A new method of construction of all sets of mutually unbiased bases for two-qubit systems

Iulia Ghiu
Centre for Advanced Quantum Physics, Department of Physics, University of Bucharest, P. O. Box MG-11, R-077125 Bucharest-Măgurele, Romania
E-mail: iulia.ghiu@g.unibuc.ro

Abstract. Mutually unbiased bases are an important tool in many applications of quantum information theory. We present a new algorithm for finding the mutually unbiased bases for two-qubit systems. We derive a system of four equations in the Galois field GF(4) and show that the solutions of this system are sufficient for obtaining the most general set of mutually unbiased bases. Further, our algorithm is applied to an example and we show that there are three possible solutions of the system of four equations, each solution leading to a different set of mutually unbiased bases.

1. Introduction

The concept of mutually unbiased bases (MUBs) was initially proposed by Julian Schwinger [1]. These states are maximally incompatible, which means that using a basis to obtain optimal outcomes, leads to maximally random results when the other bases are considered in the measurements. If we denote two elements of different orthonormal bases by \( \{ | \psi_j \rangle \} \) and \( \{ | \phi_k \rangle \} \), then the two bases are called mutually unbiased if

\[
| \langle \psi_j | \phi_k \rangle |^2 = \frac{1}{d}.
\]

where \( d \) is the dimension of the Hilbert space [2]. The MUBs constitute now a basic ingredient in many applications of quantum information processing: quantum tomography, quantum key distribution required in cryptography [3], discrete Wigner function [4], quantum teleportation [5], or quantum error correction codes [6].

If the measurements used for the state reconstruction are built with the help of the mutually unbiased bases, then this scheme is called MUB tomography [7]. The simplest example of MUBs can be given for qubits. If the system is prepared in the state \( | \uparrow \rangle \) (or \( | \downarrow \rangle \)), then a measurement of the spin along the \( x \)– or \( y \)– axis generates the outcomes up or down with the same probability, which is equal to 1/2. The eigenvectors of the Pauli operators \( \hat{\sigma}_x \), \( \hat{\sigma}_y \), and \( \hat{\sigma}_z \) form a set of MUBs for qubits.

It is known that the maximal number of mutually unbiased bases can be at most \( d + 1 \) [8]. This maximal value can be reached in the case when the dimension of the space is a prime \( (d = p) \) or a power of prime \( (d = p^n) \) [9].

It was proved in the case when \( d \) is a power of a prime number that there is an approach for finding the MUBs, namely one has to generate families of unitary operators, whose eigenvectors
solve the problem of MUBs. In other words, one needs to determine \( d + 1 \) classes of \( d - 1 \) commuting operators. These special operators are called mutually unbiased operators [10].

The paper is organized as follows: In Section 2 we present the standard set of MUBs for qubits, where three bases are obtained from tensor product of \( \hat{\sigma}_j \) and \( \hat{I} \). Further, some basic notations and definitions used in the Galois fields are recalled in Section 3. The main result of the paper is given in Section 4, where we find a system of four equations in the Galois field \( \text{GF}(4) \). The solution of these equations leads to the construction of the most general set of MUBs for two-qubit systems, not only the standard one. Finally, we make some concluding remarks in Section 5.

2. Preliminaries

In this paper we analyze the two-qubit systems. An example of 5 sets of 3 commuting operators for 2 qubits is [11]:

|   | \( \hat{\sigma}_z \hat{\sigma}_z \) | \( \hat{I} \hat{\sigma}_z \) | \( \hat{\sigma}_z \hat{I} \) |
|---|---|---|---|
| 1. | \( \hat{\sigma}_x \hat{\sigma}_x \) | \( \hat{I} \hat{\sigma}_x \) | \( \hat{\sigma}_x \hat{I} \) |
| 2. | \( \hat{\sigma}_y \hat{\sigma}_y \) | \( \hat{I} \hat{\sigma}_y \) | \( \hat{\sigma}_y \hat{I} \) |
| 3. | \( \hat{\sigma}_x \hat{\sigma}_y \) | \( \hat{\sigma}_x \hat{\sigma}_x \) | \( \hat{\sigma}_y \hat{\sigma}_z \) |
| 4. | \( \hat{\sigma}_y \hat{\sigma}_x \) | \( \hat{\sigma}_x \hat{\sigma}_y \) | \( \hat{\sigma}_x \hat{\sigma}_z \) |

Table 1. The standard set of MU operators for two qubits.

We did not write the tensor multiplication sign in the above Table. In the case of two-qubit systems, there is only one allowed structured of the bases, namely (3,2), which means that three bases are separable, while two are entangled. The three separable bases given by Table 1 are obtained as the common eigenvectors of tensor product of the operators \( \hat{\sigma}_z \) and \( \hat{I} \) (all the three possibilities: see the first row of Table 1), tensor product of \( \hat{\sigma}_x \) and \( \hat{I} \) (second row), and tensor product of \( \hat{\sigma}_y \) and \( \hat{I} \) (third row), respectively. The table of operators with this property are called the standard set of MU operators [7]. The last two rows of Table 1 generate entangled bases which are called belle and beau [12].

3. Galois fields: notations and definitions

If \( d = p^n \) is the power of a prime number, then the \( d + 1 \) MUBs can be constructed with the help of Galois fields \( \text{GF}(d) \). Wootters [12] and Gibbons et al. [13] proposed a method to associate the MUBs to the so-called discrete phase space. The discrete phase space of a d-level system is a \( d \times d \) lattice, whose coordinates are elements of the finite Galois field \( \text{GF}(d) \) [12]. Further a state is associated to a line in the discrete phase space. The set of parallel lines is called a striation. There are \( d + 1 \) striations. It turns out that the MUBs are determined by the bases associated with each striation.

In the following we will recall some basic definitions used in Galois fields. The map trace of a field element \( x \in \text{GF}(p^n) \) is as follows:

\[
\text{tr } x = x + x^2 + ... + x^{p^n-1}.
\]

A basis \( \{ \alpha_i \} \) is called self-dual if \( \text{tr}(\alpha_i \alpha_j) = \delta_{ij} \).

Let us consider two elements \( x, y \in \text{GF}(p^n) \) which can be written with the help of two bases \( E = \{ e_1, ..., e_n \} \) and \( F = \{ f_1, ..., f_n \} \) as follows:

\[
x = \sum_{i=1}^{n} x_{e_i} e_i;
\]
\[ y = \sum_{j=1}^{n} y_j f_j. \] (1)

We denote by \( \hat{\sigma}_x, \hat{\sigma}_z \) the generalized Pauli operators [14]:

\[
\hat{\sigma}_x |n\rangle = |n + 1\rangle;
\hat{\sigma}_z |n\rangle = \omega^n |n\rangle,
\]

where \( |n\rangle \) is the computational basis and \( \omega = \exp(2\pi i/d) \) is the \( d \)th root of the unity.

To the translation in the discrete phase space by the element \((x, y)\) we associate an operator \( T_{(x, y)} \) called the translation operator [13]:

\[
T_{(x, y)} := \hat{\sigma}_x^{x_1} \hat{\sigma}_x^{y_1} \otimes \ldots \otimes \hat{\sigma}_x^{x_n} \hat{\sigma}_x^{y_n}.
\] (2)

In the case when \( d = 2^2 \), there is only one irreducible polynomial: \( P(x) = x^2 + x + 1 \). We denote by \( \mu \) the primitive element of \( \text{GF}(4) \) and we get

\[ \mu^2 + \mu + 1 = 0. \]

The elements of \( \text{GF}(4) \) are:

\[ \{0, 1, \mu, \mu^2\}. \]

If we use the selfdual basis \( \{\mu, \mu^2\} \) in \( \text{GF}(4) \), then the following correspondence given by Eq. (2) between the set of points in the discrete phase space and the set of MU operators can be established:

\[
\begin{align*}
(\mu, 0) & \leftrightarrow \hat{\sigma}_x \hat{I}, \\
(\mu^2, 0) & \leftrightarrow \hat{I} \hat{\sigma}_x, \\
(0, \mu) & \leftrightarrow \hat{\sigma}_z \hat{I}, \\
(0, \mu^2) & \leftrightarrow \hat{I} \hat{\sigma}_z.
\end{align*}
\] (3)

4. The new algorithm of construction of MUBs

4.1. The commutation relations

Two operators commute if their associated points in the phase-space \((a_1, b_1)\) and \((a_2, b_2)\) satisfy [14]

\[ \text{tr}(a_1 b_2) = \text{tr}(a_2 b_1). \] (4)

The MUBs can be constructing with the help of \( d + 1 \) classes of \( d - 1 \) commuting operators, i.e. MU operators. In the case of two-qubit systems, we need to generate a table with 5 rows, each row representing the set of 3 commuting operators. We denote the operator which belongs to the row \( r \) and column \( c \), where \( r = 1, 5 \) and \( c = 1, 3 \) by \( O_{r,c} \) as one can see in the left Table of Eq. (5). The point in the phase space \((a_c^{(r)}, b_c^{(r)})\) is associated to the operator \( O_{r,c} \):

\[ O_{r,c} \leftrightarrow (a_c^{(r)}, b_c^{(r)}). \]

The correspondence between the set of MU operators and the set of points in the discrete phase space is shown below:
There are four operators which define the whole Table 1, namely the first two operators of the rows 1 and 2: $O_{1,1};$ $O_{1,2};$ $O_{2,1};$ $O_{2,2}$. The other 11 operators are determined as follows [11]:

- $O_{r,c} = O_{r,c-2}O_{r,c-1}$, for $r = 1,2$; $c = 3$ and
- $O_{r,c} = O_{2,c}O_{1,c+r-3}$ for $r > 2$.

The indices $r$ and $c$ are written modulo four.

In our new construction, we consider that the right Table of Eq. (5) of points in the discrete phase space which correspond to the set of MU operators is unique defined by the following four points:

\[
\begin{align*}
(a_1^{(1)}, b_1^{(1)}); \ (a_2^{(1)}, b_2^{(1)}); \\
(a_1^{(2)}, b_1^{(2)}); \ (a_2^{(2)}, b_2^{(2)}).
\end{align*}
\]

Therefore, we need to determine the eight parameters $a_j^{(i)}$ and $b_j^{(i)}$ given by Eq. (6) such that all the 15 points which are obtained correspond to MU operators. In other words, we have to use the commutation relation in the discrete phase space given by Eq. (4) for the set of 3 points of all the 5 rows. For each row we write 3 commutation relations, which lead to a total number of 15 equations for the whole table of points. These 15 equations are written in Appendix A.

### 4.2. The general algorithm

We proved that only 4 equations of the total number of 15 are independent. These are Eqs. (A.1), (A.4), (A.7), and (A.10) in Appendix A:

\[
\begin{align*}
\text{tr} \begin{bmatrix} a_1^{(1)} & b_2^{(1)} \end{bmatrix} &= \text{tr} \begin{bmatrix} a_2^{(1)} & b_1^{(1)} \end{bmatrix} \\
\text{tr} \begin{bmatrix} a_1^{(2)} & b_2^{(2)} \end{bmatrix} &= \text{tr} \begin{bmatrix} a_2^{(2)} & b_1^{(2)} \end{bmatrix} \\
\text{tr}[a_1^{(1)}b_2^{(2)} + a_1^{(2)}b_1^{(1)}] &= \text{tr}[a_2^{(1)}b_1^{(2)} + a_2^{(2)}b_1^{(1)}] \\
\text{tr}[a_1^{(2)}b_1^{(1)} + a_1^{(1)}b_2^{(2)} + a_2^{(1)}b_1^{(2)}] &= \text{tr}[a_2^{(2)}b_2^{(1)} + a_1^{(1)}b_1^{(2)} + a_2^{(1)}b_1^{(2)}].
\end{align*}
\]

The general algorithm of the construction:

- The parameters $b_1^{(1)}, b_2^{(1)}, a_1^{(1)}, a_1^{(2)}$ are arbitrary chosen.
- The three variables $a_2^{(1)}, a_2^{(2)},$ and $b_2^{(2)}$ are obtained from the system of equations (7).
- After obtaining the solution, one has to find the table of points in the discrete phase space analogue to the right table of Eq. (5).
- With the help of the correspondence given by Eq. (3), one generate the table which contain 5 classes of 3 commuting operators.
- The eigenvectors of each set of 3 commuting operators represent the MUBs.
4.3. Example

According to the algorithm presented in Sec. 4.2, we have to fix five parameters:

\[
\begin{align*}
(a_1^{(1)}, b_1^{(1)}) &= (\mu^2, \mu) \\
(a_1^{(2)}, b_1^{(2)}) &= (\mu, \mu) \\
b_2^{(1)} &= \mu^2.
\end{align*}
\]

The system of Eqs. (7) becomes:

\[
\begin{align*}
\text{tr} \left[ \mu a_2^{(1)} \right] &= 1 \\
\text{tr} \left[ \mu b_2^{(2)} \right] &= \text{tr} \left[ \mu a_2^{(2)} \right] \\
\text{tr}[\mu^2 b_2^{(2)} + 1] &= \text{tr}[\mu a_2^{(3)} + \mu a_2^{(2)}] \\
\text{tr}[\mu^2 + 1 + a_2^{(1)} b_2^{(2)}] &= \text{tr}[\mu^2 a_2^{(2)} + 1 + \mu a_2^{(1)}].
\end{align*}
\]

There are three possible solutions of the system (8):

Solution A): \( a_2^{(1)} = 1 \), \( a_2^{(2)} = \mu^2 \), and \( b_2^{(2)} = \mu^2 \). This solution leads to the Table 1, i.e. the standard set of MU operators.

Solution B): \( a_2^{(1)} = 1 \), \( a_2^{(2)} = 1 \), and \( b_2^{(2)} = \mu \). Therefore we obtain the following table of points in the discrete phase space and accordingly the set of MU operators:

\[
\begin{array}{|c|c|c|}
\hline
\text{No.} & \text{Set of points} & \text{MU operators} \\
\hline
1. & (1, \mu^2); (\mu, 1); (\mu^2, \mu) & \hat{\sigma}_x \hat{\sigma}_y; \hat{\sigma}_y \hat{\sigma}_z; \hat{\sigma}_z \hat{\sigma}_x \\
2. & (1, \mu); (\mu, \mu); (\mu^2, 0) & \hat{\sigma}_y \hat{\sigma}_x; \hat{\sigma}_y I; I \hat{\sigma}_x \\
3. & (0, 1); (1, 1); (1, 0) & \hat{\sigma}_z \hat{\sigma}_x; \hat{\sigma}_y \hat{\sigma}_y; \hat{\sigma}_x \hat{\sigma}_z \\
4. & (0, \mu); (\mu^2, 1); (\mu^2, \mu^2) & \hat{\sigma}_z I; \hat{\sigma}_x \hat{\sigma}_y; \hat{\sigma}_y I \\
5. & (0, \mu^2); (\mu, \mu^2); (\mu, 0) & I \hat{\sigma}_z; \hat{\sigma}_x \hat{\sigma}_z; \hat{\sigma}_x I \\
\hline
\end{array}
\]

Solution C): \( a_2^{(1)} = \mu \), \( a_2^{(2)} = 1 \), and \( b_2^{(2)} = \mu \). The table of points in the discrete phase space and the set of MU operators are shown below:

\[
\begin{array}{|c|c|c|}
\hline
\text{No.} & \text{Set of points} & \text{MU operators} \\
\hline
1. & (1, \mu^2); (\mu, \mu^2); (\mu^2, \mu) & \hat{\sigma}_y \hat{\sigma}_y; \hat{\sigma}_x \hat{\sigma}_z; \hat{\sigma}_z \hat{\sigma}_z \\
2. & (1, \mu); (\mu, \mu); (\mu^2, 0) & \hat{\sigma}_y \hat{\sigma}_x; \hat{\sigma}_y I; I \hat{\sigma}_x \\
3. & (0, 1); (\mu, 1); (\mu^2, 1) & \hat{\sigma}_z \hat{\sigma}_x; \hat{\sigma}_y \hat{\sigma}_z; \hat{\sigma}_z \hat{\sigma}_y \\
4. & (0, 1); (0, \mu); (0, \mu^2) & \hat{\sigma}_z \hat{\sigma}_z; \hat{\sigma}_z I; I \hat{\sigma}_z \\
5. & (1, \mu^2); (\mu, 0); (\mu^2, \mu^2) & \hat{\sigma}_z \hat{\sigma}_y; \hat{\sigma}_z I; I \hat{\sigma}_y \\
\hline
\end{array}
\]

5. Conclusions

In this paper we have presented a new algorithm of construction of all sets of MUBs for two-qubit systems. The main result is the system of four equations (7) in the Galois field GF(4).

With the help of the solution of this system, one can obtain different sets of MUBs, not only the well known standard set.

Acknowledgments

I wish to thank Gunnar Björk, Andrei B. Klimov, and Luis L. Sánchez-Soto for useful discussions. This work was supported by CNCSIS - UEFISCSU, postdoctoral research project PD code 151, no. 150/30.07.2010 for the University of Bucharest.
Appendix A. The 15 commutation relations

\[ \text{tr} \left[ a_1^{(1)} b_2^{(1)} \right] = \text{tr} \left[ a_2^{(1)} b_1^{(1)} \right] \quad (A.1) \]
\[ \text{tr} \left[ a_1^{(1)} (b_1^{(1)} + b_2^{(1)}) \right] = \text{tr} \left[ b_1^{(1)} (a_1^{(1)} + a_2^{(1)}) \right] \quad (A.2) \]
\[ \text{tr} \left[ a_2^{(1)} (b_1^{(1)} + b_2^{(1)}) \right] = \text{tr} \left[ b_2^{(1)} (a_1^{(1)} + a_2^{(1)}) \right] \quad (A.3) \]
\[ \text{tr} \left[ a_1^{(2)} b_2^{(2)} \right] = \text{tr} \left[ a_2^{(2)} b_1^{(2)} \right] \quad (A.4) \]
\[ \text{tr} \left[ a_1^{(2)} (b_1^{(2)} + b_2^{(2)}) \right] = \text{tr} \left[ b_1^{(2)} (a_1^{(2)} + a_2^{(2)}) \right] \quad (A.5) \]
\[ \text{tr} \left[ a_2^{(2)} (b_1^{(2)} + b_2^{(2)}) \right] = \text{tr} \left[ b_2^{(2)} (a_1^{(2)} + a_2^{(2)}) \right] \quad (A.6) \]
\[ \text{tr} \left[ (a_1^{(1)} + a_1^{(2)}) (b_2^{(1)} + b_2^{(2)}) \right] = \text{tr} \left[ (a_2^{(1)} + a_2^{(2)}) (b_1^{(1)} + b_1^{(2)}) \right] \quad (A.7) \]
\[ \text{tr} \left[ (a_1^{(1)} + a_1^{(2)}) (b_3^{(1)} + b_3^{(2)}) \right] = \text{tr} \left[ (a_2^{(1)} + a_2^{(2)}) (b_1^{(1)} + b_1^{(2)}) \right] \quad (A.8) \]
\[ \text{tr} \left[ (a_1^{(1)} + a_2^{(2)}) (b_3^{(1)} + b_3^{(2)}) \right] = \text{tr} \left[ (a_2^{(1)} + a_3^{(2)}) (b_1^{(1)} + b_1^{(2)}) \right] \quad (A.9) \]
\[ \text{tr} \left[ (a_1^{(2)} + a_1^{(2)}) (b_3^{(2)} + b_3^{(1)}) \right] = \text{tr} \left[ (a_2^{(2)} + a_3^{(2)}) (b_1^{(2)} + b_1^{(1)}) \right] \quad (A.10) \]
\[ \text{tr} \left[ (a_1^{(2)} + a_1^{(2)}) (b_3^{(2)} + b_1^{(1)}) \right] = \text{tr} \left[ (a_2^{(2)} + a_1^{(1)}) (b_1^{(2)} + b_1^{(1)}) \right] \quad (A.11) \]
\[ \text{tr} \left[ (a_2^{(2)} + a_3^{(1)}) (b_3^{(2)} + b_1^{(1)}) \right] = \text{tr} \left[ (a_3^{(2)} + a_1^{(1)}) (b_2^{(2)} + b_1^{(1)}) \right] \quad (A.12) \]
\[ \text{tr} \left[ (a_1^{(2)} + a_3^{(1)}) (b_3^{(2)} + b_1^{(1)}) \right] = \text{tr} \left[ (a_2^{(2)} + a_1^{(1)}) (b_1^{(2)} + b_1^{(1)}) \right] \quad (A.13) \]
\[ \text{tr} \left[ (a_1^{(2)} + a_3^{(1)}) (b_3^{(2)} + b_2^{(1)}) \right] = \text{tr} \left[ (a_3^{(2)} + a_2^{(1)}) (b_1^{(2)} + b_1^{(1)}) \right] \quad (A.14) \]
\[ \text{tr} \left[ (a_2^{(2)} + a_1^{(1)}) (b_3^{(2)} + b_2^{(1)}) \right] = \text{tr} \left[ (a_3^{(2)} + a_2^{(1)}) (b_2^{(1)} + b_1^{(1)}) \right] \quad (A.15) \]

We proved that these 15 equations are not independent, which means that if we start we the Eqs. (A.1), (A.4), (A.7), and (A.10) we obtain all the other 11 equations. The set of four equations is the minimal one, that generates the other equations.

References

[1] Schwinger J 1960 Proc. Natl. Acad. Sci. USA 46 570.
[2] Wootters W K and Fields B D (1989) Ann. Phys. (N. Y.) 191 363.
[3] Bechmann-Pasquinucci H and Peres A (2000) Phys. Rev. Lett. 85 3313.
[4] Wootters W K (1987) Ann. Phys. (N. Y.) 176 1.
[5] Koniorczyk M, Buzek V, and Janszky J (2001) Phys. Rev. A 64 034301.
[6] Paz J P, Roncaglia A J, and Saraceno M (2005) Phys. Rev. A 72 012309.
[7] Klimov A B, Munoz C, Fernandez A, and Saavedra C 2008 Phys. Rev. A 77 060303 (R).
[8] Ivanovic I D (1981) J. Phys. A 14 3241.
[9] Calderbank A R, Cameron P J, Kantor W M, and Seidel J J (1997) Proc. London Math. Soc. 75 436.
[10] Bandyopadhyay S, Boykin P O, Roychowdhury V, and Vatan V 2002 Algorithmica 34 512.
[11] Romeo J L, Björk G, Klimov A B, and Sánchez-Soto L L 2005 Phys. Rev. A 72 062310.
[12] Wootters W K 2004 IBM J. Res. Dev. 48 99.
[13] Gibbons K S, Hoffman M J, and Wootters W K 2004 Phys. Rev. A 70, 062101.
[14] Klimov A B, Romero J L, Björk G, Sánchez-Soto L L 2009 Ann. Phys. (N. Y.) 324 53.