About mutually unbiased bases in even and odd prime power dimensions

2005 J. Phys. A: Math. Gen. 38 5267

(http://iopscience.iop.org/0305-4470/38/23/013)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **38** (2005) 5267–5283 doi:10.1088/0305-4470/38/23/013

About mutually unbiased bases in even and odd prime power dimensions

Thomas Durt

TENA-TONA Free University of Brussels, Pleinlaan 2, B-1050 Brussels, Belgium

E-mail: thomdurt@vub.ac.be

Received 26 November 2004, in final form 30 March 2005
Published 25 May 2005
Online at stacks.iop.org/JPhysA/38/5267

Abstract

Mutually unbiased bases generalize the X, Y and Z qubit bases. They possess numerous applications in quantum information science. It is well known that in prime power dimensions $N = p^m$ (with p prime and m a positive integer), there exists a maximal set of $N + 1$ mutually unbiased bases. In the present paper, we derive an explicit expression for those bases, in terms of the (operations of the) associated finite field (Galois division ring) of N elements. This expression is shown to be equivalent to the expressions previously obtained by Ivanovic (1981 *J. Phys. A: Math. Gen.* **14** 3241) in odd prime dimensions, and Wootters and Fields (1989 *Ann. Phys.* **191** 363) in odd prime power dimensions. In even prime power dimensions, we derive a new explicit expression for the mutually unbiased bases. The new ingredients of our approach are, basically, the following: we provide a simple expression of the generalized Pauli group in terms of the additive characters of the field, and we derive an exact groupal composition law between the elements of the commuting subsets of the generalized Pauli group, renormalized by a well-chosen phase-factor.

PACS numbers: 03.65.−w, 03.67.−a, 89.70.+c

Introduction

A collection of orthonormal bases of a N-dimensional Hilbert space is said to be mutually unbiased if whenever we choose two states from different bases, the modulus squared of their in-product is equal to $1/N$. It is well known that, when the dimension of the Hilbert space is a prime power, there exists a set of $N + 1$ mutually unbiased bases. This set is maximal because it is not possible to find more than $N + 1$ mutually unbiased bases in a N-dimensional Hilbert space [1–3]. It is also a complete set because when we know all the probabilities of transition of an unknown quantum state towards the states of the bases of this set, we can

reconstruct all the coefficients of the density matrix that characterizes this state. In other words, we can perform full tomography or complete quantum state determination [1, 2, 4, 5]. A crucial element of the construction is the existence of a finite commutative division ring (or field[1]) of N elements. As is well known, finite fields with N elements exist if and only if the dimension N is a power of a prime, and a derivation of a set of mutually unbiased bases is already known in such cases. It is worth noting that nobody has managed until now to generalize this construction in the absence of a finite field so that it is still an open question whether such sets exist when the dimension is not a prime power [6, 7]. In the present paper, we obtain, in a synthetic formulation, the expressions for the mutually unbiased bases that were derived in the past. In odd prime power dimensions, we recover by a slightly different approach the expressions already obtained in the past by Ivanovic [1]. In odd prime power dimension, we derive an expression that we show to be equivalent, up to a relabelling, to that derived by Wootters and Fields [2]. We provide a synthetic expression that is also valid in even prime power dimensions (2^m). The (discrete) Heisenberg–Weyl group [3, 4, 8] (sometimes also called the generalized Pauli group), a finite group of unitary transformations, plays a central role in our approach.

1. Preliminary concepts

In what follows, we shall systematically assume that we work in a Hilbert space of prime power dimension $N = p^m$ with p a prime number and m a positive integer. Then, as is well known, it is possible to find a finite field with N elements. We shall label these elements by an integer number i, $0 \leqslant i \leqslant N-1$), or, equivalently, by a m-uple of integer numbers $(i_0, i_1, \ldots, i_{m-1})$ running from 0 to $p-1$ that we get from the p-ary expansion of i: $i = \sum_{n=0}^{m-1} i_n p^n$. This field is characterized by two operations, a multiplication and an addition, that we shall denote by $\odot_G$ and $\oplus_G$ respectively. It is always possible to label the elements of the field in such a way that the addition is equivalent to the addition modulo p componentwise. As all the fields are equivalent, up to a relabelling, there is no strict obligation to do so, but it is more natural and convenient. The fact that the addition factorizes in this way is a direct consequence of the fact that for all the finite fields the characteristics of the field, which is the smallest number of times that we must add the element 1 (neutral for the multiplication) with itself before we obtain 0 (neutral for the addition), is always equal to a prime number (p when $N = p^m$). The index G refers to Evariste Galois and is introduced in order not to confuse these operations with the usual (complex) multiplication and addition for which no index is written.

Let us denote γ_G the pth root of unity: $\gamma_G \mathrm{e}^{\mathrm{i}2\pi/p}$. Exponentiating γ_G with elements g of the field (with the usual rules for exponentiation), we obtain complex phasors of the type γ_G^g ($0 \leqslant g \leqslant N$). Such phasors can take p different values. They can be considered as a p-uple generalization of the (binary) parity operation $\mathrm{e}^{\mathrm{i}(2\pi/2)g}$ that corresponds to the m-qubits case. Indeed, the phasor γ_G^g ($0 \leqslant g \leqslant N$) only depends on the value of the first component g_0 of the p-ary expansion of g which is nothing else than the remainder of g after division by p, when the division by p is taken in the usual sense.

In virtue of the fact that the addition is the addition modulo p, componentwise, we get

$$\gamma_G^i \cdot \gamma_G^j = \gamma_G^{(i \oplus_G j)}. \tag{1}$$

Indeed, $\gamma_G^i \cdot \gamma_G^j = \gamma_G^{(i+j)} = \gamma_G^{(i_0+j_0)} = \gamma_G^{(i \oplus_G j)_0} = \gamma_G^{(i \oplus_G j)}$ (in the previous expression, we represented by the symbol x_0 the remainder of x after division by p, with x an element of the

[1] A field is a set with a multiplication and an addition operation which satisfy the usual rules, associativity and commutativity of both operations, the distributive law, existence of an additive identity 0 and a multiplicative identity 1, additive inverses, and multiplicative inverses for every element, 0 excepted.

Table 1. The field multiplication in dimension 4.

$\odot_G$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Table 2. The field addition in dimension 4.

$\oplus_G$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Table 3. The multiplication modulo 4.

$\cdot$ mod 4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Table 4. The addition modulo 4.

+mod 4	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

field comprised between 0 and $p^m - 1 = N - 1$). This relation is well-known and expresses, in the language of mathematicians, that pth roots of unity are additive characters of the Galois field [34].

The following identity also appears to play a fundamental role in our approach:

$$\sum_{j=0}^{N-1} \gamma_G^{(j \odot_G i)} = N \delta_{i,0}. \tag{2}$$

Indeed, if $i = 0$, then $\sum_{j=0}^{N-1} \gamma_G^{(j \odot_G i)} = N \cdot 1 = N$. Otherwise, $\sum_{j=0}^{N-1} \gamma_G^{(j \odot_G i)} = \sum_{j'=0}^{N-1} \gamma_G^{j'}$ in virtue of the inversibility of the multiplication. Now the exponentiation of gamma by elements of the field does only depend on the remainder after division by p, so that $\sum_{j'=0}^{N-1} \gamma_G^{j'} = p^{m-1} \sum_{j'=0}^{p-1} \gamma_G^{j'} = p^{m-1} \frac{(1-\gamma_G^p)}{(1-\gamma_G)} = 0$.

It is important to note, in order to avoid confusion, that different types of operations are present at this level. The internal field operations are labelled by the lower index G. They must not be confused with the modulo N operations. In order to emphasize the difference between these operations, we give the corresponding tables in the case of $N = 4 = 2^2$. One can check that the field and modulo 4 multiplications are distributive relative to their respective additions, but that there are no dividers of 0, 0 excepted, only in the case of the field multiplication. As a consequence, the field multiplication table, amputated from the first line and column,

exhibits an invertible (group) structure. All operations are commutative as can be seen from the symmetry of tables 1 to 4 under transposition. When N is an arbitrary integer power, it is easy to derive the addition table of the corresponding field because it reduces to the addition componentwise:

$$i \oplus_G j = \sum_{n=0}^{m-1} i_n p^n \oplus_G \sum_{n=0}^{m-1} j_n p^n = \sum_{n=0}^{m-1} (i_n +_{\mathrm{mod}\, p} j_n) p^n$$

For instance, if we express quartits as products of two qubits: $|0\rangle_4 = |0\rangle_2 \otimes |0\rangle_2$, $|1\rangle_4 = |0\rangle_2 \otimes |1\rangle_2$, $|2\rangle_4 = |1\rangle_2 \otimes |0\rangle_2$, $|3\rangle_4 = |1\rangle_2 \otimes |1\rangle_2$. It is then easy to check from table 2 that if $|i\rangle_4 = |i_1\rangle_2 \otimes |i_2\rangle_2$, and $|j\rangle_4 = |j_1\rangle_2 \otimes |j_2\rangle_2$, then $|i \oplus_G j\rangle_4 = |i_1 \oplus_{\mathrm{mod}\,2} j_1\rangle_2 \otimes |i_2 \oplus_{\mathrm{mod}\,2} j_2\rangle_2$. This is nothing else than the addition modulo p (= 2 here) componentwise. It is worth noting that it is not straightforward in general to derive the field multiplication table but this can be done. The construction of such tables is based on the properties of irreducible polynomials that we shall not describe in the present paper (see for instance appendix D in [13] and references therein). All we need to know is that such tables exist.

In prime dimensions however a simplification occurs, and the Galois and modulo N operations coincide. In prime power but non-prime dimensions, this is no longer true. It is also worth noting that the property $\sum_{p=0}^{N-1} \gamma^{(p \odot q)} = N\delta_{q,0}$ is true for the modulo N multiplication as well, in arbitrary dimension, but γ must be taken to be equal to the Nth root of unity in this case. Because of this, certain identities and properties related to the Heisenberg–Weyl group can be generalized in arbitrary dimensions provided the factor γ is chosen accordingly.

2. Construction of the dual basis

Let us now consider the unitary transformations V_l^0 that shift each label of the states of the computational basis ($\{|0\rangle, |1\rangle, \ldots, |i\rangle, \ldots, |N-1\rangle\}$) by a distance l ($|i\rangle \rightarrow |i \oplus_G l\rangle$) (the reason for our choice of notation will be made obvious soon). The transformations V_l^0 form a commutative group with N elements that is isomorphic to the Galois addition. Generalizing the procedure outlined in [9], we define the dual basis as follows,

$$|\tilde{j}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \gamma_G^{\ominus_G (k \odot_G j)} |k\rangle, \tag{3}$$

where the symbol $\ominus_G$ represents the inverse of the Galois addition $\oplus_G$. It is easy to check that the dual states are invariant, up to a global phase, under the transformations V_l^0. Indeed, we have

$$V_l^0 \cdot |\tilde{j}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \gamma_G^{\ominus_G (k \odot_G j)} |k \oplus_G l\rangle \tag{4}$$

$$= \frac{1}{\sqrt{N}} \sum_{k'=0}^{N-1} \gamma_G^{(\ominus_G (k' \ominus_G l) \odot_G j)} |k'\rangle = \gamma_G^{(l \odot_G j)} |\tilde{j}\rangle. \tag{5}$$

Obviously, the dual basis and the computational basis are mutually unbiased. When the dimension is prime ($N = p$), the dual basis is the discrete Fourier transform of the computational basis, when it is a power of 2, it is a Hadamard transform [9].

Let us denote V_0^l the unitary transformations that shift each label of the states of the dual basis ($\{|\tilde{0}\rangle, |\tilde{1}\rangle, \ldots, |\tilde{i}\rangle, \ldots, |\tilde{N-1}\rangle\}$) by a distance $\ominus_G l$ ($|\tilde{i}\rangle \rightarrow |\tilde{i} \ominus_G \tilde{l}\rangle$). The

transformations V_0^l form a commutative group with N elements that is isomorphic to the Galois addition. These operators are diagonal in the computational basis,

$$V_0^l = \sum_{k=0}^{N-1} |\tilde{k} \ominus_G \tilde{l}\rangle\langle\tilde{k}| = \sum_{k=0}^{N-1} \gamma_G^{(k\odot_G l)} |k\rangle\langle k|. \tag{6}$$

This is the dual counterpart of a similar expression for the shifts in the computational basis,

$$V_l^0 = \sum_{k=0}^{N-1} |k \oplus_G l\rangle\langle k| = \sum_{k=0}^{N-1} \gamma_G^{(k\odot_G l)} |\tilde{k}\rangle\langle\tilde{k}|. \tag{7}$$

3. Construction of the remaining $N-1$ mutually unbiased bases

In the previous section, we derived a set of two bases, the computational basis and the dual basis, that are mutually unbiased. In this section, we shall generalize this derivation in order to obtain $N-1$ other mutually unbiased bases (between each other, and also relatively to the computational and dual bases).

Let us denote V_i^j the compositions of the shifts in the computational and the dual basis, $V_i^j = V_0^j \cdot V_i^0$.

$$\begin{aligned} V_i^j = V_0^j \cdot V_i^0 &= \sum_{l=0}^{N-l} \gamma^{l\odot_G j} |l\rangle\langle l| \sum_{k=0}^{N-l} |k \oplus_G i\rangle\langle k| \\ &= \sum_{k=0}^{N-1} \gamma_G^{((k\oplus_G i)\odot_G j)} |k \oplus_G i\rangle\langle k|, \qquad i, j: 0, \ldots, N-1 \end{aligned} \tag{8}$$

Here, the product $\cdot$ expresses the matricial product (the usual composition law of two unitary transformations). Although this expression appeared, to our knowledge, in [20] for the first time, we show in the final section that the set of operators so-defined coincides with the generalized Pauli group studied in [3].

It is worth noting that most often V_0^j and V_i^0 do not commute.

$$V_i^j = V_0^j \cdot V_i^0 = \sum_{k=0}^{N-l} \gamma^{((k\oplus_G i)\odot_G j)} |k \oplus_G i\rangle\langle k| \tag{9}$$

$$\begin{aligned} V_i^0 \cdot V_0^j &= \sum_{k=0}^{N-l} |k \oplus_G i\rangle\langle k| \sum_{l=0}^{N-l} \gamma^{l\odot_G j} |l\rangle\langle l| \\ &= \sum_{k=0}^{N-l} \gamma^{(k\odot_G j)} |k \oplus_G i\rangle\langle k| \\ &= \gamma^{\ominus_G (i\odot_G j)} V_0^j \cdot V_i^0 = \gamma^{\ominus_G (i\odot_G j)} V_i^j. \end{aligned} \tag{10}$$

The commutator is thus given by the following expression:

$$V_0^j \cdot V_i^0 - V_i^0 \cdot V_0^j = \left(1 - \gamma^{\ominus_G (i\odot_G j)}\right) V_0^j \cdot V_i^0. \tag{11}$$

We recognize here a commutation rule that is known as the Weyl commutation rule, and was already studied a long time ago [8]. This is not astonishing because the set of unitary transformations V_i^j that we consider here is a discrete version of the so-called Heisenberg–Weyl group (compositions of translations in position and in impulsion). In dimension 2, it coincides with the Pauli group. When the dimension is a prime number, the field operations

are the addition and multiplication modulo p, and the properties of mutually unbiased bases are already well known in that case [1], as well as their relation with the 'Heisenberg–Weyl–Pauli' group [10]. In the present approach, we consider, instead of the usual (modulo N) operations, the Galois addition and multiplication, also for non-prime but prime power dimensions. The connection with previous works related to the Pauli group approach [2, 3, 11–13] is established in the final section.

By a straightforward computation, we can now derive the law of composition of these N^2 unitary transformations,

$$\begin{aligned} V_i^j \cdot V_l^k &= V_0^j \cdot V_i^0 \cdot V_0^k \cdot V_l^0 \\ &= \gamma^{\ominus_G(i \odot_G k)} V_0^j \cdot V_0^k \cdot V_i^0 \cdot V_l^0 \\ &= \gamma^{\ominus_G(i \odot_G k)} V_{i \oplus_G l}^{j \oplus_G k}. \end{aligned} \tag{12}$$

Up to a global phase, this looks like a groupal composition law. We shall now show that (up to phases) the N^2 unitary transformations V_i^j form $N+1$ commuting subgroups of N elements that have only the identity in common. Moreover, each of these subgroups admits a diagonal representation in a basis that is mutually unbiased relatively to the N bases in which the other subgroups are diagonal. Actually, the last property can be shown, following an alternative approach developed in [3] to be a consequence of the fact that the V operators, up to phases, form what is called a maximally commuting basis of orthogonal unitary matrices (see also the final section). The new ingredients in our approach are (1) expression (8) for the generalized Pauli operators, and (2) the recognition of the fact that the operators of the commuting subgroups exhibit exact groupal composition laws, provided they are multiplied by a convenient phase factor.

In order to derive all these results, we shall take them for granted a first time, and check afterwards that our hypothesis was correct. It is convenient to introduce new notation and definitions before we proceed. We shall denote U_l^i the elements of these subgroups, where i labels the subgroup and runs from 0 to N (there are $N+1$ of them), while l labels the elements of the subgroup and runs from 0 to $N-1$ (each subgroup contains N elements). We know already the two first subgroups, that admit a diagonal representation in the computational and dual bases. The first one ($i=0$) contains the elements $V_0^l(l\colon 0,\ldots,N-1)$, so by definition $U_l^0 = V_0^l(l\colon 0,\ldots,N-1)$. The second one contains the elements $U_l^1 = V_l^0(l\colon 0,\ldots,N-1)$.

In virtue of equalities (6) and (7), we can also write $U_l^0 = \sum_{k=0}^{N-1} \gamma_G^{(k \odot_G l)} |k\rangle\langle k|$ and $U_l^1 = \sum_{k=0}^{N-1} \gamma_G^{(k \odot_G l)} |\tilde{k}\rangle\langle\tilde{k}|$. A similar expression can be found for each of the $N-1$ remaining subgroups as we shall now show. It is convenient at this level to parametrize the basis states that diagonalize these subgroups as follows: the kth basis state that diagonalizes the ith subgroup will be denoted as $|e_k^i\rangle$. Our ultimate goal is to prove that there exist $N+1$ bases $|e_k^i\rangle$ and N^2 operators U_l^i that are in one-to-one correspondence with the V operators and differ from them by an appropriate phase factor, such that the following constraints are fulfilled:

$$U_l^i = \sum_{k=0}^{N-1} \gamma_G^{(k \odot_G l)} |e_k^i\rangle\langle e_k^i| (l\colon 0,\ldots,N-1; i\colon 0,\ldots,N) \tag{13}$$

$$\langle e_i^k | e_j^l \rangle \cdot \langle e_j^l | e_i^k \rangle = \delta_{k,l}\delta_{i,j} + (1/N).(1-\delta_{k,l}),\ (k,l\colon 0,\ldots,N, i, j\colon 0,\ldots,N-1). \tag{14}$$

In virtue of the commutativity of the Galois multiplication, of identity (1) and of definition (13), the U operations that are labelled by the same value i form a commutative subgroup and obey the (exact) group composition law $U_l^i \cdot U_{l'}^i = U_{l \oplus_G l'}^i$. We can guess that they correspond to families of operators V_l^k such that the (Galois) ratio $k/_G l$ is constant, because when $k' \odot_G l = k \odot_G l'$, then V_l^k and $V_{l'}^{k'}$ commute in virtue of the Weyl commutation rule (11). It is thus natural to try

the identification $U_l^i = V_l^{(i-1)\odot_G l}$, up to a phase, when i differs from 0 and $U_l^0 = V_0^l$ which is consistent with our previous conventions. There are in general several ways to fix the phases but in any case certain constraints must be satisfied:

- the phase $U_l^i \big/ V_l^{(i-1)\odot_G l}$ is equal to 0 when $l = 0$, because $V_0^0 = 1$, and the identity is present in all subgroups;
- as we mentioned already, the U operators must obey the composition law $U^i_{l\oplus_G l'} = U^i_l U^i_{l'}$, but the composition law $V_i^j \cdot V_l^k = \gamma^{\ominus_G(i\odot_G k)} V^{j\oplus_G k}_{i\oplus_G l}$ must be guaranteed at the same time, which restricts seriously the arbitrariness in the choice of the phase.

Let us now assume that the phase ratio between U_l^i and $V_l^{(i-1)\odot_G l}$ is fixed for all powers of p between 0 and $m-1$ ($l = p^n, 0 \leqslant n \leqslant m-1$).

We shall first treat the odd-dimensional case. Then, iterating l times the composition law (12) (with $2 \leqslant l \leqslant m-1$), we obtain the following constraints on the ratio between $U^i_{p^n\odot_G l}$ and $V^{(i-1)\odot_G p^n\odot_G l}_{p^n\odot_G l}$, $0 \leqslant l \leqslant m-1, 0 \leqslant n \leqslant m-1$:

$$\begin{aligned}\big(U^i_{p^n\odot_G l}\big) &= \sum_{k=0}^{N-1} \gamma_G^{p^n\odot_G k\odot_G l} \big|e^i_k\big\rangle\big\langle e^i_k\big| = \big(U^i_{p^n}\big)^l \\ &= \big(U^i_{p^n}\big/V^{(i-1)\odot_G p^n}_{p^n}\big)^l \cdot \big(V^{((i-1)\odot_G p^n)}_{p^n}\big)^l \\ &= \big(U^i_{p^n}\big/V^{(i-1)\odot_G p^n}_{p^n}\big)^l \cdot \gamma_G^{\ominus_G(i-1)\odot_G l\odot_G(l\ominus_G 1)\odot_G p^n\odot_G p^n/_G 2} \cdot V^{((i-1)\odot_G p^n\odot_G l)}_{p^n\odot_G l}. \end{aligned} \tag{15}$$

Here, the symbols / and $/_G$ indicate the multiplication by the multiplicative inverse for the usual (complex) and field multiplications respectively. In order to fix the phase $\big(U^{(i\odot_G p^n)}_{p^n}\big/V^{(i-1)\odot_G p^n}_{p^n}\big)$ we can make use of the fact that the characteristic of the field is p (so to say $1\oplus_G 1\oplus_G\cdots\oplus_G 1$ (p times) = 0), which implies that $\big(U^i_{p^n}\big)^p = 1$, so that

$$\big(U^i_{p^n}\big/V^{(i-1)\odot_G p^n}_{p^n}\big)^p = \gamma_G^{(i-1)\odot_G p\odot_G(p\ominus_G 1)\odot_G p^n\odot_G p^n/_G 2} = 1. \tag{16}$$

The phase $\big(U^i_1\big/V^{(i-1)\odot_G p^n}_{p^n}\big)$ is thus determined up to an integer power of $\gamma_G = \mathrm{e}^{\mathrm{i}2\pi/p}$. This is true for each integer value of n between 0 and $m-1$ so that there are $p^m = N$ different possible ways to 'fix' the phases. Let us denote γ_n the pth root of unity that we choose to be equal to $U^i_{p^n}\big/V^{(i-1)\odot_G p^n}_{p^n}$. Once this value is chosen, all the other phases are determined, according to the following development,

$$\begin{aligned} U^i_l &= \prod_{n=0}^{m-1} U^i_{l_n\odot_G p^n} = \prod_{n=0}^{m-1}\big(U^i_{p^n}\big)^{l_n} \\ &= \prod_{n=0}^{m-1} \gamma_G^{\ominus_G(i-1)\odot_G l_n\odot_G(l_n\ominus_G 1)\odot_G p^n\odot_G p^n/_G 2} (\gamma_n)^{l_n} V^{((i-1)\odot_G p^n\odot_G l_n)}_{p^n\odot_G l_n}, \end{aligned} \tag{17}$$

where the coefficients l_n are unambiguously defined by the p-ary expansion of $l, l = \sum_{n=0}^{m-1} l_n p^n$. Moreover, we can check by direct computation that the U operators so-defined obey an exact groupal composition law, independently of the choice that we could decide to perform, among the $p^m = N$ different possible ways to 'fix' the phases γ_n,

$$\begin{aligned} U^i_{l_1}\cdot U^i_{l_2} &= \prod_{n=0}^{m-1} U^i_{l_{1n}\odot_G p^n}\cdot U^i_{l_{2n}\odot_G p^n} \\ &= \prod_{n=0}^{m-1} \gamma_G^{\ominus_G(i-1)\odot_G l_{1n}\odot_G(l_{1n}\ominus_G 1)\odot_G p^n\odot_G p^n/_G 2} \gamma_G^{\ominus_G(i-1)\odot_G l_{2n}\odot_G(l_{2n}\ominus_G 1)\odot_G p^n\odot_G p^n/_G 2} \\ &(\gamma_n)^{l_{1n}}(\gamma_n)^{l_{2n}} V^{((i-1)\odot_G p^n\odot_G l_{1n})}_{p^n\odot_G l_{1n}} V^{((i-1)\odot_G p^n\odot_G l_{2n})}_{p^n\odot_G l_{2n}} \\ &= \prod_{n=0}^{m-1} \gamma_G^{\ominus_G(i-1)\odot_G p^n\odot_G p^n\odot_G(l_{1n}\odot_G(l_{1n}\ominus_G 1)\oplus_G l_{2n}\odot_G(l_{2n}\ominus_G 1)\oplus_G 2\odot_G l_{1n}\odot_G l_{2n})/_G 2} \\ &(\gamma_n)^{l_{1n}+_{mod p} l_{2n}} V^{((i-1)\odot_G p^n\odot_G(l_{1n}+_{mod p} l_{2n}))}_{p^n\odot_G(l_{1n}+_{mod p} l_{2n})}. \end{aligned} \tag{18}$$

In the previous derivation we made use of decomposition (17), of the composition law and of the fact that the γ_n are nth roots of unity. Thanks to some arithmetic made possible by the field properties and making use again of decomposition (17) the other way round, we establish an exact composition law for the U operators.

$$U^i_{l_1}\cdot U^i_{l_2}=\prod_{n=0}^{m-1}\gamma_G^{\ominus_G(i-1)\odot_G p^n\odot_G p^n\odot_G((l_{1n}+_{\mathrm{mod}\,p}l_{2n})\odot_G((l_{1n}+_{\mathrm{mod}\,p}l_{2n})\ominus_G 1)/_G 2}$$

$$(\gamma_n)^{l_{1n}+_{\mathrm{mod}\,p}l_{2n}}V^{((i-1)\odot_G p^n\odot_G(l_{1n}+_{\mathrm{mod}p}l_{2n}))}_{p^n\odot_G(l_{1n}+_{\mathrm{mod}\,p}l_{2n})}=\prod_{n=0}^{m-1}\bigl(U^i_{p^n}\bigr)^{l_{1n}+_{\mathrm{mod}\,p}l_{2n}}$$

$$=\prod_{n=0}^{m-1}\bigl(U^i_{(l_{1n}+_{\mathrm{mod}p}l_{2n})\odot_G p^n}\bigr)=U^i_{l_1\oplus_G l_2}. \tag{19}$$

In even prime power dimensions, the treatment is similar, although we may not divide by 2 in this case. Combining the constraints

$$\bigl(V^{((j-1)\odot_G 2^n)}_{2^n}\bigr)^2=\bigl(\gamma_G^{\ominus_G(j-1)\odot_G 2^n\odot_G 2^n}V^0_0\bigr)=\gamma_G^{(j-1)\odot_G 2^n\odot_G 2^n}$$

and

$$U^j_{2^n}U^j_{2^n}=U^j_{2^n\oplus_G 2^n}=U^j_0=1,$$

we obtain a decomposition law for the U operators, which expresses their factorization in terms of qubit operators,

$$U^j_l=\prod_{n=0}^{m-1}U^j_{l_n\odot_G 2^n}=\prod_{n=0}^{m-1}\bigl(U^j_{2^n}\bigr)^{l_n}$$

$$=\prod_{n=0}^{m-1}\bigl(\gamma_G^{(j-1)\odot_G 2^n\odot_G 2^n}\bigr)^{\frac{l_n}{2}}V^{((j-1)\odot_G 2^n\odot_G l_n)}_{2^n\odot_G l_n}, \tag{20}$$

where the coefficients l_n are unambiguously defined by the binary expansion of $l, l=\sum_{k=0}^{m-1}l_n 2^n$; $l_n=0$ or $l_n=1$. Similarly to what happens in the odd-dimensional case, the phase factors $\bigl(\gamma_G^{(j-1)\odot_G 2^n\odot_G 2^n}\bigr)^{\frac{1}{2}}$ can be fixed with some arbitrariness, actually up to a sign in this case. Let us now check that the U operators so-defined obey an exact group composition law.

$$U^j_{l_1}\cdot U^j_{l_2}=\prod_{n=0}^{m-1}\bigl(\gamma_G^{(j-1)\odot_G 2^n\odot_G 2^n}\bigr)^{\frac{l_{1n}+l_{2n}}{2}}\bigl(V^{((j-1)\odot_G 2^n)}_{2^n}\bigr)^{l_{1n}+l_{2n}}$$

$$=\prod_{n=0}^{m-1}\bigl(\gamma_G^{(j-1)\odot_G 2^n\odot_G 2^n}\bigr)^{\frac{l_{1n}+_{\mathrm{mod}2}l_{2n}}{2}}\bigl(V^{((j-1)\odot_G 2^n)}_{2^n}\bigr)^{l_{1n}+_{\mathrm{mod}\,2}l_{2n}}=U^j_{l_1\oplus_G l_2}. \tag{21}$$

We made use of the fact that $\bigl(V^{((j-1)\odot_G 2^n)}_{2^n}\bigr)^2=\gamma_G^{(j-1)\odot_G 2^n\odot_G 2^n}$ and $\gamma_G=-1$.

Let us now derive an explicit expression for the N phases $U^j_1/V^{(j-1)\odot_G l}_l$. We shall treat separately even and odd prime power dimensions.

3.1. Odd prime power dimensions

In odd prime power dimensions, all possible consistent choices for determining the phases (there are $p^m=N$ such choices) can be expressed by the relation

$$U^i_l/V^{(i-1)\odot_G l}_l=\bigl(\gamma_G^{\ominus((i-1)\odot_G l\odot_G l)/_G 2}\bigr)\gamma_G^{k\odot l}, \tag{22}$$

where k is an arbitrary element of the field. Each choice for k (there are N of them) leads to another consistent determination of the phase ratio between the U and V operators. This is due to the fact that if $\gamma_G^{k\odot p^n}=\gamma_G^{k'\odot p^n}$, $\forall n\colon 0\leqslant n\leqslant m-1$, then $k=k'$ in virtue of identity (2).

It is worth noting that, when $k=0$, which is the simplest determination of the phases, we obtain the following relation:

$$U^i_l=\bigl(\gamma_G^{\ominus((i-1)\odot_G l\odot_G l)/_G 2}\bigr)V^{(i-1)\odot_G l}_l. \tag{23}$$

This corresponds to the choice of phases $\gamma_n = \gamma_G^{\ominus((i-1)\odot_G p^n \odot_G p^n)/_G 2}$. It is worth noting that relation (23) is also valid for $i = 1$, which corresponds to the dual basis derived in the previous section.

For $i = 0$, $U_l^0 = V_0^l$, in agreement with the previous definitions.

In order to check the consistency of expression (22), it is sufficient, making use of the composition law for the V operators (12), to check by direct computation that the U operators obey an exact (that is, not up to a phase) group composition law. It is worth remarking that if $\tilde{U}_l^i = \gamma_G^{k\odot l} U_l^i$, and that $U_l^i \cdot U_{l'}^i = U_{l\oplus_G l'}^i$, then $\tilde{U}_l^i . \tilde{U}_{l'}^i = \tilde{U}_{l\oplus_G l'}^i$. Therefore, it is sufficient to establish the groupal composition law when expression (23) is valid, in order to establish it when expression (22) is valid, for any value of k.

$$\begin{aligned} U_l^i \cdot U_{l'}^i &= \left(\gamma_G^{\ominus((i-1)\odot_G l \odot_G l)/_G 2}\right)\left(\gamma_G^{\ominus((i-1)\odot_G l' \odot_G l')/_G 2}\right) V_l^{(i-1)\odot_G l} V_{l'}^{(i-1)\odot_G l'} \\ &= \left(\gamma_G^{\ominus((i-1)\odot_G l \odot_G l)/_G 2}\right)\left(\gamma_G^{\ominus((i-1)\odot_G l' \odot_G l')/_G 2}\right)\left(\gamma^{(\ominus_G (i-1)\odot_G l \odot_G l')}\right) V_{(l\oplus_G l')}^{(i-1)\odot_G (l\oplus_G l')} \\ &= \left(\gamma_G^{\ominus((i-1)\odot_G (l\oplus_G l')\odot_G (l\oplus_G l'))/_G 2}\right) V_{(l\oplus_G l')}^{(i-1)\odot_G (l\oplus_G l')} \\ &= U_{l\oplus_G l'}^i, \qquad i: 1, \ldots, N, \qquad l, l': 0, \ldots, N-1. \end{aligned} \tag{24}$$

Now that we have at our disposal an exact expression for the operators U, we can also derive an explicit expression for the $N-1$ dual bases associated with the subgroups that correspond to the operators $U_l^i; i - 1 = 1, \ldots, N-1$. This can be realized thanks to the following identity, a direct consequence of equations (13) and (2),

$$\left|e_k^i\right\rangle\left\langle e_k^i\right| = \frac{1}{N} \sum_{l=0}^{N-1} \gamma^{\ominus_G k \odot_G l} U_l^i. \tag{25}$$

Obviously, if we choose another determination of the phases, that is, if we replace U_l^i by $\tilde{U}_l^i = \gamma_G^{k'\odot l} U_l^i$, we obtain the same basis states, with their labels shifted by k'. It is thus more convenient to choose in what follows the simplest phase determination (23).

By a straightforward but lengthy computation that we do not reproduce here, we obtain then the expression, in the computational basis, of the states of $N-1$ bases that correspond to the non-null values of the label $i - 1$.

$$\left|e_k^i\right\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \gamma_G^{\ominus_G q \odot_G k} \left(\gamma_G^{((i-1)\odot_G q \odot_G q)/_G 2}\right) \left|e_q^0\right\rangle. \tag{26}$$

Actually, the previous expression is also valid when $i = 1$, which corresponds to the dual basis $|\tilde{j}\rangle$ (3).

Let us now check by direct computation that the N bases ($N-1$ plus the dual basis) so obtained are orthonormal and mutually unbiased between each other (it is easy to check that the computational basis also fulfils these requirements). Before we do so, we shall rewrite the factors $\left(\gamma_G^{\ominus((i-1)\odot_G q \odot_G q)/_G 2}\right)$ as follows:

$$\left(\gamma_G^{\ominus((i-1)\odot_G l \odot_G l)/_G 2}\right) = U_1^i / V_l^{(i-1)\odot_G l} = \left(\gamma_G^{\ominus((i-1)\odot_G l \odot_G l)}\right)^{\frac{1}{2}}. \tag{27}$$

This redefinition is less precise than the previous one, because there exist two determinations of the square root of a complex number, nevertheless we adopt it, having in mind that in odd prime power dimensions, the previous expression fixes the sign of the square root of $\left(\gamma_G^{\ominus((i-1)\odot_G l \odot_G l)}\right)$ without ambiguity. We shall show in the following section that a similar expression is also valid in the even-dimensional case. Let us now prove that expression (14)

is valid.

$$\langle e_j^l|e_i^k\rangle = \frac{1}{N}\sum_{q=0}^{N-1}\gamma_G^{\ominus_G q\odot_G(i\ominus_G j)}\left(\gamma_G^{((k-1)\ominus_G(l-1))\odot_G q\odot_G q}\right)^{\frac{1}{2}} \tag{28}$$

$$\begin{aligned}
\langle e_j^l|e_i^k\rangle\cdot\langle e_i^k|e_j^l\rangle\cdot &= \frac{1}{N^2}\left(\sum_{q=0}^{N-1}\gamma_G^{\ominus_G q\odot_G(i\ominus_G j)}\left(\gamma_G^{((k-1)\ominus_G(l-1))\odot_G q\odot_G q}\right)^{\frac{1}{2}}\right)\\
&\times\left(\sum_{q'=0}^{N-1}\gamma_G^{\ominus_G q'\odot_G(j\ominus_G i)}\left(\gamma_G^{((l-1)\ominus_G(k-1))\odot_G q'\odot_G q'}\right)^{\frac{1}{2}}\right)\\
&= \frac{1}{N^2}\left(\sum_{q=0}^{N-1}\gamma_G^{\ominus_G q\odot_G(i\ominus_G j)}\left(\gamma_G^{((k-1)\ominus_G(l-1))\odot_G q\odot_G q}\right)^{\frac{1}{2}}\right)\\
&\times\left(\sum_{t=0}^{N-1}\gamma_G^{\ominus_G(q\oplus_G t)\odot_G(j\ominus_G i)}\left(\gamma_G^{((l-1)\ominus_G(k-1))\odot_G(q\oplus_G t)\odot_G(q\oplus_G t)}\right)^{\frac{1}{2}}\right)\\
&= \frac{1}{N^2}\left(\sum_{q,t=0}^{N-1}\gamma_G^{t\odot_G(j\ominus_G i)}\left(\gamma_G^{2((l-1)\ominus_G(k-1))\odot_G q\odot_G t}\right)^{\frac{1}{2}}\cdot\left(\gamma_G^{((l-1)\ominus_G(k-1))\odot_G t\odot_G t}\right)^{\frac{1}{2}}\right)\\
&= \frac{1}{N^2}\left(\sum_{q,t=0}^{N-1}\gamma_G^{((t\odot_G(j\ominus_G i)\oplus_G((l-1)\ominus_G(k-1))\odot_G q\odot_G t)}\cdot\left(\gamma_G^{((l-1)\ominus_G(k-1))\odot_G t\odot_G t}\right)^{\frac{1}{2}}\right)\\
&= \frac{1}{N^2}\left(\sum_{t=0}^{N-1}\left(\sum_{q=0}^{N-1}\gamma_G^{(((l-1)\ominus_G(k-1))\odot_G t\odot_G q)}\right)\cdot\gamma_G^{(t\odot_G(j\ominus_G i))}\cdot\left(\gamma_G^{((l-1)\ominus_G(k-1))\odot_G t\odot_G t}\right)^{\frac{1}{2}}\right)\\
&= \frac{1}{N}\sum_{t=0}^{N-1}\delta_{((l-1)\ominus_G(k-1))\odot_G t,0)}\cdot\gamma_G^{(t\odot_G(j\ominus_G i))}\cdot\left(\gamma_G^{((l-1)\ominus_G(k-1))\odot_G t\odot_G t}\right)^{\frac{1}{2}}
\end{aligned} \tag{29}$$

The previous derivation is a bit lengthy but is a direct consequence of the identities 1 and 2, and of an appropriate renaming of the dummy indices. Now, there is no divider of 0 except 0 itself (the multiplication $\odot_G$ forms a division ring or field) so that $\delta_{a\odot_G b,0} = \delta_{a,0} + (1-\delta_{a,0})\cdot\delta_{b,0}$ and thus

$$\begin{aligned}
\left\|\langle e_j^l|e_i^k\rangle\right\|^2 &= \delta_{(l-1)\ominus_G(k-1),0}\delta_{i,j} + \left(1-\delta_{(l-1)\ominus_G(k-1),0}\right)\\
&\times\frac{1}{N}\sum_{t=0}^{N-1}\delta_{t,0}\cdot\gamma_G^{(t\odot_G(j\ominus_G i))}\cdot\left(\gamma_G^{((l-1)\ominus_G(k-1))\odot_G t\odot_G t}\right)^{\frac{1}{2}}\\
&= \delta_{k,l}\delta_{i,j} + (1/N)\cdot(1-\delta_{k,l}).
\end{aligned} \tag{30}$$

Finally, let us control the validity of the postulated expression (13),

$$\begin{aligned}
\sum_{k=0}^{N-1}\gamma_G^{(k\odot_G l)}|e_k^i\rangle\langle e_k^i| &= \sum_{k=0}^{N-1}\gamma_G^{(l\odot_G k)}\frac{1}{N}\sum_{q=0}^{N-1}\gamma_G^{\ominus_G q\odot_G k}\left(\gamma_G^{((i-1)\odot_G q\odot_G q)}\right)^{\frac{1}{2}}|e_q^0\rangle\\
&\times\sum_{q'=0}^{N-1}\gamma_G^{\oplus_G q'\odot_G k}\left(\gamma_G^{(\ominus(i-1)\odot_G q'\odot_G q')}\right)^{\frac{1}{2}}\langle e_{q'}^0|\\
&= \frac{N}{N}\sum_{q,q'=0}^{N-1}\delta_{q,q'\oplus_G l}\left(\gamma_G^{((i-1)\odot_G q\odot_G q\ominus(i-1)\odot_G q'\odot_G q')}\right)^{\frac{1}{2}}|e_q^0\rangle\langle e_{q'}^0|
\end{aligned}$$

$$= \sum_{q'=0}^{N-1} \left(\gamma_G^{((i-1)\odot_G(q'\oplus_G l)\odot_G(q'\oplus_G l)\ominus(i-1)\odot_G q'\odot_G q')}\right)^{\frac{1}{2}} \left|e^0_{q'\oplus_G l}\right\rangle\left\langle e^0_{q'}\right|$$

$$= \left(\gamma_G^{((i-1)\odot_G l\odot_G l)}\right)^{\frac{1}{2}} \sum_{q'=0}^{N-1} \gamma_G^{(((i-1)\odot_G l)\odot_G q')} \left|e^0_{q'\oplus_G l}\right\rangle\left\langle e^0_{q'}\right|$$

$$= U_l^i (l\colon 0, \ldots, N-1, \quad i\colon 1, \ldots, N). \tag{31}$$

Here again,most of the equalities are derived from identities (1) and (2). The last equality is a consequence of equations (8) and (23).

3.2. Even prime power dimensions

In this case the explicit expressions for the mutually unbiased bases are less easy to manipulate. Once again, there are p^m (2^m in this case) possible ways to determine the phases $U_1^j \big/ V_l^{(j-1)\odot_G l}$, but they are equivalent, up to a relabelling of the basis states.

In the next development, we shall implicitly choose a certain determination of the square root of $\gamma_G^{(j-1)\odot_G 2^n \odot_G 2^n}$ that is equal to $\mathrm{i}^{(j-1)\odot_G 2^n\odot_G 2^n}$.

$$U_l^j = \prod_{n=0}^{m-1} U^j_{l_n\odot_G 2^n} = \prod_{n=0}^{m-1} \left(U^j_{2^n}\right)^{l_n} = \prod_{n=0,l_n\neq 0}^{m-1} \left(\gamma_G^{(j-1)\odot_G 2^n\odot_G 2^n}\right)^{\frac{1}{2}} \left(V_{2^n}^{((j-1)\odot_G 2^n)}\right)^{l_n}$$

$$= \prod_{n=0,l_n\neq 0}^{m-1} \mathrm{i}^{(j-1)\odot_G 2^n\odot_G 2^n} \left(V_{2^n}^{((j-1)\odot_G 2^n)}\right)$$

$$= \left(\prod_{n=0,l_n\neq 0}^{m-1} \mathrm{i}^{(j-1)\odot_G 2^n\odot_G 2^n} \gamma_G^{(j-1)\odot_G 2^n\odot_G 2^{n'}}\right) V_l^{((j-1)\odot_G l)} \tag{32}$$

where the coefficients l_n are unambiguously defined by the p-ary (here binary) expansion of l, $l = \sum_{k=0}^{m-1} l_n 2^n$, while n' is the smallest integer strictly larger than n such that $l_{n'} \neq 0$, if it exists, 0 otherwise.

This result is a generalization of identity (23), because in both cases the phases are square roots of integer powers of gamma,

$$\left(U_1^j \big/ V_l^{(j-1)\odot_G l}\right)^2 = \gamma_G^{\ominus((j-1)\odot_G l\odot_G l)}.$$

Nevertheless, in the present case we obtain the following determination of the square root of $\left(\gamma_G^{\ominus((j-1)\odot_G l\odot_G l)}\right)$:

$$\left(\gamma_G^{\ominus((j-1)\odot_G l\odot_G l)}\right)^{\frac{1}{2}} = \left(\gamma_G^{\oplus((j-1)\odot_G l\odot_G l)}\right)^{\frac{1}{2}} = \prod_{n=0,l_n\neq 0}^{m-1} \mathrm{i}^{(j-1)\odot_G 2^n\odot_G 2^n} \gamma_G^{(j-1)\odot_G 2^n\odot_G 2^{n'}} \tag{33}$$

where n' and l_n were defined previously. What is particular with even prime powers is that the square root of an integer power of γ_G is not an integer power of γ_G as is the case in odd prime power dimensions. We are forced to introduce +i and −i. What is interesting is that this minimal extension is sufficient in order to diagonalize the operators of the generalized Pauli group in even prime power dimensions, a fact that was already recognized in [2, 16] on the subject.

Combining equations (26) and (27), we obtain the synthetic expression:

$$\left|e_k^i\right\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \gamma_G^{\ominus_G q\odot_G k} \left(\gamma_G^{((i-1)\odot_G q\odot_G q)}\right)^{\frac{1}{2}} \left|e_q^0\right\rangle. \tag{34}$$

Taking equation (33) into account we get an explicit expression for the mutually unbiased bases,

$$\left|e_k^i\right\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \gamma_G^{\ominus_G q\odot_G k} \prod_{n=0,q_n\neq 0}^{m-1} \mathrm{i}^{(j-1)\odot_G 2^n\odot_G 2^n} \gamma_G^{(j-1)\odot_G 2^n\odot_G 2^{n'}} \left|e_q^0\right\rangle, \tag{35}$$

where $q = \sum_{k=0}^{m-1} q_n 2^n$, while n' is the smallest integer strictly larger than n such that $q_{n'} \neq 0$, if it exists, 0 otherwise.

As a consequence of the composition laws (13) and (21),

$$U^j_{l_1} \cdot U^j_{l_2} = \left(\gamma_G^{(j-1)\odot_G l_1 \odot_G l_1}\right)^{\frac{1}{2}} \cdot \left(\gamma_G^{(j-1)\odot_G l_2 \odot_G l_2}\right)^{\frac{1}{2}} \gamma^{(j-1)\odot_G (l_1 \odot_G l_2)} V^{(j-1)\odot_G (l_1 \oplus_G l_2)}_{l_1 \oplus_G l_2}$$
$$= \left(\gamma_G^{(j-1)\odot_G (l_1 \oplus_G l_2)\odot_G (l_1 \oplus_G l_2)}\right)^{\frac{1}{2}} \cdot V^{(j-1)\odot_G (l_1 \oplus_G l_2)}_{l_1 \oplus_G l_2} = U^j_{l_1 \oplus_G l_2}. \tag{36}$$

Therefore,

$$\left(\gamma_G^{(j-1)\odot_G l_1 \odot_G l_1}\right)^{\frac{1}{2}} \cdot \left(\gamma_G^{(j-1)\odot_G l_2 \odot_G l_2}\right)^{\frac{1}{2}} \cdot \gamma^{(j-1)\odot_G (l_1 \odot_G l_2)} = \left(\gamma_G^{(j-1)\odot_G (l_1 \oplus_G l_2)\odot_G (l_1 \oplus_G l_2)}\right)^{\frac{1}{2}}. \tag{37}$$

Formally we can rewrite the previous equation in the form

$$\left(\gamma_G^{(j-1)\odot_G (a \oplus_G b)\odot_G (a \oplus_G b)}\right)^{\frac{1}{2}} = \left(\gamma_G^{(j-1)\odot_G (a \odot_G a)}\right)^{\frac{1}{2}} \cdot \left(\gamma_G^{(j-1)\odot_G (b \odot_G b)}\right)^{\frac{1}{2}} \cdot \left(\gamma_G^{2.((j-1)\odot_G a \odot_G b)}\right)^{\frac{1}{2}},$$

which is reminiscent of equation (1), although we are dealing here with half integer powers of γ_G instead of integer powers. Thanks to this property, it is possible to reproduce nearly literally the proofs given in odd prime power dimensions of the validity of identities (13) and (14), because the automatisms of computation are nearly equivalent. It is important to note however that in even prime power dimensions the expressions of the type $\left(\gamma_G^{(a\odot_G a)}\right)^{\frac{1}{2}}$ do well represent square roots of $\gamma_G^{(a\odot_G a)}$ but must be considered as functions that depend on the 2^m variables a instead of only two variables, as would be the case if we considered literally square roots of integer powers of γ_G (with $\gamma_G = -1$). When a is specified, the sign of the square root is also specified, according to the explicit expression (33). The even- and odd-dimensional cases are covered by the synthetic expression (34). It is worth noting that identity (37) is not valid for arbitrary determinations of the square roots that appear in it; it is valid in our case as a consequence of the fact that the U operators of the same class (labelled by the same upper index i) were shown to obey an exact groupal composition law.

4. Open questions, comments and conclusions

4.1. Other symmetries

At first sight, the computational basis plays a special role in our approach, but one can show that, to some extent, all the mutually unbiased bases can be treated on the same footing. This can be seen as follows. Now that we have at our disposal an explicit expression ((26), (35)) for all the mutually unbiased bases, we can 'reevaluate the situation from the point of view of one of them', say the ith basis (with i different from zero). In order to do so, we can express the action of the operator V^m_n in terms of its basis states. After a straightforward computation, we get that

$$V^n_m(0) = \text{phase} \cdot V^m_{\ominus_G n \oplus_G (i-1)\odot_G m}(i),$$

where

$$V^n_m(0) = \sum_{k=0}^{N-1} \gamma_G^{((k\oplus_G m)\odot_G n)} \left|e^0_{k\oplus_G m}\right\rangle\left\langle e^0_k\right|$$

and

$$V^n_m(i) = \sum_{k=0}^{N-1} \gamma_G^{((k\oplus_G m)\odot_G n)} \left|e^i_{k\oplus_G m}\right\rangle\left\langle e^i_k\right|; \qquad i: 1, \ldots, N.$$

These relations (that we give without proof but are easy to derive from (26) and (35)) are bijective. So the whole discrete Heisenberg–Weyl group is invariant (up to permutations and

phase shifts) when we reexpress it in any of the $N + 1$ mutually unbiased bases. We shall not develop this question here, but this property has important implications in the theory of cloning machines, in relation to error operators and optimal cloning [9, 14]. In prime dimensions, the invariance of the Heisenberg–Weyl group under conjugation by any unitary matrix that maps the computational basis onto a mutually unbiased basis is a well-known property of the extended Clifford group that possesses many applications in number theory and quantum computing [15].

Besides, there exists a one-to-one correspondence between generalized Bell states [20] and the Heisenberg–Weyl group. The properties of invariance of the Bell states in mutually unbiased bases were shown in [19] to be very useful in the derivation of a solution of the so-called mean King problem [10, 17, 18]. In [19], these properties are shown to lead to an elegant expression of the solution valid in all prime power dimensions, a special case of the general solution given in [18].

4.2. Connection with previous works

The expression of the states of the mutually unbiased bases that we derived in the present paper $\left(\left|e_k^i\right\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \gamma_G^{\ominus_G q \odot_G k} \left(\gamma_G^{((i-1)\odot_G q \odot_G q)}\right)^{\frac{1}{2}} \left|e_q^0\right\rangle\right)$ is actually equivalent to the solution derived by Ivanovic [1] when the dimension is an odd prime (which can be shown, when rewritten according to our conventions, to be equivalent to the expression $\left|e_k^i\right\rangle^{\text{Ivan.}} = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \gamma_G^{\ominus_G q \odot_G k} \left(\gamma_G^{((i-1)\odot_G q \odot_G q)}\right) \left|e_q^0\right\rangle$). Our expression differs by a factor $1/_G 2$ in one of the exponents of γ_G. When the dimension is prime and odd, it is easy to compensate the difference by a relabelling of the basis states, because the division by 2 is a permutation of the finite fields with p elements when p is a prime odd number. Contrarily to Ivanovic's expression, our expression is easily generalized in even prime dimension 2 (the qubit case) (in which case we rederive the eigenbases of the Pauli operators) and in prime power dimensions.

As was shown by Wootters and Fields [2], the generalization in prime power dimensions of Ivanovic's expression is the following:

$$\left|e_k^i\right\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \gamma_G^{\text{Tr}\cdot(\ominus_G q \odot_G k)} \left(\gamma_G^{\text{Tr}\cdot(r \odot_G q \odot_G q)}\right) \left|e_q^0\right\rangle, \tag{38}$$

where Tr· represents the field theoretical trace. Our expression seems to be a bit simpler, but both expressions require knowing the addition and multiplication tables of the field, so that the apparent gain in simplicity is relative. Moreover, both expressions are equivalent up to a relabelling in odd prime power dimensions as we shall now show. We could establish the equivalence at once but we prefer to base our derivation on the results of [3] where the interrelation between the Pauli group approach and the expression of Wootters and Fields with the trace factor is made (section 4.3, [3]). Actually, there also exist different groups that present properties similar to those of the generalized Pauli group [12] but do not obey the definition that we gave here. Nevertheless, the generators of the two subgroups corresponding to the computational and the dual basis that are given in [3] coincide with our choice (the subgroups V_0^l and V_l^0 correspond to the classes C_0 and C_1 studied in [3]) so that we are talking about exactly the same group, up to phases. As, in the same paper, a relation was established with the solution of Wootters and Fields [2], our expression for mutually unbiased bases must necessarily coincide with their expression. In [3], it is shown that when there exists a maximal commuting basis of orthogonal unitary matrices, the $N + 1$ bases that diagonalize these classes are unambiguously defined and, moreover, are mutually unbiased. A maximal commuting basis of orthogonal unitary matrices is a set of $N + 1$ sets of $N - 1$ commuting

unitary operators (or classes) plus the identity such that these N^2 operators are orthogonal regarding the in-product induced by the (usual operator) trace denoted by tr·. It is easy to show that the V operators defined in (8) are unitary with $\left(V_i^j\right)^+ = \left(V_i^j\right)^{-1} = \gamma^{\ominus_G(i\odot_G j)} V_{\ominus_G j}^{\ominus_G i}$ and that $\mathrm{tr}\cdot V_i^j = N\cdot\delta_{i,0}\cdot\delta_{j,0}$. Making use of the composition law (13), we obtain the relation $\mathrm{tr}\cdot\left(\left(V_i^j\right)^+\cdot V_l^k\right) = N\cdot\delta_{i,l}\cdot\delta_{j,k}$ so that they form a maximal commuting basis of unitary operators. This theorem suggests another way to derive an expression for the mutually unbiased bases: it is sufficient to find the common eigenstates of the classes of operators $V_l^{(i-1)\odot_G l}$ (where l varies from 0 to $N-1$) in order to determine the value of the states of the ith mutually unbiased basis. When the dimension is an odd (even) prime power, one can check by direct substitution of expression (26) or (35) that the states $\left|e_k^i\right\rangle$ are common eigenstates of the ith class,

$$\begin{aligned}
V_l^{(i-1)\odot_G l}\left|e_k^i\right\rangle &= \sum_{k'=0}^{N-1}\gamma_G^{((k'\oplus_G l)\odot_G(i-1)\odot_G l)}|k'\oplus_G l\rangle \\
&\quad\times\langle k'|\frac{1}{\sqrt{N}}\sum_{q=0}^{N-1}\gamma_G^{\ominus_G q\odot_G k}\left(\gamma_G^{((i-1)\odot_G q\odot_G q)/_G 2}\right)\left|e_q^0\right\rangle \\
&= \frac{1}{\sqrt{N}}\sum_{q=0}^{N-1}\gamma_G^{((q\oplus_G l)\odot_G(i-1)\odot_G l)}\gamma_G^{\ominus_G q\odot_G k}\left(\gamma_G^{((i-1)\odot_G q\odot_G q)/_G 2}\right)\left|e_{q\oplus_G l}^0\right\rangle \\
&= \gamma_G^{(l\odot_G k)}\gamma_G^{((i-1)\odot_G l\odot_G l)/_G 2)}\frac{1}{\sqrt{N}}\sum_{q\oplus_G l=0}^{N-1}\gamma_G^{\ominus_G(q\oplus_G l)\odot_G k} \\
&\quad\times\left(\gamma_G^{((i-1)\odot_G(q\oplus_G l)\odot_G(q\oplus_G l))/_G 2}\right)\left|e_{q\oplus_G l}^0\right\rangle. \qquad (39)
\end{aligned}$$

Thanks to the product law (37), the proof is entirely similar in even prime power dimensions.

In order to establish explicitly and once and for all the equivalence between the expression of Wootters and Fields (38) and ours (26), some work remains to be done because in [3] no proof is given of the fact that expression (38) represents eigenstates of the generalized Pauli operators. In order to prove this result, it is useful to introduce two (field theoretical) dual bases, the first one, which is dual relatively to the trace contains m elements $\tilde{p}$ of the field such that $\mathrm{Tr}\cdot p^i\odot_G\tilde{p}^j = \delta_{i,j}$; the second one which is dual relative to the rest after division by p contains m elements $\tilde{\tilde{p}}^j$ of the field such that $(p^i\odot_G\tilde{\tilde{p}}^j)_0 = \delta_{i,j}$, where $(q)_0$ represents (we work in dimension p^m) the rest after division of q by p. These bases can be shown to exist and to be unique, in virtue of the fact that the bilinear forms $\mathrm{Tr}\cdot(x\odot_G y)$ and $(x\odot_G y)_0$ are non-singular [34]. The non-singular character of the form $(x\odot_G y)_0$ is actually a direct consequence of identity (2). Besides, the m generators of the kth class considered in [3] are equal to $X^i\cdot\prod_{l=0}^{m-1}\left(\prod_{j=0}^{m-1}(Z^j)^{b_{ij}^l}\right)^{k_l}$, with $j,l:0,\ldots,m-1$. In the previous expression, the coefficients k_l are unambiguously defined by the p-ary expansion of k, $k=\sum_{l=0}^{m-1}k_l p^l$ while the multiplication matrix b is defined as follows: $\gamma_i\odot_G\gamma_j = \sum_{l=0}^{m-1}b_{ij}^l\gamma_l$, where the γ are a basis of the field (here we shall consider without loss of generality that $\gamma_i = p^i$). The operators X^i are 'local' operators that shift the ith component of the label of the kth basis state $\left|e_k^0\right\rangle$ (with $k=\sum_{l=0}^{m-1}k_l p^l$) by unity (modulo p), $X^i\left|e_k^0\right\rangle = \left|e_{k'}^0\right\rangle$ with $k_i' = k_i +_{\mathrm{mod}\cdot p} 1$, $k_l' = k_l$ when $l\neq i$. The operator Z^j multiplies the state $\left|e_k^0\right\rangle$ by a global phase equal to $\gamma_G^{k_j}$. In our approach, the generators of the k'th class can be shown to be the same, provided the coefficients of k' expressed in the double-tilded dual basis $\tilde{\tilde{p}}^j$ defined here above are the same as those of k in the direct basis p: $k=\sum_{l=0}^{m-1}k_l p^l$ and $k'=\sum_{j=0}^{m-1}k_j\tilde{\tilde{p}}^j$. Besides, the expressions with

and without Trace (26) and (38) are equivalent, up to a bijective relabelling, in virtue of the identity $\mathrm{Tr}\cdot(r\odot_G k)=((r'/_G 2)\odot_G k)_0$ with k and r arbitrary elements of the Galois field with $N=p^m$ elements, $r=\sum_{l=0}^{m-1} r_l\tilde{p}^l$ and $r'=\sum_{l=0}^{m-1} r_l\tilde{\tilde{p}}^l\odot_G 2$.

This comparison emphasizes the difference between our approach and previous approaches: our expression (8) of the generalized Pauli operators is global and non-local, although they can be decomposed as products of local operators. It also shows that the field theoretical trace is replaced in our approach by another non-singular bilinear form, the rest after division by p.

Although it is out of the scope of the present paper, it would be interesting to understand the relation between our results in even prime power dimensions and the results presented in [2, 16].

4.3. Other dimensions

It is still an open question to know whether maximal sets of mutually unbiased bases exist in arbitrary dimensions. For instance, in dimension 6 which is the smallest dimension that is not a power of a prime, nobody knows whether or not such a maximal set exists [6, 7]. It is not possible to apply our treatment in this case because no finite field with six elements exists. We could try to repeat the procedure with operations that do not form a field; for instance we could try to find a distributive ring with six elements. Such a ring obeys the same definition as a field (the definition that was given at the beginning of the paper), except that the multiplication need not be invertible—dividers of zero different from zero are allowed. One can show that there is only one distributive ring with six elements, that corresponds to the usual operations (multiplication and addition modulo 6). If we study the structure of the $N^2=36$ Heisenberg–Weyl unitary transformations in that case, we find that there are more than $N+1=7$ subgroups of six elements (5 + the identity). This is because, as a consequence of the non-invertibility of the multiplication modulo 6 (3 and 2 divide zero), certain operators present degeneracies and belong simultaneously to different subgroups (a treatment of similar type is given in detail in [20] for the case $N=4$). The bases that diagonalize these operators are not mutually unbiased in general and the construction that was successfully applied in prime power dimensions does not provide a maximal set of mutually unbiased bases (actually expression (29) allows us to derive collections of at most three mutually unbiased bases). Therefore the question of the existence of seven mutually unbiased bases in a six-dimensional Hilbert space is still open, and our approach unfortunately does not contribute to the elucidation of that problem.

4.4. Conclusions

As we already mentioned, there is a one-to-one correspondence between (generalized) Bell states and (generalized) Pauli operators [20] (see also [35] for a different approach based on additive and multiplicative characters of the Galois field). It can also be proven [19, 20] that the Bell states are invariant when we pass from one of the mutually unbiased bases to another one, an important result in the theory of cloning machines that was only conjectured until now [14]. Actually, the present results were largely inspired by results that we obtained in the framework of quantum cryptography [9] where the interest of mutually unbias was recognized several years ago, with regard to encryption [21–23] and cloning as well [9, 14, 24].

It is worth noting that, besides quantum cryptography and quantum cloning, the Bell states also find many applications in quantum teleportation and dense coding. For instance, the connections between mutually unbiased bases, complete orthogonal families of unitary matrices and teleportation, have already been emphasized in the past [25, 26]. There

also exists an impressive literature about the interrelation between finite fields and the discrete Wigner representation [28–31]. It is worth noting that if we perform a tomographic development of the density matrix in the basis of the V operators, we obtain [20] the identity $\rho = (1/N)\sum_{k,l} V_l^k \mathrm{Tr}\cdot\left(\left(V_l^k\right)^+\cdot\rho\right)$.

It is very instructive to compare the amplitudes of the decomposition of a density matrix into the V basis with the Wigner function:

$$\mathrm{Tr}\cdot\left(V_l^k\right)^+\rho = \mathrm{Tr}\cdot\left(V_l^k\right)^+\sum_{i,j=0}^{N-1}\rho_{i\oplus j,i}\left|e^0_{i\oplus j}\right\rangle\left\langle e^0_i\right| = \sum_{i,j=0}^{N-1}\rho_{i\oplus j,i}\gamma^{\ominus(i\oplus l)\odot k}\delta_{l,j} = \gamma^{\ominus l\odot k}\sum_{j=0}^{N-1}\rho_{j\oplus l,j}\gamma^{\ominus j\odot k}.$$

The Wigner function can be written [27] in terms of the conjugate continuous variables q and p as $W(q,p) = C\cdot\int \mathrm{d}^3r\,\rho(q-r,q+r)\mathrm{e}^{2\mathrm{i}pr/h} = C'\cdot\int \mathrm{d}^3r'\rho(r',2\cdot q-r')\mathrm{e}^{-\mathrm{i}2pr'/h}$, where C is a normalization constant, while i is the square root of -1. The analogy of both expressions is striking and, as we can see, the tomography of a quantum state that we realize in the Pauli group approach provides a discrete counterpart of the Wigner representation. In general the coefficients $\mathrm{Tr}\cdot\left(\left(V_l^k\right)^+\cdot\rho\right)$ are complex, which does not meet the requirements of a properly discretized Wigner function, but a properly discretized Wigner function can be obtained by taking well-chosen linear combinations of the V operators. These combinations are in one-to-one correspondence with the solution of the mean King problem given in [19]. It is out of the scope of the present paper but it would be interesting to study the connection with other proposals for discrete phase-space representation [29–31]. One should note that as the V operators are diagonal in the $N+1$ mutually unbiased bases, full tomography can be obtained by performing $N+1$ von Neumann measurements, as was already shown by Ivanovic in prime dimensions and Wootters and Fields in prime power dimensions.

Finally, the properties of Bell states are also directly related to the error operators [31–33], and it would be worth investigating to what extent our formalism contributes to a simplification of the theory of error correcting codes, in prime power dimensions.

To conclude, we note that, despite the fact that the problem (and its solutions) seems to be regularly rediscovered by different generations of physicists, which means also a lack of time and energy, our results about the mean King problem [19] confirm that it is important to explore alternative approaches in the treatment of the question of mutually unbiased bases.

We hope that the present paper contributes to a deeper understanding of the old problem of mutually unbiased bases.

Acknowledgments

The author acknowledges a Postdoctoral Fellowship of the Fonds voor Wetenschappelijke Onderzoek, Vlaanderen and also support from the IUAP programme of the Belgian government, the grant V-18, and the Solvay Institutes for Physics and Chemistry. Sincere thanks to Professors P Cara (VUB), E Jespers (VUB) and B-G Englert (NUS) for fruitful and enjoyable discussions and advice. Thank-you to David Gross (Postdam) for drawing the author's attention to [15, 28].

References

[1] Ivanovic I D 1981 *J. Phys. A: Math. Gen.* **14** 3241
[2] Wootters W K and Fields B D 1989 *Ann. Phys.* **191** 363

[3] Bandyopadhyay S, Boykin P, Roychowdhury V and Vatan F 2002 *Algorithmica* **34** 512
Bandyopadhyay S, Boykin P, Roychowdhury V and Vatan F 2001 *Preprint* quant-ph/0103162, 1–22
[4] Schwinger J 1960 *Proc. Natl Acad. Sci. USA* **46** 570
[5] Vlasov A Yu 2003 *Preprint* quant-ph/0302064
[6] Archer C 2003 *Preprint* quant-ph 0312204, 1–17
[7] Grassl M 2004 *Preprint* quant-ph 0406175, 1–8
[8] Weyl H 1927 *Z. Phys.* **46** 1
Weyl H 1928 *Gruppentheorie und Quantenmechanik* (Leipzig: Hirzel)
Weyl H 1931 *The Theory of Groups and Quantum Mechanics* (New York: Dutton) (Engl. Transl.)
[9] Nagler B and Durt T 2003 *Phys. Rev.* A **66** 042323
[10] Aharonov Y and Englert B-G 2001 *Z. Naturforsch.* **56** 16
[11] Bruckner C and Zeilinger A 1999 *Phys. Rev. Lett.* **83** 17, 3354
[12] Lawrence J, Bruckner C and Zeilinger A 2002 *Phys. Rev.* A **65** 032320
[13] Pittenger A O and Rubin M H 2003 *Preprint* quant-ph/0308142
[14] Cerf N J, Durt T and Gisin N 2002 *J. Mod. Opt.* **49** 1355 (special issue on quantum information)
[15] Appleby M 2004 *Preprint* quant-ph/0412001, 1–26
[16] Klappenecker A and Rotteler M 2003 *Preprint* quant-ph/0309120, 1–8
[17] Vaidman L, Aharonov Y and Albert D Z 1987 *Phys. Rev. Lett.* **58** 1385
[18] Aravind P K 2003 *Z. Naturforsch.* A **58** 2212
[19] Durt T 2004 *Preprint* quant-ph/0401037, 1–10
[20] Durt T 2004 *Preprint* quant-ph/0401046, 1–24
[21] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* (New York: IEEE) p 175
[22] Boykin P and Roychowdhury V 2000 *Preprint* quant-ph/0003059
[23] Bechmann-Pasquinucci H and Tittel W 2000 *Phys. Rev.* A **61** 062308
[24] Cerf N J 2000 *Phys. Rev. Lett.* **84** 4497
Cerf N J 1998 *Acta Phys. Slov.* **48** 115 (special issue on quantum information)
Cerf N J 2000 *J. Mod. Opt.* **47** 187 (special issue on quantum information)
[25] Fivel D I 1995 *Phys. Rev. Lett.* **974** 835
[26] Werner R F 2004 *Preprint* quant-ph/0003070, 1–21
[27] Peres A 1993 *Quantum Theory, Concepts and Methods* (Dordrecht: Kluwer)
[28] Vourdas A 1996 *J. Phys. A: Math. Gen.* **29** 4275
[29] Wootters W K 2004 Picturing qubits in phase-space *Preprint* quant-ph/0406032
[30] Gibbons K S, Hoffman M J and Wootters W K 2004 *Preprint* quant-ph/0401155, 1–60
[31] Paz J, Roncaglia A and Saraceno M 2004 *Preprint* quant-ph/0400117, 1–19
[32] Calderbank R, Rains E M, Shor P W and Sloane N J A 1997 *Phys. Rev. Lett.* **78** 405
[33] Nielsen M A and Chuang I L 2000 *Quantum Computing and Quantum Information* (Cambridge: Cambridge University Press)
[34] Karpilovski G 1988 *Field Theory* (New York: Dekker)
[35] Planat M, Rosu H, Perrine S and Saniga M 2004 *Preprint* quant-ph/0409081, 1–14