \tilde{\psi}_k(n)\tilde{\kappa}[(a+2b)n]|n\rangle, \quad a, b \in \mathcal{T}_m. \tag{31}$$

This defines a set of 2^m bases (with index a) of 2^m vectors (with index b). Using the exponential sums (27), it is easy to show that the bases are orthogonal and mutually unbiased to each other and to the computational basis. The case $\bar{\psi} \equiv \bar{\psi}_0 = 1$ was obtained earlier [24].

4. Mutual unbiasedness and maximal entanglement

By definition entangled states in $\mathcal{H}_q$ cannot be factored into tensorial products of states in Hilbert spaces of lower dimensions. We shall now show that there is an intrinsic relation between MUBs and maximal entanglement.

The familiar Bell states are defined as

$$(|\mathcal{B}_{0,0}\rangle, |\mathcal{B}_{0,1}\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle, |00\rangle - |11\rangle),$$
$$(|\mathcal{B}_{1,0}\rangle, |\mathcal{B}_{1,1}\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle, |01\rangle - |10\rangle),$$

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 $trace_2|\mathcal{B}_{u,k}\rangle\langle\mathcal{B}_{u,k}| = \frac{1}{2}I_2$, where $trace_2$ means the partial trace over the second

qubit [33]. One can define more general Bell states using the multiplicative Fourier transform (13) applied to the tensorial products of two qudits,

$$|\mathcal{B}_{u,k}\rangle = \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} \omega_q^{kn} |n, n+u\rangle. \tag{32}$$

Also these states are both orthonormal, $\langle \mathcal{B}_{u,k} | \mathcal{B}_{u',k'} \rangle = \delta_{uu'}\delta_{kk'}$, and maximally entangled, $trace_2 |\mathcal{B}_{u,k}\rangle\langle\mathcal{B}_{u,k}| = \frac{1}{q} I_q$. We define here an even more general class of maximally entangled states using the Fourier transform (15) over F_q as follows

$$|\mathcal{B}^a_{u,b}\rangle = \frac{1}{\sqrt{q}} \sum_{n=0}^{q-1} \omega_p^{tr[(an+b)n]} |n, n+u\rangle \ . \tag{33}$$

A list of the generalized Bell states of qutrits for the basis $a = 0$ can be found in [10], which is a work that relies on a coherent state formulation of entanglement. In general, for q a power of a prime, starting from (33) one obtains q^2 bases of q maximally entangled states. Each set of the q bases (with u fixed) has the property of mutual unbiasedness. Similarly, for sets of maximally entangled m-qubits one uses the Fourier transform over Galois rings (31) so that

$$|\mathcal{B}^a_{u,b}\rangle = \frac{1}{\sqrt{2^m}} \sum_{n=0}^{2^m-1} i^{\tilde{tr}[(a+2b)n]} |n, n+u\rangle. \tag{34}$$

For qubits ($m = 1$) one recovers the common family of Bell states. For two-particle sets of quartits (see [3]) one gets 4 sets of $|\mathcal{B}^a_{u,b}\rangle$, $u = 0, \ldots, 3$, each entailing 4 MUBs, $a = 0, \ldots, 3$.

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 dimensions), or of lifts of the base ring $\mathcal{Z}_4$ to Galois rings of characteristic 4 (in even dimensions). One may wonder if lifts to more general algebraic structures could play a role in the study of non-maximal entanglement.

5. Conclusion

This paper emphasized the relationship between the technological, physical and mathematical levels of understanding the complementarity in quantum mechanics. Secure quantum communications, quantum measurements and other optimal protocols of the emerging field of quantum information, such as quantum cloning, teleportation and computing, make use of mathematical concepts such as abstract algebra, algebraic number theory and finite geometry. Mutual unbiasedness is a very important concept arising from the exact formulation of quantum complementarity, and in this sense full complementarity seems to be possible only if the Hilbert space's dimension is a power of a prime number. This reminds us of the quantum phase-locking effect [21] in which the phase oscillations are smoothed out at dimensions equal to a prime power, due to the properties of the Mangoldt function in the prime number theory. It might well be that the Riemann hypothesis will eventually be formulated as a quantum complementarity

effect! The quantum theory of von Neumann measurements is being progressively replaced by MUBs-type measurements, or by other type of measurements called SIC POVMs, which are positive operator valued measurements with an optimal symmetry and efficiency. It is believed that these measures exist in arbitrary dimension and — being intimately connected to MUBs — they thus deserve the most serious attention [7]. We have also mentioned in the last section an application to phase MUBs states of a generalized Bell type. This could lead to discovery of new measures for the degree of entanglement.

Acknowledgments

M.S. would like to acknowledge the support received from a 2004 SSHN Physics Fellowship of the French Ministry of Youth, National Education and Research (#411867G/P392152B).

References

[1] Lynch R 1995 *Phys. Rep.* **256** 367-436
[2] Pegg D T and Barnett S M 1989 *Phys. Rev. A* **39** 1665–75
[3] Planat M and Rosu H 2005 *Eur. Phys. J.* **D36** 133-139 (DOI: 10.1140/epjd/e2005-00208-4) (*Preprint* quant-ph/0502167)
[4] Gibbons K S, Hoffman M J and Wootters W K 2004 *Phys. Rev* **70** 062101–23
[5] Planat M and Saniga M 2005 *Proc. Int. Conf. on Endophysics, Time, Quantum and the Subjective (Bielefeld/Germany)* ed R Buccheri, A C Elitzur and M Saniga (World Scientific: Singapore) pp 409–26 (*Preprint* quant-ph/0503159)
[6] Klimov A B, Sanchez-Soto L L and de Guise H 2005 *J. Phys. A* **38** 2747–60
[7] Klappenecker A, Rötteler M, Shparlinski I E, Winterhof A 2005 On approximately SIC-POVMs and related systems of quantum states *Preprint* quant-ph/0503239
[8] Vourdas A 2004 *Rep. Prog. Phys.* **67** 267–320
[9] Durt T 2005 *J. Phys. A: Math. Gen.* **38** 5267–83 (*Preprint* quant-ph/0409090)
[10] Fujii K 2001 A relation between coherent states and generalized Bell states *Preprint* quant-ph/0105077
[11] Kibler M R 2004 *Phys.Lett.* **A321** 147–51
[12] Kibler M R 2005 Representation theory and Wigner-Racah algebra of the SU(2) group in a noncanonical basis *Preprint* quant-ph/0504025
[13] Lev F 2003 Why is quantum physics based on complex numbers? *Preprint* hep-th/0309003
[14] Saniga M, Planat M and Rosu H 2004 *J. Opt. B: Quantum Semiclass. Opt* **6** L19–20 (*Preprint* math-ph/0403057)
[15] Saniga M and Planat M 2005 *Chaos, Solitons and Fractals* **26** 1267-70 (*Preprint* quant-ph/0409184)
[16] Pittenger A O and Rubin M H 2005 *J. Phys. A* **38** to appear (*Preprint* quant-ph/0501104)
[17] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 *Phys. Rev. Lett.* **88** 127902
[18] Ivanovic I D 1981 *J. of Phys. A* **14** 3241–5
[19] Quiprocone website, http://www.imaph.tu-bs.de/qi/problems
[20] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 *Algorithmica* **34** 512–28
[21] Planat M and Rosu H 2004 *J. Opt. B: Quantum Semiclass. Opt.* **6** S583–90
[22] Wootters W K and Fields B D 1989 *Ann. Phys.* **191** 363–81

[23] Planat M 2005 Huyghens, Bohr, Riemann and Galois: Phase-Locking *Preprint* (to appear in *Int. J. Mod. Phys. B*)
[24] Klappenecker A and Rötteler M 2003 *Lecture Notes in Computer Science* **2948** 137–44
[25] Planat M, Rosu H, Perrine S and Saniga M 2004 Finite algebraic geometrical structures underlying mutually unbiased quantum measurements *Preprint* quant-ph/0409081
[26] Lidl R and Niederreiter H 1983 *Finite Fields* (Addison-Wesley: Reading (Ma))
[27] Lidl R and Pilz G 1998 *Applied Abstract Algebra*, Second Edition (Springer Verlag: New York)
[28] Murphy T *Finite Fields* A course available at http://www.maths.tcd.ie/pub/Maths/Courseware /FiniteFields/FiniteFields.pdf
[29] Ip L. 2002 Solving Shift Problems and the Hidden Coset Problem Using the Fourier Transform *Preprint* quant-ph/0205034
[30] Wan Z X 1997 *Quaternary Codes* (World Scientific: Singapore)
[31] Hammons A R, Kumar P V, Calderbank A R, Sloane N J A and Sole P 1994 *IEEE Trans. Inform. Theory* **40**, 301–19
[32] Yunchang Oh and Heung-Joon Oh 2001 *Kangweon-Kyungki Math. J.* **9** 1–7
[33] Nielsen M A and Chuang I 2000 *Quantum Computation and Quantum Information* (Cambridge University Press: Cambridge) 582