Finite Algebraic Geometrical Structures Underlying Mutually Unbiased Quantum Measurements

Michel R. P. Planat, Haret Rosu, Serge Perrine, Metod Saniga

Finite Algebraic Geometrical Structures Underlying Mutually Unbiased Quantum Measurements

Michel Planat† §

† Institut FEMTO-ST, Département LPMO,
32 Avenue de l'Observatoire, 25044 Besançon Cedex, France

Haret Rosu†

† Dept of Applied Mathematics, IPICyT,
Apdo Postal 3-74, Tangamanga, San Luis Potosí, Mexico

Serge Perrine†

† France Telecom, Conseil Scientifique, 38-40 rue du Général Leclerc,
92794 Issy les Moulineaux Cedex 9, France

Metod Saniga†

† Astronomical Institute, Slovak Academy of Sciences,
05960 Tatranská Lomnica, Slovak Republic

Abstract.

The basic methods of constructing the sets of mutually unbiased bases in the Hilbert space of an arbitrary finite dimension are discussed and an emerging link between them is outlined. It is shown that these methods employ a wide range of important mathematical concepts like, e.g., Fourier transforms, Galois fields and rings, finite and related projective geometries, and entanglement, to mention a few. Some applications of the theory to quantum information tasks are also mentioned.

§ To whom correspondence should be addressed Tel: (33) 3 81 85 39 57; Fax: (33) 3 81 85 39 98; planat@lpmo.edu

1. Introduction

As a visionary founder of contemporary physics, Galileo Galilei wrote: *Philosophy (nature) is written in that great book which ever lies before our eyes. I mean the universe, but we cannot understand it if we do not first learn the language and grasp the symbols in which it is written. The book is written in the mathematical language... without whose help it is humanly impossible to comprehend a single word of it, and without which one wanders in vain through a dark labyrinth."* Even without advocating the unity of physics and mathematics, it is becoming a reality that the concepts of quantization invade mathematics after having profoundly changed physics. Problems pertinent to quantum information theory are touching more and more branches of pure mathematics, such as number theory, abstract algebra and projective geometry. This paper focuses on one of the most prominent issues in this respect, namely the construction of sets of mutually unbiased bases (MUBs) in a Hilbert space of finite dimension. An updated list of open problems related to the development of quantum technologies can be, for example, found in [1].

To begin with, one recalls that two different orthonormal bases A and B of a d-dimensional Hilbert space $\mathcal{H}^d$ with metrics $\langle \dots | \dots \rangle$ are called mutually unbiased if and only if $|\langle a|b\rangle| = 1/\sqrt{d}$ for all $a{\in}A$ and all $b{\in}B$. An aggregate of mutually unbiased bases is a set of orthonormal bases which are pairwise mutually unbiased. It has been found [2] that the maximum number of such bases cannot be greater than $d+1$. It is also known that this limit is reached if d is a power of prime. Yet, a still unanswered question is if there are non-prime-power values of d for which this bound is attained. It is surmised [3], [4] that the maximum number of such bases, $N(d)$, is equal to $1+min(p_i^{e_i})$, the latter quantity being the lowest factor in the prime number decomposition of d, $d = \prod_i p_i^{e_i}$. But, for example, it is still not known [5] whether they are more than three MUBs for $d = 6$, the lowest non-prime-power dimension, although the latest findings of Wootters [6] (and an earlier result of G. Tarry quoted in the last reference) seem to speak in favor of this conjecture.

MUBs have already been recognized to play an important role in quantum information theory. Their main domain of applications is the field of secure quantum key exchange (quantum cryptography). This is because any attempt by an eavesdropper to distinguish between two non-orthogonal quantum states shared by two remote parties will occur at the price of introducing a disturbance into the signal, thus revealing the attack and allowing to reject the corrupted quantum data. Until recently, most quantum cryptography protocols have solely relied, like the original BB84 one, upon 1-qubit technologies, i.e. on the lowest non-trivial dimension ($d = 2$), usually the polarization states of a single photon, or other schemes such as the sidebands of phase-modulated light [7]. But security against eavesdropping has lately been found to substantially increase by using all the three bases of qubits, employing higher dimensional states, e.g. qudits [8],[9], or even entanglement-based protocols [10]. Another, closely related, application of MUBs is so-called quantum state tomography, i.e. the most efficient way

to decipher an unknown quantum state [1].

Quantum state recovery and secure quantum key distribution can also be furnished in terms of so-called positive operator valued measures (POVMs) which are symmetric informationally complete (SIC-POVMs) [11]. These are defined as sets of d^2 normalized vectors a and b such that $|\langle a|b\rangle| = 1/\sqrt{d+1}$, where $a \neq b$, and they are, obviously, very intimately connected with MUBs. Unlike the latters, however, the SIC-POVMs can exist in all finite dimensions and they have already been constructed for $d = 6$ [5]. The intricate link between MUBs and SIC-POVMs has recently been examined by Wootters [6] and acquired an intriguing geometrical footing in the light of the "SPR conjecture" [12] stating that the question of the existence of a set of $d+1$ mutually unbiased bases in a d-dimensional Hilbert space if d differs from a power of a prime number is equivalent to the problem of whether there exist projective planes whose order d is not a power of a prime number.

The paper is organized as follows. In Sects. 2 and 3 the construction of a maximal set of MUBs in dimension $d = p^m$, p being a prime, as a quantum Fourier transform acting on a Galois field (p odd) and a Galois ring $GR(4^m)$ ($p = 2$) is discussed. This puts in perspective the earlier formulas by [2] and [4], respectively. The case of non-prime-power dimensions is briefly examined in Sect. 4. In Sect. 5, we focus on our recent conjecture on the equivalence of two problems: the surmised nonexistence of projective planes whose order is not a power of a prime and the suspected non existence of a complete set of MUBs in Hilbert spaces of non-prime-power dimensions. The geometry of qubits is discussed and the concept of a lifted Fano plane is introduced. Finally, an intricate relationship between MUBs and maximal entanglement is emphasized, which promises to shed fresh light on newly emerging concepts such as the distillation of mixed states and bound entanglement. The exposition of the theory should be self-containing. Yet, the interested reader may find it helpful to consult some introductory texts on quantum theory in a finite Hilbert space and its relation to Fourier transforms and phase space methods, e.g., the review by A. Vourdas [13].

2. MUB's, quantum Fourier transforms and Galois fields

In this section we shall examine a close connection between MUBs and Fourier transforms. Let consider an orthogonal computational basis $B_0 = (|0\rangle, |1\rangle, \cdots, |n\rangle, \cdots, |d-1\rangle)$ with indices n in the ring $\mathcal{Z}_d$ of integers modulo d. There is a dual basis which is defined by the quantum Fourier transform

$$|\theta_k\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} \omega_d^{kn} |n\rangle, \tag{1}$$

where $k \in \mathcal{Z}_d, \omega_d = \exp(\frac{2i\pi}{d})$ and $i^2 = -1$. In the context of quantum optics this Fourier transform relates Fock states $|k\rangle$ of light to the so-called phase states $|\theta_k\rangle$. The properties of the quantum phase operator underlying this construction have extensively been studied and found to be linked to prime number theory [14].

Let us start with $d = 2$, i.e. the case of qubits, where $\omega = -1$ and so

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

These two vectors can also be obtained by applying the Hadamard matrix $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ to the basis $(|0\rangle, |1\rangle)$. Note that the two orthogonal bases $B_0 = (|0\rangle, |1\rangle)$ and $B_1 = (|\theta_0\rangle, |\theta_1\rangle)$ are mutually unbiased. The third base $B_2 = (|\psi_0\rangle, |\psi_1\rangle)$ which is mutually unbiased to both B_0 and B_1 is obtained from H by the pre-action of a $\pi/2$ rotation $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$, so that $HS = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}$. The three matrices (I, H, HS) thus generate the three mutually unbiased bases. These matrices are also important for two qubits gates in quantum computation [8].

The above-outlined strategy for finding MUBs for qubits contrasts with that used by a majority of authors. The eigenvectors of Pauli spin matrices $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, where $\sigma_y = i\sigma_x\sigma_z$, are precisely the sought bases B_0, B_1 and B_2. A natural generalization of Pauli operators σ_x and σ_z for an arbitrary dimension d is the Pauli group of shift and clock operators:

$$\begin{aligned} X_d|n\rangle &= |n+1\rangle, \\ Z_d|n\rangle &= \omega_d^n|n\rangle. \end{aligned} \tag{3}$$

For a prime dimension $d = p$, it can be shown that the eigenvectors of the unitary operators $(Z_p, X_p, X_pZ_p, \cdots, X_pZ_p^{p-1})$ generate the set of $d+1$ MUB's [15]. A natural question here emerges whether this method can straightforwardly be generalized to any dimension.

To this end in view, let us attempt to rewrite Eq.(1) in such a way that the exponent of ω_d now acts on the elements of a Galois field $G = GF(p^m)$, the finite field of characteristic p and cardinality $d = p^m$. Denoting "$\oplus$" and "$\odot$" the two usual operations in the field and replacing ω_d by the root of unity ω_p, we get

$$|\theta_k\rangle = \frac{1}{\sqrt{d}}\sum_{n=0}^{d-1}\omega_p^{k\odot n}|n\rangle. \tag{4}$$

Next, we employ the Euclidean division theorem for fields [16], which says that given any two polynomials k and n in G there exists a uniquely determined pair a and b in G such that $k = a \odot n \oplus b$, $\deg b < \deg a$. This allows for the exponent in Eq.(4), E, to be written as $E = (a \odot n \oplus b) \odot n$. In the case of prime dimension $d = p$, E is an integer. Otherwise E is a polynomial and Eq.(4) generalizes to

$$|\theta_b^a\rangle = \frac{1}{\sqrt{d}}\sum_{n=0}^{d-1}\omega_p^{tr[(a\odot n\oplus b)\odot n]}|n\rangle, \tag{5}$$

where "tr" stands for the trace of $GF(p^m)$ down to $GF(p)$,

$$tr(E) = E \oplus E^p \oplus \cdots \oplus E^{p^{m-1}}, \quad E \in GF(p^m). \tag{6}$$

In a finite field of odd characteristic p, Eq.(5) defines the set of d bases, with the index a for the base and the index b for the vector in the base, mutually unbiased to each other and to the computational base B_0 as well. In a slightly different form, this equation was first derived by Wootters [2]. Its nice short elucidation, based on Weil sums, is due to Klappenecker et al [4]. Another, a more tricky derivation still in the spirit of Fourier transforms and claimed to also apply to the case of characteristic 2, was found by Durt [17]. A very recent approach based on the Weyl operators in the L^2-space over Galois fields is also worth mentioning [18].

As already pointed out in [2], the reason why (5) defines the complete set of MUB's relies on the field theoretical formula $|\sum_{n=0}^{d-1}\omega_p^{tr[(a\odot n\oplus b)\odot n]}|n\rangle| = p^{1/2}$, with $a \neq 0$ and p being an odd prime. This method, however, fails for characteristic two where $|\sum_{n=0}^{d-1}\omega_2^{tr[(a\odot n\oplus b)\odot n]}|n\rangle| = 0$ for any a, b. As shown in Sect. 3 below, here one has to use Galois rings instead of Galois fields to find a complete set of MUBs.

A closer inspection of (5) reveals an intricate relation between MUBs and quantum phase operators. It is known [14] that the Fourier basis $|\theta_k\rangle$ can be derived in terms of the eigenvectors of a quantum phase operator with eigenvalues θ_k and given by $\Theta_d = \sum_{k=0}^{d-1}\theta_k|\theta_k\rangle\langle\theta_k|$. Similarly, using well known properties of the field trace, one can show that each base of index a can be associated with a quantum phase operator

$$\Theta_d^a = \sum_{b=0}^{d-1}\theta_b^a|\theta_b^a\rangle\langle\theta_b^a|, \tag{7}$$

with eigenvectors $|\theta_b^a\rangle$ and eigenvalues θ_b^a; the latter may thus be called an "MUB operator."

3. MUB's for even characteristic from Galois rings

Our next goal is to find a Fourier transform formulation of MUBs in characteristic 2. Eq.(4), as it stands, is in principle valid for any power of a prime, $d = p^m$, thus also for 2^m-dits, and one may, therefore, be tempted to connect the Galois field algebra and generalized Pauli operators (3) by constructing discrete vector spaces over the Galois field [19]. For the one qubit case we already know that the eigenvectors of Pauli matrices σ_z, σ_x and $\sigma_x\sigma_z$ define the three MUBs. Passing to the quartit (i.e., 4-dit) case, one finds that the operators of the following tensorial products $\sigma_z\otimes\sigma_x$, $\sigma_z\otimes\sigma_x\sigma_z$ and $\sigma_x\sigma_z\otimes\sigma_z$ are associated to translations, i.e. to a single line in the corresponding vector space, and they define a unique basis represented by their simultaneous eigenvectors. Since there are $4+1$ lines in this discrete vector space, there are also $4+1$ MUBs. Other geometrically inspired derivations based on the tensorial decomposition of operators in the Pauli group can be found in [15],[20],[21].

Now, let us try adjusting Eq.(4) for the case of characteristic two. Instead of the Euclidean division in the field $GF(2^m)$, it is necessary to consider a decomposition in the Galois ring $GR(4^m)$ (defined below) so that the relevant root of unity in the Fourier formula now reads $\omega_4 = \exp(2i\pi/4) = i$. For qubits $GR(4) = \mathcal{Z}_4$, and since any number

k in $\mathcal{Z}_4$ can be written as $k = a \oplus 2 \odot b$, Eq. (4) transforms into

$$|\theta_b^a\rangle = \frac{1}{\sqrt{2}} \sum_{n=0}^{1} i^{(a \oplus 2 \odot b) \odot n} |n\rangle, \tag{8}$$

where $\oplus$ and $\odot$ now act in $\mathcal{Z}_4$. We note that the bases are identical to the ones obtained earlier from Eq.(1), i.e. $B_1 = (|\theta_0^0\rangle, |\theta_1^0\rangle)$ and $B_2 = (|\theta_0^1\rangle, |\theta_1^1\rangle)$.

To generalize further this formula one needs to introduce some abstract algebra. First one recalls that the Galois field $GF(p^m)$ is the field of polynomials defined as the quotient $\mathcal{Z}_p(x)/q(x)$ of the ring of polynomials $\mathcal{Z}_p(x)$ by a primitive polynomial of order m over $\mathcal{Z}_p = GF(p)$. By definition, this primitive element $\alpha = q(x)$ has the property to be irreducible over the base field $GF(p)$, i.e. it cannot be factored into products of lesser-degree polynomials; it is also primitive over $GF(p)$ of order $p-1$ in the sense that it generates any non zero element of $GF(p)$ by a power sequence $(\alpha^1,\ \alpha^2, \cdots, \alpha^{p-1} = 1)$ and in addition all of its roots are in the extension field $GF(p^m)$. There is at least one primitive polynomial for any extension field $GF(p^m)$. For $p = 2$ and $m = 2$, 3 and 4 they are, for example, of the form $q(x) = x^2 + x + 1$, $x^3 + x + 1$ and $x^4 + x + 1$, respectively.

A Galois ring $GR(4^m)$ of order m is a ring of polynomials which is an extension of $\mathcal{Z}_4$ of degree m containing an r-th root of unity [22],[23]. Let $h_2(x) \in \mathcal{Z}_2(x)$ be a primitive irreducible polynomial of degree m. There is a unique monic polynomial $h(x) \in \mathcal{Z}_4(x)$ of degree m such that $h(x) = h_2(x) (\mathrm{mod}\ 2)$ and $h(x) (\mathrm{mod}\ 4)$ divides $x^r - 1$, where $r = 2^m - 1$. The polynomial $h(x)$ is the basic primitive polynomial and defines the Galois ring $GR(4^m) = \mathcal{Z}_4/h(x)$ of cardinality 4^m. This ring can be found as follows. Let $h_2(x) = e(x) - d(x)$, 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 gets $h(x) = x^2 + x + 1$, $x^3 + 2x^2 + x - 1$ and $x^4 + 2x^2 - x + 1$, respectively.

Any non zero element of $GF(p^m)$ can be expressed in terms of a single primitive element. This is no longer true in $GR(4^m)$, which contains zero divisors. But in the latter case there exists a nonzero element ξ of order $2^m - 1$ which is a root of the basic primitive polynomial $h(x)$. Any element $\beta \in GR(4^m)$ can be uniquely determined in the form $\beta = a \oplus 2 \odot b$, where a and b belong to the so-called Teichmüller set $\mathcal{T}_m = (0, 1, \xi, \cdots, \xi^{2^m-2})$. Moreover, one finds that $a = \beta^{2^m}$. We can also define the trace to the base ring $\mathcal{Z}_4$ by the map

$$tr(\beta) = \sum_{k=0}^{m-1} \sigma^k(\beta), \tag{9}$$

where the summation runs over $GR(4^m)$ and the Frobenius automorphism σ reads

$$\sigma(a \oplus 2 \odot b) = a^2 \oplus 2 \odot b^2, \tag{10}$$

with $a^2 \equiv a \odot a$. Using the 2-adic decomposition of k in the exponent of (4) and the above-given trace map, we finally get

$$|\theta_b^a\rangle = \frac{1}{\sqrt{2^m}} \sum_{n=0}^{2^m-1} i^{tr[(a \oplus 2 \odot b) \odot n]} |n\rangle; \tag{11}$$

the last expression gives a set of $d = 2^m$ bases with index a for the base and index b for the vectors in the base, mutually unbiased to each other and to the computational base B_0 [4].

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

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

Extracting the Teichmüller decomposition $(a \oplus 2 \odot b) \odot n = a' \oplus 2 \odot b'$ and calculating the exponent $tr(a' \oplus 2 \odot b') = a' \oplus 2 \odot b' \oplus a'^2 \oplus 2 \odot b'^2$ one gets the four MUBs

$$\begin{aligned} B_1 &= (1/2)\{(1,1,1,1),(1,1,-1,-1),(1,-1,-1,1),(1,-1,1,-1)\} \\ B_2 &= (1/2)\{(1,-1,-i,-i),(1,-1,i,i),(1,1,i,-i),(1,1,-i,i)\} \\ B_3 &= (1/2)\{(1,-i,-i,-1),(1,-i,i,1),(1,i,i,-1),(1,i,-i,1)\} \\ B_4 &= (1/2)\{(1,-i,-1,-i),(1,-i,1,i),(1,i,1,-i),(1,i,-1,i)\}. \end{aligned} \tag{12}$$

The case of 8-dits can be examined in a similar fashion, with the ring $GR(4^3) = \mathcal{Z}_4[x]/(x^3 + 2x^2 + x - 1)$ and Teichmüller set featuring the following eight elements: $\mathcal{T}_2 = \{0, 1, x, x^2, 1 + 3x + 2x^2, 2 + 3x + 3x^2, 3 + 3x + x^2, 1 + 2x + x^2\}$.

4. MUB's for non-prime-power dimensions

For $d = 6$, the lowest non-prime-power (n-p-p) case, one constructs a set of three MUBs as follows. One takes the three MUBs in $d = 2$, viz.

$$B_0^{(1)} = (|0\rangle, |1\rangle),\ B_1^{(1)} = (|\theta_0\rangle, |\theta_1\rangle),\ B_2^{(1)} = (|\psi_0\rangle, |\psi_1\rangle), \tag{13}$$

or, in the matrix form, $B_0^{(1)}{=}I_2, B_1^{(1)}{=}H$ and $B_2^{(1)}{=}HS$, and the first three MUBs in $d = 3$, viz.

$$B_0^{(2)} = (|0\rangle, |1\rangle, |2\rangle),\ B_1^{(2)} = (|u_0\rangle, |u_1\rangle, |u_2\rangle),\ B_2^{(2)} = (|v_0\rangle, |v_1\rangle, |v_2\rangle), \tag{14}$$

or, in a more convenient form, $B_0^{(2)}{=}I_3$, $B_1^{(2)}{=}(1/\sqrt{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega_3 & \bar{\omega_3} \\ 1 & \bar{\omega_3} & \omega_3 \end{bmatrix}$, $B_2^{(2)}{=}1/\sqrt{3}\begin{bmatrix} 1 & \omega_3 & \omega_3 \\ 1 & \bar{\omega_3} & 1 \\ 1 & 1 & \bar{\omega_3} \end{bmatrix}$, and extracts the expressions for three MUBs in $d = 6$ from the rows of the following tensorial product matrices $C_0 = B_0^{(1)} \otimes B_0^{(2)} = I_6$, $C_1 = B_1^{(1)} \otimes B_1^{(2)}$ and $C_2 = B_2^{(1)} \otimes B_2^{(2)}$. This construction can easily be generalized to any n-p-p dimension [4],[24]. One considers the prime number decomposition $d = \prod_{i=1}^{r} p_i^{e_i}$, takes its smallest factor $\tilde{m} = min_i(p_i^{e_i})$, and gets $\tilde{m} + 1$ MUBs from the tensorial product $B^{(k)} = \otimes_{i=1}^{r} B_i^{(k)}$, $(k = 0, .., \tilde{m})$.

At this point, it is instructive to enlighten the above-described construction of MUBs by confining ourselves to the Galois ring in $d = 6$. Let us take the latter as the quotient $GR(6^2) = \mathcal{Z}_6[x]/(x^2 + 3x + 1)$ of polynomials over $\mathcal{Z}_6$ by a polynomial

irreducible over both $\mathcal{Z}_2$ and $\mathcal{Z}_3$. $GR(6^2)$ has 36 elements. The notion of Teichmüller set can be generalized to the so-called Sylow decomposition [3]. Any element $\beta \in GR(6)$ can be uniquely determined in the form $\beta = a \oplus b$, where a and b are in the Sylow subgroups S_a and S_b. These can be defined as $S_a = \{x \in GR(6) : 2x = 0\}$ and $S_b = \{x \in GR(6) : 3x = 0\}$, i.e.

$$\begin{aligned} S_a &= \{0, 3, 3x, 3+3x\}, \\ S_b &= \{0, 2, 4, 2x, 4x, 2+2x, 2+4x, 4+2x, 4+4x\}. \end{aligned} \tag{15}$$

Since the quotient polynomial is irreducible, one observes that S_a and S_b themselves are finite fields, being isomorphic to $GF(4)$ and $GF(9)$, respectively. One can therefore express the ring in dimension 6 as the direct product $GF(4) \oplus GF(9) = GR(6)$. Can this property be useful to constructs MUBs themselves, or it merely represents a constraint on the maximum number of MUBs? One construction of MUBs for d=6 was based on the tensorial product of MUBs in dimension 2 and 3, respectively. But the three MUBs in dimension two do not follow from the four elements of $GF(4)$, but from the four elements of $GR(4^1) = \mathcal{Z}_4$. On the other hand, the four MUBs in d=3 follow from the three elements of $GF(3) = \mathcal{Z}_3$. So the decomposition of $GR(6)$ as a product of two fields appears to be irrelevant to the topic of MUBs. Moreover, it was shown that complete sets of MUBs in n-p-p dimensions cannot be constructed using a majority of generalizations of known formulas for finite rings [3]. This, however, should not deter us from looking at other possible constructions. For example, using the properties of sets of mutually orthogonal Latin squares, it has recently been shown that in a particular square dimension 26^2 it is, in principle, possible to construct at least 6 MUBs, while the construction based on the prime number decomposition determines only $min_i(p_i^{e_i}) + 1 = 2^2 + 1 = 5$ of them [25].

5. MUB's and finite projective planes

An intriguing similarity between mutually unbiased measurements and finite projective geometry has recently been noticed [12]. Let us find the minimum number of different measurements we need to determine uniquely the state of an ensemble of identical d-state particles. The density matrix of such en ensemble, being Hermitean and of unit trace, is specified by $(2d^2/2) - 1 = d^2 - 1$ real parameters. When one performs a non-degenerate orthogonal measurement on each of many copies of such a system one eventually obtains $d - 1$ real numbers (the probabilities of all but one of the d possible outcomes). The minimum number of different measurements needed to determine the state uniquely is thus $(d^2 - 1)/(d - 1) = d + 1$ [2],[19].

It is striking that the identical expression can be found within the context of finite projective geometry. A finite projective plane is an incidence structure consisting of points and lines such that any two points lie on just one line, any two lines pass through just one point, and there exist four points, no three of them on a line [26]. From these properties it readily follows that for any finite projective plane there exists an integer

d with the properties that any line contains exactly $d+1$ points, any point is the meet of exactly $d+1$ lines, and the number of points is the same as the number of lines, namely d^2+d+1. This integer d is called the order of the projective plane. The most striking issue here is that the order of known finite projective planes is a power of prime. The question of which other integers occur as orders of finite projective planes remains one of the most challenging problems of contemporary mathematics. The only "no-go" theorem known so far in this respect is the Bruck-Ryser theorem [27] saying that there is no projective plane of order d if $d-1$ or $d-2$ is divisible by 4 and d is not the sum of two squares. Out of the first few non-prime-power numbers, this theorem rules out finite projective planes of order 6, 14, 21, 22, 30 and 33. Moreover, using massive computer calculations, it was proved that there is no projective plane of order ten. It is surmised that the order of any projective plane is a power of a prime.

It is conjectured [12] that the question of the existence of a set of $d+1$ mutually unbiased bases in a d-dimensional Hilbert space if d differs from a power of a prime number is identical with the problem of whether there exist projective planes whose order d is not a power of a prime number.

5.1. $GF(8)$ and the Fano plane

The smallest projective plane, also called the Fano plane, is obviously the $d=2$ one; it contains 7 points and 7 lines, any line contains 3 points and each point is on 3 lines. It comprises a 3-dimensional vector space over the field $GF(2)$, each point being a triple (g_1, g_2, g_3), excluding the (0,0,0) one, where $g_i \in GF(2) = \{0, 1\}$ [26]. The points of this plane can also be represented in terms of the non-zero elements of the Galois field $G = GF(2^3)$.

To see this, we recall that this field is isomorphic to $\mathcal{Z}_2(x)/(\alpha)$ with the polynomial $\alpha = p(x) = x^3 + x + 1$ irreducible in $GF(2)$. It is well-known that there are three useful representations of the elements of $GF(8)$ as shown in Table I [26], [28],[29].

Table 1. Representations of the elements of the Galois field $GF(8)$

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)

The first representation emphasizes the fact that $G^* = G - \{0\}$ is a multiplicative cyclic group of order 7, for $\alpha^7 = 1$. The second representation is obtained from the first

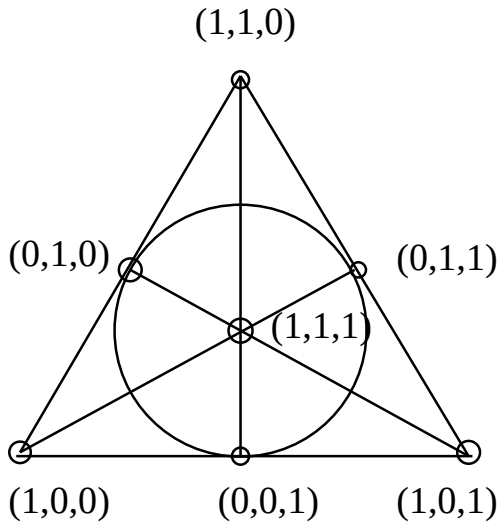

Figure 1. The Fano plane

by calculating modulo the primitive polynomial α. Finally, the 3-tuple representation is obtained from the coefficients of the three powers $x^0 = 1$, $x^1 = x$ and x^2. Taking these 3-tuples as the points of a 3-dimensional vector space, we recover the Fano plane − see Fig. 1.

5.2. The lifted Fano plane in $GR(4^3)$

We already know from Sect. 3 that the relevant object for 2^m-dits is not the Galois field $GF(2^m)$, but rather the Galois ring $GR(4^m)$. It is therefore important to have a look at the geometry in the space $A = GR(4^3)$. For a ring, the concept of a vector space must be replaced by that of a module. The largest cycle in A is the set $\mathcal{T}_3^* = \mathcal{T}_3 - \{0\}$ (see Sect. 3), and each element of $\mathcal{T}_3^*$ can be represented in the same way as in the case of a Galois field. This is summarized in Table II. Any polynomial $h(x)$ in $\mathcal{T}_3^*$ (column 2)

Table 2. Representations of the elements of the cyclic group in the Galois ring $GR(4^3)$

as powers of ξ	as polynomials	as 3-tuples in $\mathcal{Z}_4^3$	as 3-tuples in $\mathcal{Z}_2^3$
0	0	(0,0,0)	(0,0,0)
1	1	(0,0,1)	(0,0,1)
ξ	ξ	(0,1,0)	(0,1,0)
ξ^2	ξ^2	(1,0,0)	(1,0,0)
ξ^3	$1 + 3\xi + 2\xi^2$	(2,3,1)	(0,1,1)
ξ^4	$2 + 3\xi + 3\xi^2$	(3,3,2)	(1,1,0)
ξ^5	$3 + 3\xi + \xi^2$	(1,3,3)	(1,1,1)
ξ^6	$1 + 2\xi + \xi^2$	(1,2,1)	(1,0,1)

is uniquely projected as a polynomial $h_2(x) = h(x) \pmod 2$ in $GF(8)$, which results in the 3-tuple representation in $\mathcal{Z}_2^3$ (column 4). Vice versa, any polynomial in $GF(8)$ has a unique lift in $\mathcal{T}_3^*$. Since the geometrical structure we are looking at is combinatorial and doesn't depend on particular coordinates, it follows that the lifted Fano plane in $\mathcal{T}_3^*$ is still the Fano plane up to isomorphism. So the Fano geometry is inherent in the geometry of qubits, but we needed a special coordinatization in order to be able to see that.

6. MUB's of maximally entangled states

The above-discussed methods of constructing MUBs can straightforwardly be used for recognizing orthogonal bases of maximally entangled states, of which some can be mutually unbiased. Following the methodology outlined in Sects. 2 and 3, let us consider a set of generalized Bell states defined as a two particle quantum Fourier transform [9],[30]

$$|\mathcal{B}_{h,k}\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} \omega_d^{kn} |n, n+h\rangle, \tag{16}$$

where $|n, n+h\rangle$ denotes the two-particle state $|n\rangle, |n+h\rangle$ and the operation $n+h$ is performed modulo d. These states are both orthonormal, $\langle \mathcal{B}_{h,k} | \mathcal{B}_{h',k'} \rangle = \delta_{hh'}\delta_{kk'}$, and maximally entangled, $trace_2 |\mathcal{B}_{h,k}\rangle\langle\mathcal{B}_{h,k}| = \frac{1}{d} I_d$, where $trace_2$ means the partial trace over the second qudit [8]. If one restricts to the case of 2-qubits, one recovers the well-known representation of Bell states

$$\begin{aligned}
(|\mathcal{B}_{0,0}\rangle, |\mathcal{B}_{0,1}\rangle) &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle, |00\rangle - |11\rangle), \\
(|\mathcal{B}_{1,0}\rangle, |\mathcal{B}_{1,1}\rangle) &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle, |01\rangle - |10\rangle),
\end{aligned} \tag{17}$$

where a more compact notation $|00\rangle = |0,0\rangle$, $|01\rangle = |0,1\rangle, \ldots$, is employed. Let us first focus on 2-qubits starting from Eq.(8). Paralleling of what we did in Sect. 3, one first identifies kn in (16) as the multiplication $k \odot n$ of polynomials in $GR(4)$ and then makes use of Teichmüller decomposition $k = a \oplus 2 \odot b$. This leads to a set of 4 bases $(h, a = 0, 1)$ of two vectors $(b = 0, 1)$, namely

$$|\mathcal{B}_{h,b}^a\rangle = \frac{1}{\sqrt{2}} \sum_{n=0}^{1} i^{(a \oplus 2 \odot b) \odot n} |n, n \oplus h\rangle. \tag{18}$$

Casting the last equation into its matrix form (safe for the proportionality factor),

$$\begin{bmatrix} (|00\rangle) + |11\rangle, |00\rangle - |11\rangle); & (|01\rangle + |10\rangle, |01\rangle - |10\rangle) \\ (|00\rangle + i|11\rangle, |00\rangle - i|11\rangle); & (|01\rangle + i|10\rangle, |01\rangle) - i|10\rangle) \end{bmatrix}, \tag{19}$$

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

Eq.(18) can easily be extended to maximally entangled two-particle sets of 2^m-dits by applying, as in Eq.(11), the Frobenius map (9) to the base field $\mathcal{Z}_4$

$$|\mathcal{B}^a_{h,b}\rangle = \frac{1}{\sqrt{2^m}} \sum_{n=0}^{2^m-1} i^{tr[(a\oplus 2\odot b)\odot n]} |n, n\oplus h\rangle. \tag{20}$$

For 2-particle sets of quartits, using Eqs.(12) and (20), one thus gets 4 sets ($|\mathcal{B}^a_{h,b}\rangle$, $h = 0, ..., 3$) of 4 MUBs ($a = 0, ..., 3$),

$$\begin{aligned}
&\{(|00\rangle + |11\rangle + |22\rangle + |33\rangle, |00\rangle + |11\rangle - |22\rangle - |33\rangle,\\
&|00\rangle - |11\rangle - |22\rangle + |33\rangle, |00\rangle - |11\rangle + |22\rangle - |33\rangle);\\
&(|00\rangle - |11\rangle - i|22\rangle - i|33\rangle, |00\rangle - |11\rangle + i|22\rangle + i|33\rangle,\\
&|00\rangle + |11\rangle + i|22\rangle - i|33\rangle, |00\rangle + |11\rangle - i|22\rangle + i|33\rangle);\\
&\cdots\}\\
&\\
&\{(|01\rangle + |12\rangle + |23\rangle + |30\rangle, |01\rangle + |12\rangle - |23\rangle - |30\rangle,\\
&|01\rangle - |12\rangle - |23\rangle + |30\rangle, |01\rangle - |12\rangle + |23\rangle - |30\rangle);\\
&(|01\rangle - |12\rangle - i|23\rangle - i|30\rangle, |01\rangle - |12\rangle + i|23\rangle + i|30\rangle,\\
&|01\rangle + |12\rangle + i|23\rangle - i|30\rangle, |01\rangle + |12\rangle - i|23\rangle + i|30\rangle);\\
&\cdots\}\\
&\\
&\{(|02\rangle + |13\rangle + |20\rangle + |31\rangle, |02\rangle + |13\rangle - |20\rangle - |31\rangle,\\
&|02\rangle - |13\rangle - |20\rangle + |31\rangle, |02\rangle - |13\rangle + |20\rangle - |31\rangle); \cdots\\
&\cdots\}\\
&\\
&\{(|03\rangle + |10\rangle + |21\rangle + |32\rangle, |03\rangle + |10\rangle - |21\rangle - |32\rangle,\\
&|03\rangle - |10\rangle - |21\rangle + |32\rangle, |03\rangle - |10\rangle + |21\rangle - |32\rangle); \cdots\\
&\cdots\},
\end{aligned} \tag{21}$$

where, for the sake of brevity, we omitted the normalization factor (1/2). Within each set, the four bases are mutually unbiased, as in (12), while the vectors of the bases from different sets are orthogonal.

Turning now to odd characteristic, i.e. to $d = p^m$ with p an odd prime, we can similarly extend Wootters formula (5) to the generalized Bell states

$$|\mathcal{B}^a_{h,b}\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} \omega_d^{tr[(a\odot n\oplus b)\odot n]} |n, n\oplus h\rangle, \tag{22}$$

where the trace is defined by Eq.(6). A list of the generalized Bell states of qutrits for the base $a = 0$ can be found in [31], the work that relies on a coherent state formulation of entanglement. In general, for d a power of a prime, starting from (16) or (22) one obtains d^2 bases of d maximally entangled states. Each set of the d bases (with h fixed) has the property of mutual unbiasedness.

Eq.(16) can be used, without any substantial restriction, to find d bases ($h = 0, .., d-1$) of maximally entangled states in any composite dimension $d = \prod_{i=1}^{r} p_i^{e_i}$.

Or one can also follow the strategy of Sect. 4 to get $\tilde{m} = min_i(p_i^{e_i})$ sets of mutually unbiased bases of maximally entangled states. In $d = 6$, for example, one expects that two such sets of d bases can be constructed. Using the tensorial products in Sect. 4, one indeed finds the two 2×6 sets (with the $1/\sqrt{6}$ factor omitted)

$$\{(|00\rangle + |11\rangle + |22\rangle + |33\rangle + |44\rangle + |55\rangle, |00\rangle + \omega_3|11\rangle + \bar{\omega_3}|22\rangle + |33\rangle + \omega_3|44\rangle + \bar{\omega_3}|55\rangle,$$
$$|00\rangle + \bar{\omega_3}|11\rangle + \omega_3|22\rangle + |33\rangle + \bar{\omega_3}|44\rangle + \omega_3|55\rangle, |00\rangle + |11\rangle + |22\rangle - |33\rangle - |44\rangle - |55\rangle,$$
$$|00\rangle + \omega_3|11\rangle + \bar{\omega_3}|22\rangle - |33\rangle - \omega_3|44\rangle - \bar{\omega_3}|55\rangle, |00\rangle + \bar{\omega_3}|11\rangle + \omega_3|22\rangle - |33\rangle - \bar{\omega_3}|44\rangle - \omega_3|55\rangle);$$
$$(|00\rangle + \omega_3|11\rangle + \omega_3|22\rangle + i|33\rangle + i\omega_3|44\rangle + i\omega_3|55\rangle, |00\rangle + \bar{\omega_3}|11\rangle + |22\rangle + i|33\rangle + i\bar{\omega_3}|44\rangle + i|55\rangle,$$
$$|00\rangle + |11\rangle + \bar{\omega_3}|22\rangle + i|33\rangle + i|44\rangle + i\bar{\omega_3}|55\rangle, |00\rangle + \omega_3|11\rangle + \omega_3|22\rangle - i|33\rangle - i\omega_3|44\rangle - i\omega_3|55\rangle,$$
$$|00\rangle + \bar{\omega_3}|11\rangle + |22\rangle - i|33\rangle - i\bar{\omega_3}|44\rangle - i|55\rangle, |00\rangle + |11\rangle + \bar{\omega_3}|22\rangle - i|33\rangle - i|44\rangle - i\bar{\omega_3}|55\rangle); \ldots\}$$

.

.

.

$$\{(|01\rangle + |12\rangle + |23\rangle + |34\rangle + |45\rangle + |50\rangle, |01\rangle + \omega_3|12\rangle + \bar{\omega_3}|23\rangle + |34\rangle + \omega_3|45\rangle + \bar{\omega_3}|50\rangle, \cdots\}.$$

Multipartite entanglement is a key ingredient of many quantum protocols, still needing much work to be properly understood. Sets of orthogonal product states that are unextendible, meaning that no further product states can be found orthogonal to all the existing ones, have recently attracted a lot of attention. These unextendible product bases [32], and their complement [33], certainly deserve reconsideration in terms of the above-outlined theory, which is based on abstract algebra and finite geometry.

The Fourier transform approach implies that mutual unbiasedness and maximal entanglement are complementary aspects in orthogonal quantum measurements. In such measurements, the quantum states are encoded in a three-dimensional lattice of indices h (entanglement), a (unbiasedness) and b (dimensionality of Hilbert space). If d is a power of a prime, the lattice is a cube since in this case h, a and b reach their limiting value d. If one forgets about entanglement ($h = 0$), the finite geometry which seems to be of most relevance is that of a finite projective plane. On the other hand, when unbiasedness is not taken into account, as well as for multipartite information tasks when d is not (a power of) a prime, other concepts have been introduced, such as Bell inequalities [34], coherent states [31], entanglement swapping [35], generalized Hopf fibrations [36], topological entanglement [37] and bound entanglement [32], to mention a few.

Acknowledgement

One of us (M.S.) wishes to acknowledge the support received from a "Séjour Scientifique de Haut Niveau" fellowship of the French Ministry of Youth, National Education and Research (No. 411867G/P392152B).

[1] Quiprocone website, http://www.imaph.tu-bs.de/qi/problems
[2] W.K. Wootters and B.D. Fields, Ann. of Phys. **191**, 363 (1989).

[3] C. Archer, e-print quant-ph/0312204 (2003).
[4] A. Klappenecker and M. Rötteler, e-print quant-ph/0309120 (2003).
[5] M. Grassl, e-print quant-ph/0406175 (2004).
[6] W.K. Wootters, e-print quant-ph/0406032 (2004).
[7] J.M. Merolla, Y. Mazurenko, J.P. Goedgebuer and W.T. Rhodes, Phys. Rev. Lett. **82**, 1656 (1999).
[8] M.A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000), p. 582.
[9] N.J. Cerf, M. Bourennane, A. Karlsson and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[10] T. Durt, D. Kaszlikowski, J.L. Chen, L.C. Kwek, e-print quant-ph/0302078 (2003).
[11] J.M. Renes, R. Blume-Kohout, A.J. Scott and C.M. Caves, e-print quant-ph/0310075 (2003).
[12] M. Saniga, M. Planat and H. Rosu, J. Opt. B: Quantum Semiclass. Opt. **6**, L19 (2004); e-print math-ph/0403057 (2004).
[13] A. Vourdas, Rep. Prog. Phys. **67**, 267 (2004).
[14] M. Planat and H. Rosu, J. Opt. B: Quantum Semiclass. Opt. **6**, S583 (2004).
[15] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury and F. Vatan, Algorithmica **34**, 512 (2002).
[16] R. Lidl and G. Pilz, *Applied Abstract Algebra*, Second Edition (Springer Verlag, New York, 1998).
[17] T. Durt, e-print quant-ph/0401046 (2004).
[18] K.R. Parthasarathy, e-print quant-ph/0408069 (2004).
[19] K.S. Gibbons, M.J. Hoffman and W.K. Wootters, e-print quant-ph/0401155 (2004).
[20] C. Rigetti, R. Mosseri and M. Devoret, e-print quant-ph/0312196, (2003).
[21] A.O. Pittenger and M.H. Rubin, e-print quant-ph/0308142 (2003).
[22] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Sole, IEEE Trans. Inform. Theory **40**, 301 (1994).
[23] Z.X. Wan, *Quaternary Codes* (World Scientific, Singapore, 1997).
[24] G. Zauner, *Quantendesigns-Grundzüge einer nichtkommutativen Designtheorie* (Dissertation, Universität Wien, 1999).
[25] P. Wocjan and T. Beth, e-print quant-ph/0407081 (2004).
[26] A. Beutelspacher and U. Rosenbaum, *Projective geometry: from foundations to applications* (Cambridge University Press, Cambridge, 1998).
[27] R.H. Bruck and H.J. Ryser, Canadian Journal of Mathematics **1**, 88 (1949).
[28] J.W.P. Hirschfeld, *Projective geometries over finite fields* (Oxford University Press, Oxford, 1998).
[29] L.M. Batten, *Combinatorics of finite geometries* (Cambridge University Press, Cambridge, 1997).
[30] D.I. Fivel, Phys. Rev. Lett. **74**, 835 (1995).
[31] K. Fujii, e-print quant-ph/0105077 (2001).
[32] D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin and B.M. Terhal, Commun. Math. Phys. **238**, 379 (2003); e-print quant-ph/9908070 (2000).
[33] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[34] S. Yu, Z.B. Chen , J.W. Pan and Y.D. Zhang, quant-ph/0211063 (2002).
[35] S. Bose, V. Vedral and P.L. Knight, Phys. Rev. A **57**, 822 (1998).
[36] B.A. Bernevig and H.D. Chen, J. Phys. A: Math. Gen. **36**, 8325 (2003); e-print quant-ph/0302081 (2003).
[37] L.H. Kauffman and S.J. Lomonaco, New J. of Phys. **4**, 73.1 (2002).