FORMULA FOR UNBIASED BASES

Maurice R. Kibler

The present paper deals with mutually unbiased bases for systems of qudits in d dimensions. Such bases are of considerable interest in quantum information. A formula for deriving a complete set of $1 + p$ mutually unbiased bases is given for $d = p$ where p is a prime integer. The formula follows from a nonstandard approach to the representation theory of the group $SU(2)$. A particular case of the formula is derived from the introduction of a phase operator associated with a generalized oscillator algebra. The case when $d = p^e$ ($e \geq 2$), corresponding to the power of a prime integer, is briefly examined. Finally, complete sets of mutually unbiased bases are analysed through a Lie algebraic approach.

Keywords: mutually unbiased bases, Weyl pairs, phase states, Lie algebras

Classification: 81R05, 81R10, 81R15, 81R50

1. INTRODUCTION

This paper is based on a talk given at the conference *Analytic and algebraic methods in physics VI* (AAMP6) that took place in Prague, Czech Republic (8–11 May 2010). In the oral presentation at AAMP6, the accent was put on phase operators and phase states associated with a generalized oscillator algebra discussed in a group-theoretical context involving $SU(2)$ and $SU(1,1)$. Then, the whole material was applied to the so-called mutually unbiased bases (MUBs), to be defined below, which are of paramount importance in quantum information. In the present written presentation, we prefer to start with a construction of MUBs since such a presentation can be of interest to a larger audience. The connection with a phase operator for $SU(2)$, that leads to an unexpected relationship between MUBs and phase states, is thus considered in a second part of the paper.

Two orthonormal bases $B_a = \{|a\alpha\rangle : \alpha = 0, 1, \ldots, d-1\}$ and $B_b = \{|b\beta\rangle : \beta = 0, 1, \ldots, d-1\}$ of $\mathbb{C}^d$ are said to be unbiased if and only if the inner product $\langle a\alpha|b\beta\rangle$ has a modulus independant of α and β. In other words

$$\forall\alpha \in \mathbb{Z}_d, \forall\beta \in \mathbb{Z}_d : |\langle a\alpha|b\beta\rangle| = \delta_{a,b}\delta_{\alpha,\beta} + (1 - \delta_{a,b})\frac{1}{\sqrt{d}} \tag{1}$$

where $\mathbb{Z}_d := \mathbb{Z}/d\mathbb{Z}$. From Eq. (1), we see that if two MUBs undergo the same unitary or antiunitary transformation, they remain mutually unbiased. It is well-known that the maximum number N of MUBs in $\mathbb{C}^d$ is $N = 1 + d$ and that this number is attained when d is a prime number p or a power p^e ($e \geq 2$) of a prime number p [10, 12, 16, 28]. In the other cases ($d \neq p^e$, p prime and e integer with $e \geq 1$), the number N is not known although it can be shown that $3 \leq N \leq 1 + d$. In the general composite case $d = \prod_i p_i^{e_i}$, it is known that $1 + \min(p_i^{e_i}) \leq N \leq 1 + d$. In the particular composite case $d = 6$, there is a large consensus according to which $N = 3$. Indeed, in spite of an enormous amount of works, no more than $N = 3$ MUBs were found for $d = 6$ (see for example [6, 9, 15]).

The main aim of this paper is to report on a formula for obtaining $N = 1+p$ MUBs when $d = p$ where p is a prime integer. The paper is organized as follows. The basic formula is derived in Section 2 from a nonstandard approach to the representation theory of $SU(2)$. Sections 3 and 4 deal with complete sets of MUBs in the cases where d is a prime integer and a power of a prime integer, respectively. A particular case of the formula is obtained in Section 5 from the derivation of temporally stable phase states associated with a generalized oscillator algebra. Finally in Section 6, complete sets of MUBs for $d = p$ prime are briefly discussed in a group-theoretical approach.

2. A NONSTANDARD ANGULAR MOMENTUM BASIS

2.1. A nonstandard quantization scheme

The various irreducible representation classes of the group $SU(2)$ are characterized by a label j with $2j \in \mathbb{N}$. The standard irreducible matrix representation associated with j is spanned by the orthonormal basis

$$B_{2j+1} := \{|j, m\rangle : m = j, j-1, \ldots, -j\}$$

where the vector $|j, m\rangle$ is a common eigenvector of the Casimir operator J^2 and of the Cartan operator J_z of the Lie algebra $su(2)$ of $SU(2)$. More precisely, we have the relations

$$J^2|j, m\rangle = j(j+1)|j, m\rangle, \quad J_z|j, m\rangle = m|j, m\rangle$$

which are familiar in angular momentum theory.

Following the works in [1, 17, 20], let us define the linear operators v_{ra} and h by

$$v_{ra} := e^{i2\pi jr}|j, -j\rangle\langle j, j| + \sum_{m=-j}^{j-1} q^{(j-m)a}|j, m+1\rangle\langle j, m| \tag{2}$$

and

$$h := \sum_{m=-j}^{j} \sqrt{(j+m)(j-m+1)}|j, m\rangle\langle j, m|$$

where

$$r \in \mathbb{R}, \quad q := e^{2\pi i/(2j+1)}, \quad a \in \mathbb{Z}_{2j+1}$$

It is important to note that there are two types of phase factors in Eq. (2). They can be reduced to a single phase factor (viz. $q^{(j-m)a}$) solely in the case where $r = 0$. The introduction of $r \neq 0$ renders feasible to distinguish various sets of MUBs. It can be checked that the three operators

$$J_+ := h v_{ra}, \quad J_- := (v_{ra})^\dagger h, \quad J_z := \frac{1}{2}\left[h^2 - (v_{ra})^\dagger h^2 v_{ra}\right] \tag{3}$$

where $(v_{ra})^\dagger$ stands for the adjoint of v_{ra}, satisfy the commutation relations

$$[J_z, J_+] = +J_+, \quad [J_z, J_-] = -J_-, \quad [J_+, J_-] = 2J_z$$

of the algebra $su(2)$.

The operator v_{ra} is unitary while the operator h is Hermitian. Thus, Eq. (3) corresponds to a polar decomposition of $su(2)$ with the help of the operators v_{ra} and h. It is obvious that v_{ra} and J^2 commute. Therefore, the $\{J^2, v_{ra}\}$ scheme constitutes an alternative to the $\{J^2, J_z\}$ quantization scheme (well-known in the theory of angular momentum). To be more specific, we have the following result.

Theorem 2.1. For fixed j, r and a, the $2j+1$ vectors

$$|j\alpha; ra\rangle := \frac{1}{\sqrt{2j+1}} \sum_{m=-j}^{j} q^{(j+m)(j-m+1)a/2 - jmr + (j+m)\alpha} |j, m\rangle \tag{4}$$

with $\alpha = 0, 1, \ldots, 2j$, are common eigenvectors of v_{ra} and J^2. The eigenvalues of v_{ra} are given by

$$v_{ra}|j\alpha; ra\rangle = q^{j(r+a)-\alpha}|j\alpha; ra\rangle$$

so that the spectrum of v_{ra} is nondegenerate.

2.2. Introduction of qudits

Alternatively, by introducing the notation

$$j + m \equiv n, \quad d \equiv 2j+1, \quad |j, m\rangle \equiv |d-1-n\rangle, \quad |j\alpha; ra\rangle \equiv |a\alpha; r\rangle \tag{5}$$

the eigenvectors of v_{ra} read

$$|a\alpha; r\rangle := q^{(d-1)^2 r/4} \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} q^{n(d-n)a/2 - n(d-1)r/2 + n\alpha} |d-1-n\rangle \tag{6}$$

with $\alpha = 0, 1, \ldots, d-1$.

For fixed d, r and a, the inner product

$$\langle a\alpha; r | a\beta; r\rangle = \delta_{\alpha,\beta}$$

shows that

$$B_{ra} := \{|a\alpha; r\rangle : \alpha = 0, 1, \ldots, d-1\} \tag{7}$$

is an orthonormal basis of $\mathbb{C}^d$. This basis constitutes a nonstandard basis for the irreducible representation of $SU(2)$ associated with j. Each basis B_{ra} ($r \in \mathbb{R}$, $a \in \mathbb{Z}_d$) provides us with an alternative to the standard basis $B_{2j+1} \equiv B_d$ of angular momentum theory, known as the computational (or Fock) basis in quantum information and quantum computating.

Before giving two examples, let us mention that in some previous works by the author a notation different (although equivalent) was used in place of (5). The notation used here ensures that the states $|1/2, 1/2\rangle \equiv |0\rangle$ and $|1/2, -1/2\rangle \equiv |1\rangle$ correspond to the usual qubits with the good angular momentum label. More generally in dimension d, the qudits $|0\rangle, |1\rangle, \ldots, |d-1\rangle$ correspond to the angular momentum states $|j, j\rangle, |j, j-1\rangle, \ldots, |j, -j\rangle$, respectively.

Example 2.2. For $d = 2$, we have two families of bases: the B_{r0} family and the B_{r1} family (a can take the values $a = 0$ and $a = 1$). Thus Eq. (6) leads to

$$|a\alpha; r\rangle = \frac{1}{\sqrt{2}}(q^{r/4}|1\rangle + q^{a/2-r/4+\alpha}|0\rangle)$$

with $q = e^{i\pi}$. In detail, we have

$$\begin{aligned}
B_{r0}: \qquad & |00; r\rangle = \frac{1}{\sqrt{2}}\left(e^{i\pi r/4}|1\rangle + e^{-i\pi r/4}|0\rangle\right) \\
& |01; r\rangle = \frac{1}{\sqrt{2}}\left(e^{i\pi r/4}|1\rangle - e^{-i\pi r/4}|0\rangle\right) \\
B_{r1}: \qquad & |10; r\rangle = \frac{1}{\sqrt{2}}\left(e^{i\pi r/4}|1\rangle + ie^{-i\pi r/4}|0\rangle\right) \\
& |11; r\rangle = \frac{1}{\sqrt{2}}\left(e^{i\pi r/4}|1\rangle - ie^{-i\pi r/4}|0\rangle\right)
\end{aligned}$$

In particular, for $r = 0$ the bases B_{00} and B_{01} are (up to a rearrangement) nothing but the familiar bases used in quantum information.

Example 2.3. For $d = 3$, we have three families of bases, that is to say B_{r0}, B_{r1} and B_{r2}, since a can be 0, 1 and 2. In the case $r = 0$, Eq. (6) gives

$$|a\alpha; 0\rangle = \frac{1}{\sqrt{3}}(|2\rangle + q^{a+\alpha}|1\rangle + q^{a+2\alpha}|0\rangle)$$

which yields

$$\begin{aligned}
B_{00}: \qquad & |00; 0\rangle = \frac{1}{\sqrt{3}}\left(|2\rangle + |1\rangle + |0\rangle\right) \\
& |01; 0\rangle = \frac{1}{\sqrt{3}}\left(|2\rangle + q|1\rangle + q^2|0\rangle\right) \\
& |02; 0\rangle = \frac{1}{\sqrt{3}}\left(|2\rangle + q^2|1\rangle + q|0\rangle\right)
\end{aligned}$$

$$
\begin{aligned}
B_{01}: \qquad & |10;0\rangle = \frac{1}{\sqrt{3}} \left(|2\rangle + q|1\rangle + q|0\rangle\right) \\
& |11;0\rangle = \frac{1}{\sqrt{3}} \left(|2\rangle + q^2|1\rangle + |0\rangle\right) \\
& |12;0\rangle = \frac{1}{\sqrt{3}} \left(|2\rangle + |1\rangle + q^2|0\rangle\right) \\
B_{02}: \qquad & |20;0\rangle = \frac{1}{\sqrt{3}} \left(|2\rangle + q^2|1\rangle + q^2|0\rangle\right) \\
& |21;0\rangle = \frac{1}{\sqrt{3}} \left(|2\rangle + |1\rangle + q|0\rangle\right) \\
& |22;0\rangle = \frac{1}{\sqrt{3}} \left(|2\rangle + q|1\rangle + |0\rangle\right)
\end{aligned}
$$

with $q = e^{i2\pi/3}$.

3. THE CASE OF A PRIME DIMENSION

For $d = 2$ and fixed r, it can be checked that the bases B_{r0}, B_{r1} and B_2 (see Example 2.2) are $1 + d = 3$ MUBs. A similar result follows for $d = 3$: the bases B_{00}, B_{01}, B_{02} and B_3 (see Example 2.3) are $1 + d = 4$ MUBs. This can be generalized by the following main result.

Theorem 3.1. For $d = p$, with p a prime number, the bases $B_{r0}, B_{r1}, \ldots, B_{rp-1}, B_p$ corresponding to a fixed value of r form a complete set of $1 + p$ MUBs. The p^2 vectors $|a\alpha; r\rangle$, with $a, \alpha = 0, 1, \ldots, p-1$, of the bases $B_{r0}, B_{r1}, \ldots, B_{rp-1}$ are given by a single formula (namely Eq. (6)). The index r makes it possible to distinguish different sets of complete MUBs.

Proof. First, Eq. (6) can be seen as a quadratic discrete Fourier transform of the states $|0\rangle, |1\rangle, \ldots, |d-1\rangle$ (quadratic because n^2 occurs in the coefficients of the transformation). Therefore

$$
|\langle p-1-n|a\alpha; r\rangle| = \frac{1}{\sqrt{p}}
$$

holds for fixed r and for all n, a and α in the Galois field $\mathbb{F}_p$ so that each basis B_{ra} is unbiased with B_p. Second, we get

$$
\langle a\alpha; r|b\beta; r\rangle = \frac{1}{p} \sum_{k=0}^{p-1} q^{k(p-k)(b-a)/2+k(\beta-\alpha)} \tag{8}
$$

or

$$
\langle a\alpha; r|b\beta; r\rangle = \frac{1}{p} \sum_{k=0}^{p-1} e^{i\pi\{(a-b)k^2+[p(b-a)+2(\beta-\alpha)]k\}/p} \tag{9}
$$

The right-hand side of (9) can be expressed in terms of a generalized quadratic Gauss sum [7]

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

where u, v and w are integers such that u and w are mutually prime, $uw \neq 0$ and $uw + v$ is even. This leads to

$$\langle a\alpha; r|b\beta; r\rangle = \frac{1}{p} S(u, v, w) \tag{10}$$

with

$$u := a - b, \quad v := -(a - b)p - 2(\alpha - \beta), \quad w := p \tag{11}$$

The generalized Gauss sum $S(u, v, w)$ in (10) // (11) can be calculated from the methods described in [7]. We thus obtain

$$|\langle a\alpha; r|b\beta; r\rangle| = \frac{1}{\sqrt{p}}$$

which completes the proof. □

At this stage, it is interesting to note a connection between MUBs and generalized Hadamard matrices (see also [27, 2, 6, 9, 19]). In the case where d is arbitrary, for fixed r and a, let us introduce from (6) the d-dimensional matrix F_{ra} defined by its matrix elements

$$(F_{ra})_{n\alpha} := \frac{1}{\sqrt{d}} q^{-n^2a/2+n[da/2+\alpha-(d-1)r/2]+(d-1)^2r/4}$$

where $n, \alpha = 0, 1, \ldots, d-1$. The matrix F_{ra} is a unitary matrix for which each entry has a modulus equal to $1/\sqrt{d}$. Thus, F_{ra} is a generalized Hadamard matrix (see [13, 26] for a definition of a complex Hadamard matrix with two different normalizations). Then, Eq. (8) can be rewritten as

$$\langle a\alpha; r|b\beta; r\rangle = \left(F_{ra}^{\dagger} F_{rb}\right)_{\alpha\beta}$$

Therefore, going back to the case where $d = p$ is a prime integer, we find that the product $F_{ra}^{\dagger} F_{rb}$ is another generalized Hadamard matrix for d prime.

To close this section, we may ask what becomes Theorem 3.1 when the prime integer p is replaced by an arbitrary (not prime) integer d. In this case, the formula (6) does not provide a complete set of $1 + d$ MUBs. However, it is possible to show that the bases B_{ra}, $B_{ra\oplus 1}$ and B_d are 3 MUBs in $\mathbb{C}^d$ (the addition $\oplus$ is understood modulo d) [19]. This result is in agreement with the well-known result according to which the maximum number of MUBs in $\mathbb{C}^d$, with d arbitrary, is greater or equal to 3 (see for example [15]). Moreover, it can be proved [19] that the bases B_{ra} and $B_{ra\oplus 2}$ are unbiased for d odd with $d \geq 3$ (d prime or not prime).

4. THE CASE OF A POWER OF A PRIME DIMENSION

Equation (6) can be used for deriving a complete set of $1+p^e$ MUBs in the case where $d = p^e$ is a power ($e \geq 2$) of a prime integer p. The general case is very much involved. Hence, we shall start with the case $p = e = 2$ corresponding to two qubits.

Example 4.1. For $d = 4$, Eq. (7) yields four families of bases B_{ra} ($a = 0, 1, 2, 3$). For each family, the basis vectors can be determined from Eq. (6). As a matter of fact, the bases B_{r0}, B_{r1}, B_{r2}, B_{r3} and B_4 do not form a complete set of $1 + d = 5$ MUBs. However, it is possible to construct a set of 5 MUBs from repeated application of (6).

For the purpose of simplicity, we shall take $r = 0$ and adopt the notation

$$|a\alpha\rangle \equiv |a\alpha; 0\rangle$$

Four of the 5 MUBs for $d = 4$ can be constructed from the direct products $|a\alpha\rangle \otimes |b\beta\rangle$ which are eigenvectors of the operators $v_{0a} \otimes v_{0b}$. Obviously, the set

$$B_{0a0b} := \{|a\alpha\rangle \otimes |b\beta\rangle : \alpha, \beta = 0, 1\}$$

is an orthonormal basis in $\mathbb{C}^4$. It is evident that B_{0000} and B_{0101} are two unbiased bases since the modulus of the inner product of $|0\alpha\rangle \otimes |0\beta\rangle$ by $|1\alpha'\rangle \otimes |1\beta'\rangle$ is

$$|\langle 0\alpha|1\alpha'\rangle\langle 0\beta|1\beta'\rangle| = \frac{1}{\sqrt{4}}$$

A similar result holds for the two bases B_{0001} and B_{0100}. However, the four bases B_{0000}, B_{0101}, B_{0001} and B_{0100} are not mutually unbiased. A possible way to overcome this uninteresting result is to keep the bases B_{0000} and B_{0101} intact and to re-organize the vectors inside the bases B_{0001} and B_{0100} in order to obtain 4 MUBs. We are thus left with 4 bases

$$W_{00} \equiv B_{0000}, \quad W_{11} \equiv B_{0101}, \quad W_{01}, \quad W_{10}$$

which together with the computational basis B_4 give 5 MUBs. In a detailed way, we have

$$\begin{aligned}
W_{00} &:= \{|0\alpha\rangle \otimes |0\beta\rangle : \alpha, \beta = 0, 1\} \\
W_{11} &:= \{|1\alpha\rangle \otimes |1\beta\rangle : \alpha, \beta = 0, 1\} \\
W_{01} &:= \{\lambda|0\alpha\rangle \otimes |1\beta\rangle + \mu|0\alpha \oplus 1\rangle \otimes |1\beta \oplus 1\rangle : \alpha, \beta = 0, 1\} \\
W_{10} &:= \{\lambda|1\alpha\rangle \otimes |0\beta\rangle + \mu|1\alpha \oplus 1\rangle \otimes |0\beta \oplus 1\rangle : \alpha, \beta = 0, 1\}
\end{aligned}$$

where

$$\lambda := \frac{1-i}{2}, \quad \mu := \frac{1+i}{2}$$

and the vectors of type $|a\alpha\rangle$ are given by the master formula (6). As a résumé, only two formulas are necessary for obtaining the $d^2 = 16$ vectors $|ab, \alpha\beta\rangle$ for the bases W_{ab}, namely

$$W_{00}, W_{11} \quad : \quad |aa, \alpha\beta\rangle := |a\alpha\rangle \otimes |a\beta\rangle \tag{12}$$

$$W_{01}, W_{10} \quad : \quad |aa \oplus 1, \alpha\beta\rangle := \lambda|a\alpha\rangle \otimes |a \oplus 1\beta\rangle + \mu|a\alpha \oplus 1\rangle \otimes |a \oplus 1\beta \oplus 1\rangle \tag{13}$$

for all a, α, β in $\mathbb{Z}_2$. By developing (12) and (13) with the help of (6), we end up with the results given in [19]. By introducing the triplet

$$t_1 := |0\rangle \otimes |0\rangle, \quad t_0 := \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle), \quad t_{-1} := |1\rangle \otimes |1\rangle \tag{14}$$

which spans the irreducible representation of SU(2) associated with $j = 1$, and the singlet

$$s := \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) \tag{15}$$

which spans the irreducible representation of SU(2) associated with $j = 0$, we can write (up to irrelevant phase factors) the vectors of the 5 MUBs for $d = 4$ as follows.

The W_{00} basis:

$$\begin{aligned}
|00,00\rangle &= \frac{1}{2}(t_1 + \sqrt{2}t_0 + t_{-1}) \\
|00,01\rangle &= \frac{1}{2}(t_1 - \sqrt{2}s - t_{-1}) \\
|00,10\rangle &= \frac{1}{2}(t_1 + \sqrt{2}s - t_{-1}) \\
|00,11\rangle &= \frac{1}{2}(t_1 - \sqrt{2}t_0 + t_{-1})
\end{aligned}$$

The W_{11} basis:

$$\begin{aligned}
|11,00\rangle &= \frac{1}{2}(t_1 + i\sqrt{2}t_0 - t_{-1}) \\
|11,01\rangle &= \frac{1}{2}(t_1 - i\sqrt{2}s + t_{-1}) \\
|11,10\rangle &= \frac{1}{2}(t_1 + i\sqrt{2}s + t_{-1}) \\
|11,11\rangle &= \frac{1}{2}(t_1 - i\sqrt{2}t_0 - t_{-1})
\end{aligned}$$

The W_{01} basis:

$$\begin{aligned}
|01,00\rangle &= \frac{1}{2}(t_1 + \sqrt{2}\lambda t_0 + \sqrt{2}\mu s + it_{-1}) \\
|01,11\rangle &= \frac{1}{2}(t_1 - \sqrt{2}\lambda t_0 - \sqrt{2}\mu s + it_{-1}) \\
|01,01\rangle &= \frac{1}{2}(t_1 - \sqrt{2}\mu t_0 - \sqrt{2}\lambda s - it_{-1}) \\
|01,10\rangle &= \frac{1}{2}(t_1 + \sqrt{2}\mu t_0 + \sqrt{2}\lambda s - it_{-1})
\end{aligned}$$

The W_{10} basis:

$$
\begin{aligned}
|10,00\rangle &= \frac{1}{2}(t_1 + \sqrt{2}\lambda t_0 - \sqrt{2}\mu s + i t_{-1}) \\
|10,11\rangle &= \frac{1}{2}(t_1 - \sqrt{2}\lambda t_0 + \sqrt{2}\mu s + i t_{-1}) \\
|10,01\rangle &= \frac{1}{2}(t_1 + \sqrt{2}\mu t_0 - \sqrt{2}\lambda s - i t_{-1}) \\
|10,10\rangle &= \frac{1}{2}(t_1 - \sqrt{2}\mu t_0 + \sqrt{2}\lambda s - i t_{-1})
\end{aligned}
$$

The computational basis:

$$|0\rangle \otimes |0\rangle = t_1, \ |0\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(t_0 + s), \ |1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(t_0 - s), \ |1\rangle \otimes |1\rangle = t_{-1}$$

Each of the 3 vectors (14) and the vector (15) transform under the the group S_2 (generated by the interchange $|i\rangle \otimes |j\rangle \leftrightarrow |j\rangle \otimes |i\rangle$) as the irreducible representations [2] and $[1^2]$, respectively. It should be noted that only 6 of the 20 quartits for $d = 4$ transform as an irreducible representation of S_2 (viz. the symmetric representation [2]). Furthermore, the vectors of the W_{00} and W_{11} bases are not intricated (i. e., each vector is the direct product of two vectors) while the vectors of the W_{01} and W_{10} bases are intricated (i. e., each vector is not the direct product of two vectors).

Generalization of (12) and (13) can be obtained in more complicated situations (two qupits, three qubits, ...). The generalization of (12) is immediate. The generalization of (13) can be achieved by taking linear combinations of vectors such that each linear combination is made of vectors corresponding to the same eigenvalue of the relevant tensor product of operators of type v_{ra}. By way of illustration, let us consider the case $p = e - 1 = 2$ corresponding to three qubits.

Example 4.2. For $d = 8$, we can start from the eight bases

$$B_{0a0b0c} := \{|a\alpha\rangle \otimes |b\beta\rangle \otimes |c\gamma\rangle : \alpha, \beta, \gamma = 0, 1\}$$

for all a, b and c in $\mathbb{Z}_2$. The analogs of (12) are

$$W_{000} \equiv B_{000000}, \quad W_{111} \equiv B_{010101}$$

Clearly, W_{000} and W_{111} are unbiased. Similarly, the bases B_{000001} and B_{010100} are mutually unbiased but are not unbiased with W_{000} and W_{111}. Then, we can replace B_{000001} and B_{010100} respectively by W_{001} and W_{110} defined by

$$W_{aaa\oplus 1} := \{|aaa \oplus 1, \alpha\beta\gamma\rangle : \alpha, \beta, \gamma = 0, 1\}, \quad a = 0, 1 \tag{16}$$

with

$$
\begin{aligned}
|aaa \oplus 1, \alpha\beta\gamma\rangle \quad := \quad & \frac{\lambda}{\sqrt{2}} |a\alpha\rangle \otimes |a\beta\rangle \otimes |a \oplus 1\gamma\rangle \\
+ \quad & \frac{\mu}{\sqrt{2}} |a\alpha\rangle \otimes |a\beta \oplus 1\rangle \otimes |a \oplus 1\gamma \oplus 1\rangle \\
+ \quad & \frac{\lambda}{\sqrt{2}} |a\alpha \oplus 1\rangle \otimes |a\beta\rangle \otimes |a \oplus 1\gamma \oplus 1\rangle \\
- \quad & \frac{\mu}{\sqrt{2}} |a\alpha \oplus 1\rangle \otimes |a\beta \oplus 1\rangle \otimes |a \oplus 1\gamma\rangle
\end{aligned}
\tag{17}
$$

It can be seen that the bases W_{000}, W_{111}, W_{001} and W_{110} together with the computational basis B_8 form a set of 5 MUBs. Four more MUBs can be derived from $B_{0a0a\oplus 10a}$ and $B_{0a\oplus 10a0a}$ (with $a = 1, 2$). This leads to the bases $W_{aa\oplus 1a}$ and $W_{a\oplus 1aa}$ (with $a = 1, 2$) defined by formuls analogous to (16) and (17) up to permutations.

5. UNBIASED BASES AND PHASE OPERATOR

A connection between MUBs and a phase operator associated with a generalized oscillator algebra was recently addressed in two works [11, 3]. We establish here a link between these works and the results in Section 2.

The starting point is to consider the one-parameter algebra A_κ spanned by the three linear operators a^-, a^+ and N satisfying

$$
[a^-, a^+] = I + 2\kappa N, \quad [N, a^\pm] = \pm a^\pm, \quad \left(a^-\right)^\dagger = a^+, \quad N^\dagger = N
$$

where I is the identity operator and κ a real parameter. For $\kappa < 0$, by putting

$$
J_- := \frac{1}{\sqrt{-\kappa}} a^-, \quad J_+ := \frac{1}{\sqrt{-\kappa}} a^+, \quad J_3 := \frac{1}{2\kappa}(I + 2\kappa N)
$$

it is immediate to see that J_-, J_+ and J_3 span the Lie algebra of $SU(2)$. Similarly for $\kappa > 0$, the operators

$$
K_- := \frac{1}{\sqrt{\kappa}} a^-, \quad K_+ := \frac{1}{\sqrt{\kappa}} a^+, \quad K_3 := \frac{1}{2\kappa}(I + 2\kappa N)
$$

generate the Lie algebra of $SU(1,1)$.

In both cases ($A_\kappa \sim su(2)$ or $su(1,1)$), we can consider the Hilbertian representation of A_κ defined by the following actions

$$
\begin{aligned}
a^+|n\rangle &= \sqrt{F(n+1)}e^{-i[F(n+1)-F(n)]\varphi}|n+1\rangle \\
a^-|n\rangle &= \sqrt{F(n)}e^{+i[F(n)-F(n-1)]\varphi}|n-1\rangle \\
a^-|0\rangle &= 0, \quad N|n\rangle = n|n\rangle
\end{aligned}
\tag{18}
$$

of the operators a^+, a^- and N on a Hilbert space $\mathcal{F}_\kappa$, with an orthonormal basis $\{|n\rangle : n = 0, 1, \ldots, d_\kappa\}$. The function $F : \mathbb{N} \to \mathbb{R}_+$ satisfies

$$
F(n+1) - F(n) = 1 + 2\kappa n, \quad F(0) = 0 \quad \Rightarrow \quad F(n) = n[1 + \kappa(n-1)]
$$

and φ is an arbitrary real parameter. In the case $\kappa > 0$, corresponding to $A_\kappa \sim su(1,1)$, the dimension of $\mathcal{F}_\kappa$ is infinite. In the case $\kappa < 0$, corresponding to $A_\kappa \sim su(2)$, $\mathcal{F}_\kappa$ is finite-dimensional with a dimension d given by

$$d := d_\kappa + 1 = 1 - \frac{1}{\kappa}, \quad -\frac{1}{\kappa} \in \mathbb{N}^*$$

We now continue with the case $\kappa < 0$.

In order to transcribe (18) in the language of the representation theory of $SU(2)$, we introduce the correspondence

$$|n\rangle \leftrightarrow |j,m\rangle, \quad n \leftrightarrow j+m, \quad d = 2j+1 = 1 - \frac{1}{\kappa} \Leftrightarrow 2j\kappa = -1$$

where $|j,m\rangle$ is an eigenvector of J_z and of the Casimir operator $J^2 := J_+J_- + J_z(J_z - 1)$. As a result, (18) yields

$$\begin{aligned} J_+|j,m\rangle &= \sqrt{(j-m)(j+m+1)}e^{-2im\kappa\varphi}|j,m+1\rangle \\ J_-|j,m\rangle &= \sqrt{(j+m)(j-m+1)}e^{2i(m-1)\kappa\varphi}|j,m-1\rangle \\ J_3|j,m\rangle &= m|j,m\rangle \end{aligned}$$

which differ from the standard relations of angular momentum theory by two phase factors.

We now define the operator E_d via

$$J_- = E_d\sqrt{J_+J_-}$$

Consequently

$$E_d|j,m\rangle = e^{2i(m-1)\kappa\varphi}|j,m-1\rangle \quad \text{for} \quad m \neq -j$$

and

$$E_d|j,-j\rangle = e^{-i\varphi}|j,j\rangle \quad \text{for} \quad m = -j$$

which show that E_d is unitary. Let us look for vectors $|z\rangle$ such that

$$E_d|z\rangle = z|z\rangle, \quad |z\rangle := \sum_{m=-j}^{j} d_m z^{j+m}|j,m\rangle, \quad z \in \mathbb{C}, \quad d_m \in \mathbb{C}$$

The solution requires

$$z^{2j+1} = 1 \;\Rightarrow\; z = q^\alpha, \quad q = e^{2\pi i/(2j+1)}, \quad \alpha = 0, 1, \ldots, 2j$$

As a result, $|z\rangle$ depends on a continuous parameter φ and a discrete parameter α. In detail, we have

$$|z\rangle \equiv |\varphi,\alpha\rangle = \frac{1}{\sqrt{2j+1}} \sum_{m=-j}^{j} e^{i(j+m)(j-m+1)\kappa\varphi} q^{(j+m)\alpha}|j,m\rangle$$

which has a form similar to (4).

We are now ready to establish a connection with MUBs. By assuming

$$\varphi = -\pi \frac{2j}{2j+1} a \Leftrightarrow \kappa\varphi = \frac{\pi}{2j+1} a, \quad a = 0, 1, \ldots, 2j \tag{19}$$

the state vector $|\varphi, \alpha\rangle$ becomes

$$|\varphi, \alpha\rangle \equiv |a\alpha\rangle = \frac{1}{\sqrt{2j+1}} \sum_{m=-j}^{j} q^{(j+m)(j-m+1)a/2+(j+m)\alpha} |j, m\rangle$$

to be compared with (4). We thus obtain the state $|j\alpha; ra\rangle$ with $r = 0$. Furthermore, it can be shown that the operators E_d and ${v_{0a}}^{\dagger}$ are linearly dependent.

6. MUTUALLY UNBIASED BASES AND LIE AGEBRAS

6.1. Weyl pairs

Let us denote V_{ra} the matrix of the operator v_{ra} builded on the basis vectors $|j, j\rangle \equiv |0\rangle, |j, j-1\rangle \equiv |1\rangle, \ldots, |j, -j\rangle \equiv |d-1\rangle$ (with the lines and columns in the order $0, 1, \ldots, d-1$ from top to bottom and from left to right). From (2), we thus obtain the d-dimensional unitary matrix

$$V_{ra} = \begin{pmatrix} 0 & q^a & 0 & \ldots & 0 \\ 0 & 0 & q^{2a} & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & q^{(d-1)a} \\ e^{i\pi(d-1)r} & 0 & 0 & \ldots & 0 \end{pmatrix}$$

(Recall that r is a real parameter, $q := e^{2\pi i/d}$ is a primitive root of unity and a belongs to the ring $\mathbb{Z}_d$ with $d = 2j + 1$.)

The matrix V_{ra} can be decomposed as

$$V_{ra} = P_r X Z^a$$

where

$$P_r := \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & e^{i\pi(d-1)r} \end{pmatrix}$$

and

$$X := \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}, \quad Z := \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & q & 0 & \ldots & 0 \\ 0 & 0 & q^2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & q^{d-1} \end{pmatrix}$$

The unitary matrices X and Z q-commute in the sense that

$$XZ - qZX = 0 \tag{20}$$

In addition, they satisfy

$$X^d = Z^d = I_d \tag{21}$$

where I_d is the d-dimensional unit matrix. Equations (20) and (21) show that X and Z constitute a Weyl pair. The Weyl pair (X, Z) turns out to be an integrity basis for generating a set $\{X^a Z^b : a, b \in \mathbb{Z}_d\}$ of d^2 generalized Pauli matrices in d dimensions (see for instance [14, 21, 5, 23, 25, 18] in the context of MUBs and [24, 4, 22] in group-theoretical contexts). In this respect, note that for $d = 2$ we have

$$X = \sigma_x, \quad Z = \sigma_z, \quad XZ = -i\sigma_y, \quad X^0 Z^0 = \sigma_0$$

in terms of the ordinary Pauli matrices $\sigma_0 = I_2$, σ_x, σ_y and σ_z. Equations (20) and (21) can be generalized through

$$V_{ra}Z - qZV_{ra} = 0, \quad (V_{ra})^d = e^{i\pi(d-1)(r+a)} I_d, \quad Z^d = I_d$$

so that other pairs of Weyl can be obtained from V_{ra} and Z.

6.2. MUBs and the special linear group

In the case where d is a prime integer or a power of a prime integer, it is known that the set $\{X^a Z^b : a, b = 0, 1, \ldots, d-1\}$ of cardinality d^2 can be partitioned into $1 + d$ subsets containing each $d - 1$ commuting matrices (cf. [5]). Let us give an example.

Example 6.1. For $d = 5$, we have the 6 following sets of 4 commuting matrices

$$\begin{aligned}
\mathcal{V}_0 &:= \{01, 02, 03, 04\} \\
\mathcal{V}_1 &:= \{10, 20, 30, 40\} \\
\mathcal{V}_2 &:= \{11, 22, 33, 44\} \\
\mathcal{V}_3 &:= \{12, 24, 31, 43\} \\
\mathcal{V}_4 &:= \{13, 21, 34, 42\} \\
\mathcal{V}_5 &:= \{14, 23, 32, 41\}
\end{aligned}$$

where ab is used as an abbreviation of $X^a Z^b$.

More generally, for $d = p$ with p prime, the $1+p$ sets of $p-1$ commuting matrices are easily seen to be

$$\begin{aligned}
\mathcal{V}_0 &:= \{X^0 Z^a : a = 1, 2, \ldots, p-1\} \\
\mathcal{V}_1 &:= \{X^a Z^0 : a = 1, 2, \ldots, p-1\} \\
\mathcal{V}_2 &:= \{X^a Z^a : a = 1, 2, \ldots, p-1\} \\
\mathcal{V}_3 &:= \{X^a Z^{2a} : a = 1, 2, \ldots, p-1\} \\
&\vdots \\
\mathcal{V}_{p-1} &:= \{X^a Z^{(p-2)a} : a = 1, 2, \ldots, p-1\} \\
\mathcal{V}_p &:= \{X^a Z^{(p-1)a} : a = 1, 2, \ldots, p-1\}
\end{aligned}$$

Each of the $1+p$ sets $\mathcal{V}_0, \mathcal{V}_1, \ldots, \mathcal{V}_p$ can be put in a one-to-one correspondance with one basis of the complete set of $1+p$ MUBs. In fact, $\mathcal{V}_0$ is associated with the computational basis while $\mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_p$ are associated with the p remaining MUBs in view of

$$V_{0a} \in \mathcal{V}_{a \oplus 1}, \quad a = 0, 1, \ldots, p-1$$

Keeping into account the fact that the set $\{X^a Z^b : a, b = 0, 1, \ldots, p-1\} \setminus \{X^0 Z^0\}$ spans the Lie algebra of the special linear group $SL(p, \mathbb{C})$, we have the following result.

Corollary 6.2. For $d = p$, with p a prime integer, the Lie algebra $sl(p, \mathbb{C})$ of the group $SL(p, \mathbb{C})$ can be decomposed into a sum (vector space sum) of $1+p$ abelian subalgebras each of dimension $p-1$, i. e.

$$sl(p, \mathbb{C}) \simeq v_0 \uplus v_1 \uplus \ldots \uplus v_p$$

where the $1+p$ subalgebras $v_0, v_1, \ldots, v_p$ are Cartan subalgebras generated respectively by the sets $\mathcal{V}_0, \mathcal{V}_1, \ldots, \mathcal{V}_p$ containing each $p-1$ commuting matrices.

Corollary 6.2 can be extended when $d = p^e$ with p a prime integer and e an integer ($e \geq 2$): there exists a decomposition of $sl(p^e, \mathbb{C})$ into $1+p^e$ abelian subalgebras of dimension $p^e - 1$ (cf. [22, 8, 19]).

7. CONCLUSION

There exist numerous ways of constructing sets of MUBs. In many of the papers dealing with the construction of MUBs, the explicit derivation of the bases requires the diagonalization of a set of matrices. Theorem 2.1 of the present paper gives a closed form formula which in last analysis corresponds to the diagonalization of a single matrix, the matrix V_{ra}. This formula is easily codable on a classical computer. It makes it possible to derive in one step the $(1+p)p$ vectors of the $1+p$ MUBs in dimension p, with p a prime integer (Theorem 3.1). It can be useful equally well in the case where p is replaced by a power p^e by considering tensor products of order e of vectors in $\mathbb{C}^p$.

Indeed, the formula can be understood as the quadratic discrete Fourier transform of the computational basis. This formula can also be applied in arbitrary dimension d. However for $d \neq p^e$ with p prime and $e \geq 1$, the formula does give a complete sets of MUBs. It was shown that a special case of the formula, corresponding to the eigenvectors of the matrix V_{0a}, follows from the diagonalization of a phase operator for a generalized oscillator algebra. As an open question, it would be interesting to find the significance of the quantization condition (19) which is required to establish a connection between the phase operator and MUBs.

To close, let us note that from the master matrix V_{ra} we can deduce the Weyl pair (X, Z) via

$$X = V_{00}, \quad Z = V_{00}^{\dagger} V_{01}$$

The operators X and Z are known as the flip or shift and clock operators, respectively. For d arbitrary, they are at the root of the Pauli group, a finite subgroup of order d^3 of the group $U(d)$, of considerable importance in quantum information and quantum computing (e. g., see [18]). The matrix V_{ra} is thus central for the study of the Pauli group. Finally, another interest of the Weyl pair (X, Z) is provided by Corollary 6.2 concerning the decomposition for $d = p$ prime of the Lie algebra $sl(p, \mathbb{C})$ into $1 + p$ Cartan subalgebras of dimension $p - 1$.

ACKNOWLEDGEMENT

I thank M. Znojil for the nice organization of the 6th international microconference *Analytic and algebraic methods in physics VI*. Thanks are due to M. Daoud, N.M. Atakishiyev and K.B. Wolf for a collaboration on phase operators. Finally, I am grateful to J. Tolar and U. Günther for interesting comments on this work and to the two referees for pertinent remarks and suggestions.

(Received June 28, 2010)

REFERENCES

[1] O. Albouy and M. R. Kibler: SU(2) nonstandard bases: Case of mutually unbiased bases. SIGMA *3* (2007), 076 (22 pages).

[2] M. Aschbacher, A. M. Childs, and P. Wocjan: The limitations of nice mutually unbiased bases. J. Algebr. Comb. *25* (2007), 111–123.

[3] N. M. Atakishiyev, M. R. Kibler, and K. B. Wolf: SU(2) and SU(1,1) approaches to phase operators and temporally stable phase states: applications to mutually unbiased bases and discrete Fourier transforms. (in preparation)

[4] R. Balian and C. Itzykson: Observations sur la mécanique quantique finie. C. R. Acad. Sci. (Paris) *303* (1986), 773–778.

[5] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan: A new proof for the existence of mutually unbiased bases. Algorithmica *34* (2002), 512–528.

[6] I. Bengtsson, W. Bruzda, Å. Ericsson, J. Å. Larsson, W. Tadej, and K. Życkowski: Mutually unbiased bases and Hadamard matrices of order six. J. Math. Phys. *48* (2007), 052106 (21 pages).

[7] B. C. Berndt and R. J. Evans: The determination of Gauss sums. Bull. Am. Math. Soc. *5* (1981), 107–130.

[8] P. O. Boykin, M. Sitharam, P. H. Tiep and P. Wocjan: Mutually unbiased bases and orthogonal decompositions of Lie algebras. Quantum Inf. Comput. *7* (2007), 371–382.

[9] S. Brierley and S. Weigert: Constructing mutually unbiased bases in dimension six. Phys. Rev. A *79* (2009), 052316 (13 pages).

[10] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel: Z4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. Proc. London Math. Soc. *75* (1997), 436–480.

[11] M. Daoud and M. R. Kibler: Phase operators, temporally stable phase states, mutually unbiased bases and exactly solvable quantum systems. J. Phys. A: Math. Theor. *43* (2010), 115303 (18 pages).

[12] P. Delsarte, J. M. Goethals, and J. J. Seidel: Bounds for systems of lines and Jacobi polynomials. Philips Res. Repts. *30* (1975), 91–105.

[13] P. Diţă: Some results on the parametrization of complex Hadamard matrices. J. Phys. A: Math. Gen. *37* (2004), 5355–5374.

[14] D. Gottesman, A. Kitaev, and J. Preskill: Encoding a qubit in an oscillator. Phys. Rev. A *64* (2001), 012310 (21 pages).

[15] M. Grassl: Tomography of quantum states in small dimensions. Elec. Notes Discrete Math. *20* (2005), 151–164.

[16] I. D. Ivanović: Geometrical description of quantum state determination. J. Phys. A: Math. Gen. *14* (1981), 3241–3245.

[17] M. R. Kibler: Angular momentum and mutually unbiased bases. Int. J. Mod. Phys. B *20* (2006), 1792–1801.

[18] M. R. Kibler: Variations on a theme of Heisenberg, Pauli and Weyl. J. Phys. A: Math. Theor. *41* (2008), 375302 (19 pages).

[19] M. R. Kibler: 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. *42* (2009), 353001 (28 pages).

[20] M. R. Kibler and M. Planat: A SU(2) recipe for mutually unbiased bases. Int. J. Mod. Phys. B *20* (2006), 1802–1807.

[21] J. Lawrence, Č. Brukner, and A. Zeilinger: Mutually unbiased binary observable sets on N qubits. Phys. Rev. A *65* (2002), 032320 (5 pages).

[22] J. Patera and H. Zassenhaus: The Pauli matrices in n dimensions and finest gradings of simple Lie algebras of type A_{n-1}. J. Math. Phys. *29* (1988), 665–673.

[23] A. O. Pittenger and M. H. Rubin: Wigner functions and separability for finite systems. J. Phys. A: Math. Gen. *38* (2005), 6005–6036.

[24] P. Šťovíček and J. Tolar: Quantum mechanics in a discrete space-time. Rep. Math. Phys. *20* (1984), 157–170.

[25] P. Šulc and J. Tolar: Group theoretical construction of mutually unbiased bases in Hilbert spaces of prime dimensions. J. Phys. A: Math. Gen. *40* (2007), 15099 (13 pages).

[26] W. Tadej and K. Życzkowski: A concise guide to complex Hadamard matrices. Open Sys. Info. Dynamics *13* (2006), 133–177.

[27] P. Wocjan and T. Beth: New construction of mutually unbiased bases in square dimensions. Quantum Inf. Comput. *5* (2005), 93–101.

[28] W. K. Wootters and B. D. Fields: Optimal state-determination by mutually unbiased measurements. Ann. Phys. (N.Y.) *191* (1989), 363–381.

Maurice R. Kibler, Université de Lyon, 37 rue du repos, 69361 Lyon, Université Claude Bernard, 43 Bd du 11 Novembre 1918, F-69622 Villeurbanne, and CNRS/IN2P3, Institut de Physique Nucléaire, 4 rue Enrico Fermi, F-69622 Villeurbanne. France.
e-mail: kibler@ipnl.in2p3.fr