EXTRAORDINARY SUBGROUPS NEEDED FOR THE CONSTRUCTION OF MUTUALLY UNBIASED BASES FOR THE DIMENSION $d = 8$*

IULIA GHIU[1,a], CRISTIAN GHIU[2]

[1]Centre for Advanced Quantum Physics, Department of Physics, University of Bucharest, PO Box
MG-11, R-077125, Bucharest-Magurele, Romania
E-mail[a]: iulia.ghiu@g.unibuc.ro
[2]University Politehnica of Bucharest, Faculty of Applied Sciences, Department of Mathematical
Methods and Models, Splaiul Independentei 313, R-060042 Bucharest, Romania

Received January 12, 2015

The mutually unbiased bases are widely used in many applications of quantum information theory. Recently it was proved that there is a correspondence between mutually unbiased bases and mutually orthogonal extraordinary supersquares. An extraordinary supersquare is obtained starting from its generating extraordinary subgroup, therefore knowing the general expression of these kinds of subgroups is extremely important. We are focus here on finding the extraordinary subgroups for $\mathbb{F}_8 \times \mathbb{F}_8$. Further we construct the set of mutually orthogonal extraordinary supersquare of order 8 with the help of nine extraordinary subgroups, whose unique intersection element is the element zero. Then, we show how the complete set of mutually unbiased bases for $d = 8$ can be obtained. The case $d = 8$ corresponds to systems of three particles of spin-1/2.

Key words: mutually unbiased bases, Latin squares, supersquares.

1. INTRODUCTION

The mutually unbiased bases (MUBs) are the fundamental tools in many processes of quantum information theory such as: quantum tomography, quantum key distribution, discrete Wigner function, quantum teleportation [1–3]. Two bases $\{|\, u_j\,\rangle\}$ and $\{|\, v_k\,\rangle\}$ of a Hilbert space of dimension d are called mutually unbiased if [1]

$$|\langle\, u_j\,|\, v_k\,\rangle|^2 = 1/d.$$

There are many methods for constructing MUBs [4–9].

The connection between Latin squares and MUBs has been investigated in many recent articles [10–15]. One approach of construction of the MUBs is based on the case when the two striations with vertical and horizontal lines are always present among the set of mutually orthogonal striations needed for generating the set of MUBs [11]. This construction provides only a particular class of MUBs, the one which contains the eigenvectors of tensor products of the Pauli operators X and the

*Paper presented at the conference "Advanced many-body and statistical methods in mesoscopic systems II", September 1-5, 2014, Brasov, Romania.

identity, Z and the identity, or their combinations, which leads to the fact that the associated striations of MUBs are Latin squares. Also in Ref. [12] a set of Latin operators was obtained, whose eigenvectors represent MUBs.

We want to emphasize that the connection between the MUBs described in the previous references is done only with the Latin squares and not with a wider class. We have proposed an algorithm for generating the most general MUBs, not only those whose associated striations are Latin squares [16].

In this paper in Sec. 2 we present a proposition where the general expression of the extraordinary subgroups for $\mathbb{F}_8 \times \mathbb{F}_8$ is provided. Further in Sec. 3 we give an example of such subgroup and illustrate how this can be employed in order to generate an extraordinary supersquare. In Sec. 4 we show an example of nine extraordinary subgroups, whose unique intersection element is zero, *i.e.* the associated set of nine extraordinary supersquares are orthogonal. Finally we apply our algorithm for generating the complete set of MUBs for the dimension $d = 8$. We make the concluding remarks in Sec. 5. The proof of the Proposition given in Sec. 2 is presented in Appendix A.

2. DEFINITION OF THE EXTRAORDINARY SUPERSQUARES. THE GENERAL EXPRESSION OF THE EXTRAORDINARY SUBGROUPS OF $\mathbb{F}_8 \times \mathbb{F}_8$

Definition. [17] Consider a square of order d denoted by $S = \{A_1, A_2, ..., A_d\}$. S is called a **supersquare of order d** if A_1 is a subgroup with d elements of $\mathbb{F}_d \times \mathbb{F}_d$ and $S = \mathbb{F}_d \times \mathbb{F}_d / A_1$ is the quotient set. The other $d-1$ subsets A_j are obtained as follows:

$$A_1 = \hat{0};\ \ A_2 = a_2 + A_1 = \hat{a}_2; \ldots\ \ A_d = a_d + A_1 = \hat{a}_d,$$

where $a_j \in \mathbb{F}_d \times \mathbb{F}_d$, j= 2, 3, ..., d. A_1 is called the generating subgroup of the supersquare.

Let us consider $v_1 = (x_1, y_1)$ and $v_2 = (x_2, y_2) \in \mathbb{F}_d \times \mathbb{F}_d$ with $d = p^n$, p being a prime number. We denote by $|v_1 \quad v_2|$ the following determinant:

$$|v_1 \quad v_2| = \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}.$$

The trace of an element $\alpha \in \mathbb{F}_{p^n}$ is given by tr $\alpha = \alpha + \alpha^p + \alpha^{p^2} + ... + \alpha^{p^{n-1}}$. We denote by K the subgroup of $\mathbb{F}_{p^n}$, whose elements have the trace equal to zero:

$$K = \{\alpha \in \mathbb{F}_{p^n} :\ \mathrm{tr}\,\alpha = 0\}. \tag{1}$$

Definition. [17] The subgroup $G \subseteq \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ is called **extraordinary** if for any of its two elements g_1 and $g_2 \in G$, one has $|g_1 \quad g_2| \in K$.

Definition. [17] A square of order d, $S = \{A_1, ..., A_d\}$ is called **extraordinary** if there is $j \in \{1, 2, ..., d\}$ such that A_j is an extraordinary subgroup of $\mathbb{F}_d \times \mathbb{F}_d$.

Further we investigate the case $d = 2^3$. We consider the irreducible polynomial: $P(x) = x^3 + x + 1$, therefore the elements of $\mathbb{F}_8$ are: $\mathbb{F}_8$ =$\{$0, 1, μ, μ^2, μ^3, μ^4, μ^5, $\mu^6\}$, μ being a primitive element. The subgroup K defined by Eq. (1) is $K = \{0, \mu, \mu^2, \mu^4\}$.

Proposition. Suppose that $G \subseteq \mathbb{F}_8 \times \mathbb{F}_8$ is a subgroup which contains eight elements. Let v_1 be a nonzero element of G. Consider $v_2 \in \mathbb{F}_8 \times \mathbb{F}_8$ such that $|v_1 \quad v_2| = k$ with $k \in K$ and $k \neq 0$ (there is such v_2 according to Corollary 4.5 in Ref. [17]).

Then G is an extraordinary subgroup if and only if:

$$\text{i) } G = \mathbb{F}_8\, v \quad (v \neq 0,\ v \in \mathbb{F}_8 \times \mathbb{F}_8) \quad \text{or} \quad \text{ii) } G = \mathbb{Z}_2\, v_1 + (K k^{-1})\, v_2. \tag{2}$$

3. APPLICATION: THE CONSTRUCTION OF THE EXTRAORDINARY SUPERSQUARES OF ORDER 8

In this section we present an example of how one can use the extraordinary subgroups to generate extraordinary supersquares of order 8. Let us consider $v_1 = (\mu^6, 1)$ and $v_2 = (\mu^5, 1)$. Therefore $k = |v_1 \quad v_2| = \mu$. We apply the main result of Sec. 3, *i.e.* Eq. (2) and obtain

$$G = \{(0,0), (\mu^5,1), (\mu^6,\mu), (\mu,\mu^3), (\mu^6,1), (\mu,0), (0,\mu^3), (\mu^5,\mu)\}. \tag{3}$$

By using the definition of a supersquare given in Sec. 2, we obtain the supersquare of order 8 shown in Fig. 1, whose generating subgroup is the extraordinary one given by Eq. (3).

μ^6	7	4	7	8	4	8	3	3
μ^5	3	8	3	4	8	4	7	7
μ^4	7	4	7	8	4	8	3	3
μ^3	**1**	6	**1**	2	6	2	5	5
μ^2	3	8	3	4	8	4	7	7
μ	5	2	5	6	2	6	**1**	**1**
1	5	2	5	6	2	6	**1**	**1**
0	**1**	6	**1**	2	6	2	5	5
	0	1	μ	μ^2	μ^3	μ^4	μ^5	μ^6

Fig. 1 – An example of an extraordinary supersquare of order 8. The elements which are used for obtaining the extraordinary subgroup are $v_1 = (\mu^6, 1)$ and $v_2 = (\mu^5, 1)$. The generating extraordinary subgroup is denoted by bold red 1 and is given by Eq. (3).

4. THE GENERATION OF THE COMPLETE SET OF MUTUALLY UNBIASED BASES

In order to construct a complete set of mutually unbiased bases, one needs to generate the complete set of $d+1$ mutually orthogonal supersquares. For the generation of a set of mutually orthogonal supersquares it is sufficient to obtain the $d+1$

extraordinary subgroups such that the intersection of any two of these subgroups is the element zero according to Proposition 3.3 and Corollary 3.6 from Ref. [17]. Once we get the expressions of the $d+1$ extraordinary subgroups, we can construct the associated supersquares according to Sec. 3.

For the case $d = 8$, let us denote by a the generating extraordinary subgroup of the first supersquare, by b the second one,..., by i the ninth one. Further we use Eq. (2) for writing the nine extraordinary subgroups. We present in Fig. 2 an example of nine extraordinary subgroups whose unique intersection element is zero, this leading to the fact that the nine associated supersquares are mutually orthogonal. The element zero is denoted by a star, since belongs to all the subgroups.

μ^6	f	h	h	g	g	a	d	b
μ^5	c	h	h	f	b	c	a	d
μ^4	c	b	g	d	a	c	f	g
μ^3	e	g	e	b	d	g	f	a
μ^2	i	i	a	i	f	d	b	i
μ	h	a	d	f	h	b	e	e
1	c	d	b	a	f	c	e	e
0	*	i	e	i	h	c	g	i
	0	1	μ	μ^2	μ^3	μ^4	μ^5	μ^6

Fig. 2 – An example of nine extraordinary subgroups whose unique intersection element is zero. The extraordinary subgroup of Eq. (3) shown in Fig. 1 as bold 1 is denoted here by e. The MUBs obtained from this complete set of mutually orthogonal supersquares correspond to the structure with nine biseparable bases, *i.e.* the optimal one for quantum tomography.

After we have obtained the complete set of mutually orthogonal extraordinary supersquares, we follow the algorithm proposed by us for the construction of the complete set of MUBs [16]. This means that from each extraordinary supersquare, one generates a set of seven commuting operators. In the case of our example given in Sec. 4, the seven commuting operators associated to the extraordinary supersquare of Fig. 1 are:

$$\{Z\otimes Y\otimes Z; I\otimes Z\otimes Y; Z\otimes X\otimes X; Z\otimes Z\otimes Y; I\otimes X\otimes X; Z\otimes I\otimes I; I\otimes Y\otimes Z\},$$

where X, Y, and Z are the Pauli matrices.

The extraordinary subgroup of Eq. (3) shown in Fig. 1 as bold 1 is denoted by e in Fig. 2. For each set of commuting operators from each supersquare, we derive its set of common eigenvectors. The nine families of common eigenvectors represent the complete set of MUBs.

5. CONCLUSIONS

In this paper we have found the general expression of the extraordinary subgroups of $\mathbb{F}_8 \times \mathbb{F}_8$. These subgroups are of great importance for the construction of the most general set of MUBs for three-qubit systems. Namely, one has to obtain the complete set of mutually orthogonal supersqures, then the mutually unbiased operators are generated, and finally the set of their common eigenvectors that represent the MUBs.

The analysis of the three-qubits systems is difficult since there are four kinds of structures, *i.e.* possibilities of express the set of MUBs regarding the number of factorized bases, biseparable bases and nonseparable bases. Among these, one has to focus on the family that contain nine biseparable bases, since these are the optimal MUBs for quantum tomography. In Fig. 2, we have presented a complete set of mutually orthogonal supersquares, whose associated MUBs correspond to the structure with nine biseparable bases.

A. THE PROOF OF THE PROPOSITION PRESENTED IN SECTION 2

”$\Rightarrow$” There are two possible cases:

(i) $\exists\, u \in \mathbb{F}_8 \times \mathbb{F}_8$ such that $G \subseteq \mathbb{F}_8\, u$ or

(ii) $\forall\, u \in \mathbb{F}_8 \times \mathbb{F}_8$ one has $G \nsubseteq \mathbb{F}_8\, u$.

Case (i): Since G and $\mathbb{F}_8 u$ have eight elements, it means that $G = \mathbb{F}_8 u$. Since $v \in G \subseteq \mathbb{F}_8\, u$, we obtain $v \in \mathbb{F}_8\, u$; $\mathbb{F}_8 v \subseteq \mathbb{F}_8 u = G$. This leads to $G = \mathbb{F}_8\, v$.

Case (ii): We have now that $\forall u \in \mathbb{F}_8 \times \mathbb{F}_8 \Rightarrow G \nsubseteq \mathbb{F}_8\, u$. This means that $G \nsubseteq \mathbb{F}_8\, v_1$ or equivalent there exists $\tilde{v} \in G \backslash \mathbb{F}_8\, v_1$. From the condition $|v_1 \quad v_2| = k$, we obtain that $\{v_1, v_2\}$ is a basis in $\mathbb{F}_8 \times \mathbb{F}_8$. Let us write $\tilde{v}$ as $\tilde{v} = \lambda\, v_1 + \rho\, v_2$, where $\lambda, \rho \in \mathbb{F}_8$. Since G is an extraordinary subgroup, one has $|v_1 \quad \tilde{v}| \in K$ and since $\tilde{v} \notin \mathbb{F}_8\, v$ this leads to the fact that $\{v_1, \tilde{v}\}$ is a basis in $\mathbb{F}_8 \times \mathbb{F}_8$, therefore $|v_1 \quad \tilde{v}| \neq 0$. Let us denote by $\tilde{k}$ the following expression $|v_1 \quad \tilde{v}| = \tilde{k}$, where $\tilde{k} \in K$ and $\tilde{k} \neq 0$. We compute $|v_1 \quad \tilde{v}| = \lambda |v_1 \quad v_1| + \rho |v_1 \quad v_2| = \rho k$. This means $\rho = \tilde{k}\, k^{-1}$, *i.e.* $\tilde{v} = \lambda\, v_1 + \tilde{k}\, k^{-1}\, v_2$.

Further we apply Lemma 4.6 (b) from Ref. [17], where we replace v_2 by $\tilde{v}$ and obtain $G \subseteq K\tilde{k}^{-1}\, v_1 + K\tilde{k}^{-1}\, \tilde{v} = K\tilde{k}^{-1}\, (1+\lambda)\, v_1 + K\, k^{-1}\, v_2$. The number of elements of the set in the right hand side is 16. One has $K\, \tilde{k}^{-1} = \{0, 1, \tilde{k}, \tilde{k}^3\}$. In order to get an equality it is sufficient to choose $\lambda = 0$ and to keep only two elements from the set $K\, \tilde{k}^{-1}$, namely $\{0, 1\}$. This is equivalent to $G = \mathbb{Z}_2\, v_1 + (Kk^{-1})\, v_2$.

”$\Leftarrow$” (i) If $G = \mathbb{F}_8\, v$, then from Lemma 4.6 (a) from Ref. [17] we obtain that G is an extraordinary subgroup.

(ii) Suppose $G = \mathbb{Z}_2\, v_1 + (Kk^{-1})\, v_2$. One can easily check that G is a subgroup. Let g_1 and $g_2 \in \mathbb{Z}_2\, v_1 + (Kk^{-1})\, v_2$; this means that there are λ_1 and $\lambda_2 \in \mathbb{Z}_2$ and k_1, $k_2 \in K$ such that

$$g_1 = \lambda_1\, v_1 + k_1 k^{-1} v_2; \quad g_2 = \lambda_2\, v_1 + k_2 k^{-1} v_2.$$

We evaluate now

$$\begin{aligned}|g_1 \quad g_2| &= |\lambda_1 v_1 \quad k_2 k^{-1} v_2| + |k_1 k^{-1} v_2 \quad \lambda_2 v_1| \\ &= \lambda_1 k_2 k^{-1} k + k_1 k^{-1} k \lambda_2 = \lambda_1 k_2 + \lambda_2 k_1 \in K,\end{aligned}$$

i.e., G is an extraordinary subgroup.

Acknowledgements. The work of Iulia Ghiu was supported by the Romanian National Authority for Scientific Research through Grant PN-II-ID-PCE-2011-3-1012 for the University of Bucharest. The work of Cristian Ghiu has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU/159/1.5/S/132395.

REFERENCES

1. T. Durt, B-G Englert, I. Bengtsson, and K. Życzkowski, Int. J. Quantum Inf. **8**, 535 (2010).
2. P. Adam, V. A. Andreev, I. Ghiu, A. Isar, M. A. Man'ko, and V. I. Man'ko, J. Russ. Laser Res. **35**, 3 (2014).
3. P. Adam, V. A. Andreev, I. Ghiu, A. Isar, M. A. Man'ko, and V. I. Man'ko, J. Russ. Laser Res. **35**, 427 (2014).
4. K. S. Gibbons, M. J. Hoffman, andW. K. Wootters, Phys. Rev. A **70**, 062101 (2004).
5. A. B. Klimov, J. L. Romero, G. Björk, L. L. Sánchez-Soto, J. Phys. A: Math. Theor. **40**, 3987 (2007).
6. A. Klappenecker and M. Rötteler, *Constructions of Mutually Unbiased Bases*, Finite Fields and Applications, 7th International Conference, Fq7, Lecture Notes in Computer Science, vol. 2948, Springer, pp. 137, 2003, available at arXiv:quant-ph/0309120.
7. I. Bengtsson, *Three Ways to Look at Mutually Unbiased Bases*, Foundations of Probability and Physics - 4. Proceedings held at Växjo, Sweden, 4-9 June 2006. AIP Conference Proceedings Volume 889. Edited by Guillaume Adenier, Christopher A. Fuchs, and Andrei Yu. Khrennikov. Melville, NY: American Institute of Physics, p.40-51, 2006, available at arXiv:quant-ph/0610216.
8. I. Ghiu, J. Phys.: Conf. Ser. **338**, 012008 (2012).
9. I. Ghiu, Phys. Scr. **T153**, 014027 (2013).
10. L. Pawela, P. Gawron, Z. Puchala, J. Sladkowski, PLoS ONE **8**, e64694 (2013).
11. W. K. Wootters, Found. Phys. **36**, 112 (2006).
12. T. Paterek, B. Dakic, C. Brukner, Phys. Rev. A **79**, 012109 (2009).
13. T. Paterek, M. Pawlowski, M. Grassl, C. Brukner, Phys. Scr. **T140**, 014031 (2010).
14. J. L. Hall and A. Rao, Phys. Rev. A **83**, 036101 (2011).
15. J. L. Hall and A. Rao A, J. Phys. A: Math. Theor. **43**, 135302 (2010).
16. I. Ghiu and C. Ghiu, Rep. Math. Phys. **73**, 49 (2014).
17. C. Ghiu and I. Ghiu, Cent. Eur. J. Math. **12**, 337 (2014).