Entropy **2013**, *15*, 1726-1737; doi:10.3390/e15051726

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

Equiangular Vectors Approach to Mutually Unbiased Bases

Maurice R. Kibler [1,2,3]

[1] Faculté des Sciences et Technologies, Université de Lyon, 37 rue du repos, 69361 Lyon, France

[2] Département de Physique, Université Claude Bernard Lyon 1, 43 Bd du 11 Novembre 1918, 69622 Villeurbanne, France

[3] Groupe Théorie, Institut de Physique Nucléaire, CNRS/IN2P3, 4 rue Enrico Fermi, 69622 Villeurbanne, France; E-Mail: kibler@ipnl.in2p3.fr; Tel: 33(0)472448235, FAX: 33(0)472448004

Received: 26 April 2013 / Accepted: 6 May 2013 / Published: 8 May 2013

Abstract: Two orthonormal bases in the d-dimensional Hilbert space are said to be unbiased if the square modulus of the inner product of any vector of one basis with any vector of the other equals $\frac{1}{d}$. The presence of a modulus in the problem of finding a set of mutually unbiased bases constitutes a source of complications from the numerical point of view. Therefore, we may ask the question: Is it possible to get rid of the modulus? After a short review of various constructions of mutually unbiased bases in $\mathbb{C}^d$, we show how to transform the problem of finding $d+1$ mutually unbiased bases in the d-dimensional space $\mathbb{C}^d$ (with a modulus for the inner product) into the one of finding $d(d+1)$ vectors in the d^2-dimensional space $\mathbb{C}^{d^2}$ (without a modulus for the inner product). The transformation from $\mathbb{C}^d$ to $\mathbb{C}^{d^2}$ corresponds to the passage from equiangular lines to equiangular vectors. The transformation formulas are discussed in the case where d is a prime number.

Keywords: finite-dimensional quantum mechanics; mutually unbiased bases; projection operators; positive-semidefinite Hermitian operators; equiangular lines; Gauss sums

Classification: PACS 03.65.-w; 03.65.Aa; 03.65.Fd

1. Introduction

We start by revisiting a definition. Two distinct orthonormal bases of the $\mathbb{C}^d$ Hilbert space, say,

$$B_a = \{|a\alpha\rangle : \alpha = 0, 1, \ldots, d-1\} \tag{1}$$

and

$$B_b = \{|b\beta\rangle : \beta = 0, 1, \ldots, d-1\} \tag{2}$$

(with $a \neq b$ and $d \geq 2$) are said to be *unbiased* if the modulus of the $\langle a\alpha|b\beta\rangle$ inner product is independent of α and β. In other words

$$\langle a\alpha|a\beta\rangle = \langle b\alpha|b\beta\rangle = \delta_{\alpha,\beta} \tag{3}$$

and

$$|\langle a\alpha|b\beta\rangle| = \frac{1}{\sqrt{d}} \tag{4}$$

for $\alpha, \beta \in \mathbb{Z}/d\mathbb{Z}$. (An exhaustive, although incomplete, set of references concerning unbiased bases is given in what follows. References therein should be consulted too.)

The concept of *unbiased bases* and, more generally, of a set of *mutually unbiased bases* (MUBs) takes its origin in the work by Schwinger [1] on unitary operator bases (see also [2–4]). It is of paramount importance in quantum mechanics. It makes it possible to transcribe the Bohr complementary principle to *finite* quantum mechanics so that the idea of complementarity can be applied also to finite quantum systems [5,6]. Furthermore, MUBs turn out to be useful for discrete Wigner functions [3,7,8], the solution of the mean King problem [9], and the understanding of the Feynman path integral formalism in terms of temporally proximal bases [10]. Many of the applications of MUBs concern classical information (coding theory [11]) and quantum information (quantum cryptography [12] and quantum state tomography [13]). They are also useful in quantum computing, a field where intrication of qupits [14] plays a crucial role.

Three important results on MUBs are known. First, the maximum number N of MUBs in a d-dimensional Hilbert space is $N = d + 1$ [2,4]. Thus, the number of MUBs in $\mathbb{C}^d$ cannot exceed $d + 1$. (A set containing $d + 1$ MUBs is called a complete set.) Second, this maximum number, *i.e.*, $N = d + 1$, is reached when d is a prime number (noted p) or any power of a prime number (noted p^n with $n \geq 2$) [2,4]. Indeed, it is possible to construct several complete sets of MUBs when d is prime or prime power. Third, when d is a composite number ($d = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ with $p_1, p_2, \ldots, p_r$ prime integers and $e_1, e_2, \ldots, e_r$ strictly positive integers), we have (see for instance [15])

$$\min_{i=1}^{r} (p_i^{e_i}) + 1 \leq N \leq d + 1 \tag{5}$$

but the value of N is unknown. More precisely, it is not known if it is possible to construct a complete set of MUBs in $\mathbb{C}^d$ in the case where d is not a prime or the power of a prime. Equation (5) reflects the fact that it is always possible to construct three MUBs when d is a composite number. For example in the $d = 2 \times 3 = 6$ case, several sets of three MUBs are known but no set with more than three MUBs were found in spite of an enormous number of numerical studies [16–21]; in the present days, there is a consensus according to which no complete set (with seven MUBs) exists for $d = 6$ and it is widely believed that only sets with three MUBs exist in this case (cf. the Zauner conjecture [22]).

¿From a mathematical point of view, it is remarkable that MUBs may be connected to many disciplinary fields. A non-exhaustive list is: theory of finite fields, group theory, Lie and Clifford algebras, finite geometries, combinatorics and graph theory, frames and 2-designs, and Hopf fibrations. This can be illustrated by some of the numerous ways of constructing sets of MUBs. Most of them are based on discrete Fourier transform over Galois fields and Galois rings [4,6,7,23], discrete Wigner distribution [3,7,8], generalized Pauli spin operators [24–28], generalized Hadamard matrices [15,17], mutually orthogonal Latin squares [15,29,30], finite geometry methods [30–32], projective 2-designs [5,15,22], angular momentum theory and quadratic discrete Fourier transform [33–35], finite group approaches [23,28], Lie-like approaches [28,34–37], and phase states associated with a generalized Weyl–Heisenberg algebra [38]. (For a review on the subject, see [39].)

It is the aim of the present paper to emphasize another approach for the search of MUBs. Instead of looking for equiangular lines in $\mathbb{C}^d$ satisfying Equation (4), we deal here with the search of equiangular vectors in $\mathbb{C}^{d^2}$ satisfying a relation of type Equation (4) without a modulus for the inner product. The transformation that makes it possible to pass from $\mathbb{C}^d$ to $\mathbb{C}^{d^2}$ is given in Section 2. The reverse problem is the object of Section 3. Finally, some conclusions are drawn in Section 4. A preliminary note on some of the results of this paper was posted on arXiv [40].

2. The Passage from $\mathbb{C}^d$ to $\mathbb{C}^{d^2}$

If we include the $a = b$ case, Equation (3) leads to

$$|\langle a\alpha|b\beta\rangle| = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{\sqrt{d}}(1 - \delta_{a,b}) \tag{6}$$

or equivalently

$$|\langle a\alpha|b\beta\rangle|^2 = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1 - \delta_{a,b}) \tag{7}$$

The problem of finding a complete set of $d+1$ MUBs in $\mathbb{C}^d$ amounts to finding $d(d+1)$ vectors $|a\alpha\rangle$ satisfying Equation (7), where $a = 0, 1, \ldots, d$ and $\alpha = 0, 1, \ldots, d-1$ (the indexes of type a refer to the bases and, for fixed a, the index α refers to one of the d vectors of the basis corresponding to a). By following the approach developed in [41] for positive operator valued measures and MUBs, we can transform this problem into a (possibly) simpler one (not involving a square modulus like in Equation (7)). The idea of the transformation is to introduce a projection operator associated with the $|a\alpha\rangle$ vector. This yields the following proposition.

Proposition 1. *For $d \geq 2$, finding $d+1$ MUBs in $\mathbb{C}^d$ (if they exist) is equivalent to finding $d(d+1)$ vectors $\mathbf{w}(a\alpha)$ in $\mathbb{C}^{d^2}$, of components $w_{pq}(a\alpha)$ such that*

$$w_{pq}(a\alpha) = \overline{w_{qp}(a\alpha)}, \quad p, q = 0, 1, \ldots, d-1 \tag{8}$$

satisfying

$$\sum_{p=0}^{d-1} w_{pp}(a\alpha) = 1 \tag{9}$$

and the inner product relations

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(a\beta) = \delta_{\alpha,\beta} \tag{10}$$

and

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta) = \frac{1}{d} \text{ for } a \neq b \tag{11}$$

where $a, b = 0, 1, \ldots, d$ *and* $\alpha = 0, 1, \ldots, d-1$.

Proof. A proof was given in [41] by making use of Racah operators, which are useful tools in spectroscopy. Here we give a new proof based on the canonical generators of the $\mathrm{GL}(d, \mathbb{C})$ linear group, which are simpler to handle and more adapted for applications. Let us suppose that it is possible to find $d+1$ sets B_a (with $a = 0, 1, \ldots, d$) of vectors of $\mathbb{C}^d$ such that Equation (7) is satisfied. It is thus possible to construct $d(d+1)$ projection operators

$$\Pi_{a\alpha} = |a\alpha\rangle\langle a\alpha|, \quad a = 0, 1, \ldots, d, \quad \alpha = 0, 1, \ldots, d-1 \tag{12}$$

From Equations (7) and (12), it is clear that the $\Pi_{a\alpha}$ operators (of rank 1) satisfy the trace conditions

$$\mathrm{Tr}\,(\Pi_{a\alpha}\Pi_{b\beta}) = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1 - \delta_{a,b}) \tag{13}$$

and

$$\mathrm{Tr}\,(\Pi_{a\alpha}) = 1 \tag{14}$$

where the traces are taken over $\mathbb{C}^d$ (see also [26]). Each operator $\Pi_{a\alpha}$ can be developed on an orthonormal basis $\{E_{pq} : p, q = 0, 1, \ldots, d-1\}$ of the space of linear operators on $\mathbb{C}^d$ (orthonormal with respect to the Hilbert–Schmidt inner product), that is,

$$\Pi_{a\alpha} = \sum_{p=0}^{d-1} \sum_{q=0}^{d-1} w_{pq}(a\alpha) E_{pq} \tag{15}$$

The E_{pq} operators are generators of the $\mathrm{GL}(d, \mathbb{C})$ complex Lie group. Their main properties are

$$E^{\dagger}_{pq} = E_{qp}, \; E_{pq}E_{rs} = \delta_{q,r}E_{ps}, \; \mathrm{Tr}\,(E_{pq}) = \delta_{p,q}, \; \mathrm{Tr}\left(E^{\dagger}_{pq}E_{rs}\right) = \delta_{p,r}\delta_{q,s}, \; p, q, r, s \in \mathbb{Z}/d\mathbb{Z} \tag{16}$$

and they can be represented by the projectors

$$E_{pq} = |p\rangle\langle q|, \quad p, q \in \mathbb{Z}/d\mathbb{Z} \tag{17}$$

The $w_{pq}(a\alpha)$ expansion coefficients in Equation (15) are complex numbers such that

$$\overline{w_{pq}(a\alpha)} = w_{qp}(a\alpha), \quad p, q \in \mathbb{Z}/d\mathbb{Z} \tag{18}$$

where the bar denotes complex conjugation. By combining Equations (13) and (15), we get

$$\sum_{p=0}^{d-1} \sum_{q=0}^{d-1} \overline{w_{pq}(a\alpha)} w_{pq}(b\beta) = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1 - \delta_{a,b}) \tag{19}$$

The $\Pi_{a\alpha}$ operators can be considered as vectors

$$\mathbf{w}(a\alpha) = (w_{00}(a\alpha), w_{01}(a\alpha), \ldots, w_{mm}(a\alpha)), \quad m = d - 1 \tag{20}$$

in the Hilbert space $\mathbb{C}^{d^2}$ (not $\mathbb{C}^d$) of dimension d^2 endowed with the usual inner product

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta) = \sum_{p=0}^{d-1} \sum_{q=0}^{d-1} \overline{w_{pq}(a\alpha)} w_{pq}(b\beta) \tag{21}$$

In Equation (20), we use the dictionary order for ordering the components of $\mathbf{w}(a\alpha)$. Equation (19) can then be rewritten as

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta) = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1 - \delta_{a,b}) \tag{22}$$

to be compared with Equation (7). The determination of the $\Pi_{a\alpha}$ operators is equivalent to the determination of the $w_{pq}(a\alpha)$ components of the $\mathbf{w}(a\alpha)$ vectors in $\mathbb{C}^{d^2}$. This completes the proof.

For $a \neq b$, Equations (10) and (11) show that angle $\omega_{a\alpha b\beta}$ between any vector $\mathbf{w}(a\alpha)$ and any vector $\mathbf{w}(b\beta)$ is

$$\omega_{a\alpha b\beta} = \cos^{-1}(\frac{1}{d}) \tag{23}$$

and therefore does not depend on a, α, b and β. This justifies the terminology *equiangular vectors* in the title of this paper. Note also that Equation (23) is connected to the fact that mutually unbiased bases are complex projective 2-designs [5].

Proposition 1 can be transcribed in terms of matrices. Let $M_{a\alpha}$ be the Hermitian matrix of dimension d whose elements are $w_{pq}(a\alpha)$. To be more precise, we take

$$(M_{a\alpha})_{pq} = w_{pq}(a\alpha), \quad p, q \in \mathbb{Z}/d\mathbb{Z} \tag{24}$$

The $M_{a\alpha}$ matrix is positive-semidefinite. Equation (21) can be rewritten as

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta) = \mathrm{Tr}\,(M_{a\alpha} M_{b\beta}) \tag{25}$$

Therefore, we have the following proposition.

Proposition 2. *For $d \geq 2$, finding $d + 1$ MUBs in $\mathbb{C}^d$ (if they exist) is equivalent to finding $d(d + 1)$ positive-semidefinite (and thus Hermitian) matrices $M_{a\alpha}$ of dimension d satisfying the trace relations*

$$\mathrm{Tr}\,(M_{a\alpha}) = 1 \tag{26}$$

and

$$\mathrm{Tr}\,(M_{a\alpha} M_{b\beta}) = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1 - \delta_{a,b}) \tag{27}$$

where $a, b = 0, 1, \ldots, d$ *and* $\alpha, \beta = 0, 1, \ldots, d-1$.

Proof. The proof is trivial.

It is to be noted that Proposition 2 is in agreement with the result of [29] according to which a complete set of $d+1$ MUBs forms a convex polytope in the set of Hermitian matrices of dimension d and unit trace.

Finally, as a test of the validity of Propositions 1 and 2, we have the following result.

Proposition 3. *For d prime, Equations (8) to (11) admit the solution*

$$w_{pq}(a\alpha) = \frac{1}{d} \mathrm{e}^{\mathrm{i}\pi(p-q)[(d-2-p-q)a-2\alpha]/d}, \quad a, \alpha, p, q \in \mathbb{Z}/d\mathbb{Z} \tag{28}$$

and

$$w_{pq}(d\alpha) = \delta_{p,q}\delta_{p,\alpha}, \quad \alpha, p, q \in \mathbb{Z}/d\mathbb{Z} \tag{29}$$

for $a = d$.

Proof. Clearly the $M_{a\alpha}$ corresponding matrix is Hermitian and it is a simple matter of long calculation to show that it is positive-semidefinite. The rest of the proof is based on the use of Gauss sums [42] in connection with ordinary [43] and quadratic [44] discrete Fourier transforms. Indeed, the principal task is to calculate $\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta)$ as given by (21) with the help of Equations (28) and (29) in the cases $a = b$ (for $a = 0, 1, \ldots, d$), $a \neq b$ (for $a, b = 0, 1, \ldots, d-1$) and $a \neq b$ (for $a = 0, 1, \ldots, d-1$ and $b = d$). The main steps are the following.

(i) Case $a = b = d$: We have

$$\mathbf{w}(d\alpha) \cdot \mathbf{w}(d\beta) = \sum_{p=0}^{d-1} \sum_{q=0}^{d-1} \delta_{p,q}\delta_{p,\alpha}\delta_{p,\beta} = \delta_{\alpha,\beta} \tag{30}$$

(ii) Case $a = b = 0, 1, \ldots, d-1$: We have

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(a\beta) = \frac{1}{d^2} \sum_{p=0}^{d-1} \sum_{q=0}^{d-1} \mathrm{e}^{\mathrm{i}2\pi(p-q)(\alpha-\beta)/d} = \delta_{\alpha,\beta} \tag{31}$$

(iii) Case $a \neq b$ ($a = 0, 1, \ldots, d-1$ and $b = d$): We have

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(d\beta) = \frac{1}{d} \sum_{p=0}^{d-1} \sum_{q=0}^{d-1} \mathrm{e}^{-\mathrm{i}\pi(p-q)[(d-2-p-q)a-2\alpha]/d}\delta_{p,q}\delta_{p,\alpha} = \frac{1}{d} \sum_{p=0}^{d-1} \delta_{p,\alpha} = \frac{1}{d} \tag{32}$$

(iv) Case $a \neq b$ ($a, b = 0, 1, \ldots, d-1$): We have

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta) = \frac{1}{d^2} \sum_{p=0}^{d-1} \sum_{q=0}^{d-1} \mathrm{e}^{\mathrm{i}\pi(p-q)[(d-2-p-q)(b-a)+2(\alpha-\beta)]/d} \tag{33}$$

The double sum in Equation (33) can be factored into the product of two sums. This leads to

$$\mathbf{w}(a\alpha)\cdot\mathbf{w}(b\beta)=\frac{1}{d^2}\left|\sum_{k=0}^{d-1}\mathrm{e}^{\mathrm{i}\pi\{(a-b)k^2+[(d-2)(b-a)+2(\alpha-\beta)]k\}/d}\right|^2 \tag{34}$$

By introducing the generalized Gauss sums [42]

$$S(u,v,w)=\sum_{k=0}^{|w|-1}\mathrm{e}^{\mathrm{i}\pi(uk^2+vk)/w} \tag{35}$$

where u, v and w are integers such that u and w are coprime, uw is nonvanishing and $uw+v$ is even, we obtain

$$\mathbf{w}(a\alpha)\cdot\mathbf{w}(b\beta)=\frac{1}{d^2}|S(u,v,w)|^2 \tag{36}$$

with

$$u=a-b,\quad v=-(a-b)(d-2)+2(\alpha-\beta),\quad w=d \tag{37}$$

The $S(u,v,w)$ Gauss sum in Equations (36,37) can be calculated from the methods in [42]; this yields

$$|S(u,v,w)|=\sqrt{d} \tag{38}$$

for d prime, u and v integers, u and d coprime, $ud\neq 0$, and $ud+v$ even. Finally, we get

$$\mathbf{w}(a\alpha)\cdot\mathbf{w}(b\beta)=\frac{1}{d} \tag{39}$$

which completes the proof.

Let us remark that the proof holds true for $d=2$ (Equation (38) is valid for $d=2$ in contrast with some other Gauss sums [2]).

3. The Reverse Problem

It is legitimate to consider the question: How to pass from the $\mathbf{w}(a\alpha)$ to $|a\alpha\rangle$ vectors in the case where d is the power of a prime integer?

Suppose we find $d(d+1)$ vectors of type Equation (20) satisfying Equations (8) to (11). Then, the $\Pi_{a\alpha}$ operators given by Equation (15) are known. A matrix realization of each $\Pi_{a\alpha}$ operator immediately follows from the standard matrix realization of the generators of the $\mathrm{GL}(d,\mathbb{C})$ group. (In order to set up the matrix of $\Pi_{a\alpha}$, remember that, in terms of matrices, the generators E_{pq} of $\mathrm{GL}(d,\mathbb{C})$ are matrices of dimension $d\times d$, the elements of which are 1 at the intersection of row p and column q and 0 elsewhere. The matrix thus obtained is nothing but $M_{a\alpha}$.) The eigenvector of the matrix of $\Pi_{a\alpha}$ corresponding to the eigenvalue equal to 1 gives the $|a\alpha\rangle$ vector. This leads to the following recipe.

Proposition 4. *In the case where d is a prime power, from the knowledge of the $\mathbf{w}(a\alpha)$ vectors, the matrices of the $\Pi_{a\alpha}$ operators can be constructed via Equation (15) (for $a=0,1,\ldots,d$ and $\alpha=0,1,2,\ldots,d-1$). The $d+1$ MUBs are then given, as column vectors, by the eigenvectors* *(normalized to 1) of the matrices of* $\Pi_{a\alpha}$ *corresponding to the eigenvalues equal to* 1*. For fixed* a*, the eigenvectors of* $\Pi_{a0}, \Pi_{a1}, \ldots, \Pi_{ad-1}$ *associated with the eigenvalue* 1 *constitute one of the* $d+1$ *MUBs.*

Proof. The proof follows from the fact that each $\Pi_{a\alpha}$ operator (or the $M_{a\alpha}$ corresponding matrix) has $d-1$ eigenvalues equal to 0 and one eigenvalue equal to 1.

Example. As a pedagogical example, let us consider the situation where $d = 2$. By taking $w_{pq}(a\alpha)$ given by Equations (28) and (29), we have

$$w_{pq}(a\alpha) = \frac{1}{2}\mathrm{e}^{-\mathrm{i}\pi(p-q)[(p+q)a+2\alpha]/2}, \quad a, \alpha, p, q \in \mathbb{Z}/2\mathbb{Z} \tag{40}$$

and

$$w_{pq}(2\alpha) = \delta_{p,q}\delta_{p,\alpha}, \quad \alpha, p, q \in \mathbb{Z}/2\mathbb{Z} \tag{41}$$

The cases $a = 0, 1$ and $a = 2$ need to be treated separately.

For $a = 2$, we get

$$\Pi_{2\alpha} = \sum_{p=0}^{1}\sum_{q=0}^{1} w_{pq}(2\alpha)E_{pq} = \delta_{0,\alpha}E_{00} + \delta_{1,\alpha}E_{11} \tag{42}$$

The normalized eigenvectors of Π_{20} and Π_{21} associated with the eigenvalue equal to 1 are

$$|20\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |21\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{43}$$

For $a = 0$ and 1, we have

$$\Pi_{a\alpha} = \sum_{p=0}^{1}\sum_{q=0}^{1} w_{pq}(a\alpha)E_{pq} = \frac{1}{2}\left[E_{00} + \mathrm{e}^{\mathrm{i}(a+2\alpha)\pi/2}E_{01} + \mathrm{e}^{-\mathrm{i}(a+2\alpha)\pi/2}E_{10} + E_{11}\right] \tag{44}$$

When $a = 0$, the diagonalization of

$$\Pi_{00} = \frac{1}{2}(E_{00} + E_{01} + E_{10} + E_{11}) \tag{45}$$

$$\Pi_{01} = \frac{1}{2}(E_{00} - E_{01} - E_{10} + E_{11}) \tag{46}$$

leads to

$$|00\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |01\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \tag{47}$$

Similarly for $a = 1$, the matrices

$$\Pi_{10} = \frac{1}{2}(E_{00} + \mathrm{i}E_{01} - \mathrm{i}E_{10} + E_{11}) \tag{48}$$

$$\Pi_{11} = \frac{1}{2}(E_{00} - \mathrm{i}E_{01} + \mathrm{i}E_{10} + E_{11}) \tag{49}$$

yield

$$|10\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-\mathrm{i}\end{pmatrix}, \quad |11\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\\mathrm{i}\end{pmatrix} \tag{50}$$

The vectors (43), (47) and (50) correspond to the familiar bases of qubits associated with the eigenvectors of the Pauli matrices σ_z, σ_x and σ_y, respectively.

4. Conclusions

In conclusion, we have found a transformation that allows to replace the search of $d+1$ MUBs in $\mathbb{C}^d$ by the determination of $d(d+1)$ vectors in $\mathbb{C}^{d^2}$. Passing from $\mathbb{C}^d$ to $\mathbb{C}^{d^2}$ amounts to replacing the square of the modulus of the inner product $\langle a\alpha|b\beta\rangle$ in $\mathbb{C}^d$, see Equation (7), by the inner product $\mathbf{w}\ (a\alpha)\ \cdot\ \mathbf{w}(b\beta)$ in $\mathbb{C}^{d^2}$, see Equations (10) and (11). It is expected that the determination of the $d(d+1)$ vectors $\mathbf{w}(a\alpha)$ satisfying Equations (8) to (11) (or the $d(d+1)$ corresponding Hermitian positive-semidefinite matrices $M_{a\alpha}$ satisfying Equations (27) and (26)) should be easier than the determination of the $d(d+1)$ vectors $|a\alpha\rangle$ satisfying Equation (7). In this respect, the absence of a modulus in Equation (11) represents an incremental step.

Of course, the impossibility of finding $d(d+1)$ vectors $\mathbf{w}(a\alpha)$ or $d(d+1)$ matrices $M_{a\alpha}$ would mean that $d+1$ MUBs do not exist in $\mathbb{C}^d$ when d is not a strictly positive power of a prime. The techniques used in the determination of equiangular lines and equiangular tight frames [32,45] could perhaps be of value for determining the number of vectors in $\mathbb{C}^{d^2}$ satisfying Equation (23).

Transforming a given problem into another one is always interesting even in the case where the new problem does not lead to the solution of the first one. In this vein, the existence problem of MUBs in d dimensions was approached in the past from the points of view of various fields, e.g., finite geometry, Latin squares, Hadamard matrices, and Lie groups, just to name a few (see [39] and references therein), with some interesting developments both for MUBs and the involved fields. We hope that the results presented here will stimulate further works, especially a new way to handle the $d=6$ unsolved problem.

To close, let us mention that it should be interesting to apply the developments above (especially Proposition 1) to the concept of *weakly* MUBs recently introduced for dealing in the $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ phase space [46]. In addition, the results presented in this paper might be of interest in studies involving the concept of constellations of MUBs introduced in [18].

Acknowledgements

The author is indebted to Markus Grassl, Michel Planat, Apostol Vourdas, Stefan Weigert, and Karol Życzkowski for useful comments on a preliminary version of this paper.

References

1. Schwinger, J. Unitary operator bases. *Proc. Nat. Acad. Sci. USA* **1960**, *46*, 570–579.
2. Ivanović, I.D. Geometrical description of quantum state determination. *J. Phys. A-Math. Gen.* **1981**, *14*, 3241–3245.

3. Wootters, W.K. A Wigner-function formulation of finite-state quantum mechanics. *Ann. Phys. (N.Y.)* **1987**, *176*, 1–21.
4. Wootters, W.K.; Fields, B.D. Optimal state-determination by mutually unbiased measurements. *Ann. Phys. (N.Y.)* **1989**, *191*, 363–381.
5. Klappenecker, A.; Rötteler, M. Mutually Unbiased Bases are Complex Projective 2-Designs. In Proceedings of the 2005 IEEE International Symposium on Information Theory (ISIT'05), Adelaide, Australia, 4–9 September 2005; pp. 1740–1744.
6. Klimov, A.B.; Sánchez-Soto, L.L.; de Guise, H. Multicomplementary operators via finite Fourier transform. *J. Phys. A-Math. Gen.* **2005**, *38*, 2747–2760.
7. Gibbons, K.S.; Hoffman, M.J.; Wootters, W.K. Discrete phase space based on finite fields. *Phys. Rev. A* **2004**, *70*, 062101:1– 062101:23.
8. Pittenger, A.O.; Rubin, M.H. Wigner functions and separability for finite systems. *J. Phys. A-Math. Gen.* **2005**, *38*, 6005–6036.
9. Englert, B.-G.; Aharonov, Y. The mean king's problem: Prime degrees of freedom. *Phys. Lett. A* **2001**, *284*, 1–5.
10. Tolar, J.; Chadzitaskos, G. Feynman's path integral and mutually unbiased bases. *J. Phys. A-Math. Theor.* **2009**, *42*, 245306:1–245306:11.
11. Calderbank, A.R.; Cameron, P.J.; Kantor, W.M.; Seidel, J.J. Z4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. *Proc. Lond. Math. Soc.* **1997**, *75*, 436–480.
12. Cerf, N.J.; Bourennane, M.; Karlsson, A.; Gisin, N. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.* **2002**, *88*, 127902:1–127902:4.
13. Grassl, M. Tomography of quantum states in small dimensions. *Elec. Notes Discrete Math.* **2005**, *20*, 151–164.
14. Lawrence, J. Entanglement patterns in mutually unbiased basis sets for N prime-state particles. **2011**, arXiv:1103.3818 [quant-ph].
15. Wocjan, P.; Beth, T. New construction of mutually unbiased bases in square dimensions. *Quantum Inf. Comput.* **2005**, *5*, 93–101.
16. Grassl, M. On SIC-POVMs and MUBs in dimension 6. In Proceedings of the ERATO Conference on Quantum Information Science (EQIS'04), Tokyo, Japan, 1–5 September 2004; arXiv:quant-ph/0406175.
17. Bengtsson, I.; Bruzda, W.; Ericsson, Å.; Larsson, J.Å.; Tadej, W.; Życzkowski, K. Mutually unbiased bases and Hadamard matrices of order six. *J. Math. Phys.* **2007**, *48*, 052106:1–052106:21.
18. Brierley, S.; Weigert, S. Maximal sets of mutually unbiased quantum states in dimension 6. *Phys. Rev. A* **2008**, *78*, 042312:1–042312:8.
19. Brierley, S.; Weigert, S. Constructing mutually unbiased bases in dimension six. *Phys. Rev. A* **2009**, *79*, 052316:1–052316:13.
20. McNulty, D.; Weigert, S. The limited role of mutually unbiased product bases in dimension 6. *J. Phys. A-Math. Theor.* **2012**, *45*, 102001:1–102001:5.
21. McNulty, D.; Weigert, S. On the impossibility to extend triples of mutually unbiased product bases in dimension six. *Int. J. Quantum Inf.* **2012**, *10*, 1250056:1–1250056:11.

22. Zauner, G. Quantendesigns: Grundzuege einer nichtcommutativen Designtheorie. Dissertation, Universitaet Wien, Austria, 1999.
23. Chaturvedi, S. Aspects of mutually unbiased bases in odd-prime-power dimensions. *Phys. Rev. A* **2002**, *65*, 044301:1–044301:3.
24. Bandyopadhyay, S.; Boykin, P.O.; Roychowdhury, V.; Vatan, F. A new proof for the existence of mutually unbiased bases. *Algorithmica* **2002**, *34*, 512–528.
25. Lawrence, J.; Brukner, Č.; Zeilinger, A. Mutually unbiased binary observable sets on N qubits. *Phys. Rev. A* **2002**, *65*, 032320:1–032320:5.
26. Lawrence, J. Mutually unbiased bases and trinary operator sets for N qutrits. *Phys. Rev. A* **2004**, *70*, 012302:1–012302:10.
27. Pittenger, A.O.; Rubin, M.H. Mutually unbiased bases, generalized spin matrices and separability. *Linear Alg. Appl.* **2004**, *390*, 255–278.
28. Albouy, O.; Kibler, M.R. SU_2 nonstandard bases: Case of mutually unbiased bases. *SIGMA* **2007**, *3*, 076:1–076:22.
29. Bengtsson, I.; Ericsson, Å. Mutually unbiased bases and the complementary polytope. *Open Syst. Inf. Dyn.* **2005**, *12*, 107–120.
30. Bengtsson, I. MUBs, Polytopes, and Finite Geometries. In Proceedings of the AIP Conference 750, Vaxjo, Sweden, 7–12 June 2004; pp. 63–69.
31. Saniga, M.; Planat, M.; Rosu, H. Mutually unbiased bases and finite projective planes. *J. Opt. B Quantum Semiclassical Opt.* **2004**, *6*, L19–L20.
32. Godsil, C.D.; Roy, A. Equiangular lines, mutually unbiased bases, and spin models. *Eur. J. Combin.* **2009**, *30*, 246–262.
33. Kibler, M.R. Angular momentum and mutually unbiased bases. *Int. J. Mod. Phys. B* **2006**, *20*, 1792–1801.
34. Kibler, M.R.; Planat, M. A SU(2) recipe for mutually unbiased bases. *Int. J. Mod. Phys. B* **2006**, *20*, 1802–1807.
35. Kibler, M.R. An angular momentum approach to quadratic Fourier transform, Hadamard matrices, Gauss sums, mutually unbiased bases, unitary group and Pauli group. *J. Phys. A Math. Theor.* **2009**, *42*, 353001:1–353001:28.
36. Boykin, P.O.; Sitharam, M.; Tiep, P.H.; Wocjan, P. Mutually unbiased bases and orthogonal decompositions of Lie algebras. *J. Quantum Inform. Comput.* **2007**, *7*, 371–382.
37. Garcia, A.; Romero, J.L.; Klimov, A.B. Group-theoretical approach to the construction of bases in 2^n-dimensional Hilbert space. *Phys. Atom. Nuclei* **2011**, *74*, 876–883.
38. Daoud, M.; Kibler, M.R. Phase operators, temporally stable phase states, mutually unbiased bases and exactly solvable quantum systems. *J. Phys. A-Math. Theor.* **2010**, *43*, 115303:1–115303:18.
39. Durt, T.; Englert, B.-G.; Bengtsson, I.; Życzkowski, K. On mutually unbiased bases. *Int. J. Quantum Inf.* **2010**, *8*, 535–640.
40. Kibler, M.R. On mutually unbiased bases: Passing from d to d**2. **2012**, arXiv:1210.8173 [quant-ph].
41. Albouy, O.; Kibler, M.R. A unified approach to SIC-POVMs and MUBs. *J. Russ. Laser Res.* **2007**, *28*, 429–438.

42. Berndt, B.C.; Evans, R.J.; Williams, K.S. *Gauss and Jacobi Sums*; Wiley: New York, NY, USA, 1998.
43. Vourdas, A. Quantum systems with finite Hilbert space. *Rep. Prog. Phys.* **2004**, *67*, 267–320.
44. Kibler, M.R. Quadratic Discrete Fourier Transform and Mutually Unbiased Bases. In *Fourier Transforms-Approach to Scientific Principles*; Nikolić, G.S., Ed.; InTech: Rijeka, Croatia, 2011; pp. 103–138.
45. Mohammad-Abadi, S.A.; Najafi, M. Type of equiangular tight frames with $n + 1$ vectors in $\mathbf{R}^n$. *Int. J. Appl. Math. Res.* **2012**, *1*, 391–401.
46. Shalaby, M.; Vourdas, A. Weak mutually unbiased bases. *J. Phys. A: Math. Theor.* **2012**, *45*, 052001:1–052001:15.