Reply to "Comment on 'Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models' "

Tomasz Paterek,[1] Borivoje Dakić,[2,3] and Časlav Brukner[2,3]

[1]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543 Singapore, Singapore*

[2]*Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Wien, Austria*

[3]*Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Wien, Austria*

(Received 28 February 2011; published 30 March 2011)

In this Reply to the preceding Comment by Hall and Rao [Phys. Rev. A **83**, 036101 (2011)], we motivate terminology of our original paper and point out that further research is needed in order to (dis)prove the claimed link between every orthogonal Latin square of order being a power of a prime and a mutually unbiased basis.

DOI: 10.1103/PhysRevA.83.036102 PACS number(s): 03.65.Ta, 02.10.Ox

The comment of Hall and Rao [1] deals with one specific part of our work [2]: the algorithm to generate mutually unbiased bases (MUBs) from mutually orthogonal Latin squares (MOLS) *in dimensions being a power of a prime*. Other parts of our work include construction of the algorithm for other dimensions, constraints on the number and form of MUBs, and development of efficient hidden-variable models related to MUBs.

One of the points the authors comment upon is that the algorithm is based on finite fields rather than on MOLS. Indeed, for prime-power dimensions we explicitly use multiplication and addition in the field to construct MUBs. For other dimensions, however, there is no finite field with corresponding number of field elements and this is why we suggest to build MUBs from MOLS.

In their abstract the authors write that they show "the algorithm only works for particular sets of orthogonal Latin squares" [1]. This is in response to our claim that we "link every MOLS of order being a power of a prime with a MUB" [2]. While we recognize that this claim remains a conjecture, it is in fact not disproved in the comment as the authors themselves mention below their Eq. (9).

This work is supported by the National Research Foundation and the Ministry of Education in Singapore, by the EU project QESSENCE, and by the Austrian Science Foundation FWF within Project No. P19570-N16, SFB, and CoQuS No. W1210-N16.

[1] J. L. Hall and A. Rao, Phys. Rev. A **83**, 036101 (2011).

[2] T. Paterek, B. Dakić, and Č. Brukner, Phys. Rev. A **79**, 012109 (2009).

Comment on "Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models"

Joanne L. Hall* and Asha Rao†

School of Mathematical and Geospatial Sciences, RMIT University, GPO Box 2476V, Melbourne, 3001, Australia

(Received 15 November 2010; published 30 March 2011)

In a recent article Paterek, Dakić, and Brukner [Phys. Rev. A **79**, 012109 (2009)] show an algorithm for generating mutually unbiased bases from sets of orthogonal Latin squares. They claim that this algorithm works for every set of orthogonal Latin squares. We show that the algorithm only works for particular sets of orthogonal Latin squares. Furthermore, the algorithm is a more readable version of work previously published [Phys. Rev. A **70**, 062101 (2004)].

DOI: 10.1103/PhysRevA.83.036101 PACS number(s): 03.65.Ta, 02.10.Ox

I. INTRODUCTION

In a recent article Paterek, Dakić, and Brukner provide an algorithm for generating complete sets of mutually unbiased bases (MUBs) from mutually orthogonal Latin squares (MOLS) [1]. MUBs are a mathematical structure encapsulating the concept of complementarity which is at the core of quantum theory. Given two MUBs, a measurement in one basis leaves complete uncertainty as to the outcome of a measurement over the second basis. This feature is used in quantum state tomography [2] and quantum cryptography [3]. The maximum number of MUBs in $\mathbb{C}^d$ is $d+1$ [2]. A set of $d+1$ MUBs is called *complete*. There are constructions of complete sets of MUBs when d is a prime power [4], it is however unknown if complete sets of MUBs exist in nonprime power dimensions. It has been conjectured that complete sets of MUBs exist in $\mathbb{C}^d$ if and only if a complete set of MOLS of side length d also exists [5]. Thus concrete connections between MUBs and MOLS are useful.

There are two points that we comment upon.

(1) The construction of MUBs given in [1] is a specific case of a construction already published in [6]. The construction as given in [1] is however much more readable.

(2) The construction given by [1] is based on Galois fields, not MOLS as stated in the title.

II. SAME AS A CONSTRUCTION ALREADY PUBLISHED

Section V [1] states "we prove this result in a simple way related to [6]." It is better to state "we prove the construction of [6] in a simple way."

We detail the construction as given in Secs. III and IV of [6] and show that it is the same as the construction [1].

The basic operators used are generalizations of the Pauli operators as given in [7]

$$Z_d|j\rangle = \omega_d^j|j\rangle, \tag{1}$$

$$X_d|j\rangle = |j+1\rangle. \tag{2}$$

Gibbons, Hoffman, and Wootters [6] generate lines in "discrete phase space" using the equation

$$a \odot x \oplus b \odot y = c, \tag{3}$$

where $\odot$ and $\oplus$ denote multiplication and addition in the field. Thus on choosing $c=0$ a striation is defined by the pair (a,b) (scalar multiples define the same striation), with points defined as pairs (x,y), and lines as sets of pairs that satisfy Eq. (3). Two bases $E=\{e_1,\ldots,e_n\}$ and $F=\{f_1,\ldots,f_n\}$ are chosen for $\mathbb{F}_{p^n}$ such that F is a multiple of the dual basis of E, $f_i = w\bar{e}_i$, $w \in \mathbb{F}_{p^n}$. For each striation choose a point (p,q) on the line which contains $(0,0)$. Let

$$T_{xy} = X_n^{x_1} Z_n^{y_1} \otimes X_n^{x_n} Z_n^{y_n}, \tag{4}$$

where $x_i = \mathrm{tr}(xw^{-1}f_i) = \mathrm{tr}(x\bar{e}_i)$, $y_i = \mathrm{tr}(ywe_i)$, and $\otimes$ is the Kronecker product. The MUBs are then the eigenvectors of the chosen T_{xy}.

Paterek, Dakić, and Brukner generate sets of commuting operators using the elements of a net constructed from the MOLS [1]. The eigenvectors of the sets of commuting operators form a complete set of MUBs [7]. Two constructions are given, one for d a prime, and one for d a power of a prime. However when we look deeper into the construction we find that the net is not actually used, but pairs (n,m) which satisfy the equation

$$n = a \odot m \oplus b. \tag{5}$$

When generating MUBs only the first column of the net is used and thus requires that either $(a,b)=(0,1)$ or $b=0$. In prime dimensions let $S_{mn} = X_d^m Z_d^n$. For $d=p^r$ a power of a prime, let $E=\{e_1,e_2,\ldots,e_r\}$ and $\bar{E}=\{\bar{e}_1,\bar{e}_2,\ldots,\bar{e}_r\}$ be dual bases for $\mathbb{F}_d$. Then let

$$S_{mn} = X_p^{m_1} Z_p^{n_1} \otimes X_p^{m_2} Z_p^{n_2} \otimes \cdots X_p^{n_r} Z_p^{n_r}, \tag{6}$$

where

$$m_i = \mathrm{tr}(me_i) \quad \text{and} \quad n_i = \mathrm{tr}(n\bar{e}_i). \tag{7}$$

The MUBs are then the eigenvectors of the chosen S_{mn}.

It is clear that for $x=m, x_i=m_i$. For $y=n$, if $w=1$ then $y_i=n_i$. Thus the proof given in [1] is a special case of that given in [6].

The presentation in [1] is much easier to follow. With only a minor change (the introduction of the scalar w) the proof in [1] may be extended to include all cases covered by [6]; and thus may be considered a simpler proof of a special case.

III. NOT BASED ON MOLS

In Sec. I of [1] Paterek, Dakić, and Brukner state that they "link every OLS of order being a power of a prime with a

*joanne.hall@rmit.edu.au
†asha@rmit.edu.au

MUB." It has been conjectured that a complete set of MUBs exists in $\mathbb{C}^d$ if and only if a complete set of OLS of side length d also exists [5]. This remains a conjecture. The link shown is actually between a particular family of MOLS which are generated using a Galois field.

Paterek, Dakić, and Brukner show an algorithm for finding sets of pairs (m,n) such that the operators S_{mn} commute. Take S_{mn} with "mn taken from the first column of the net," which has been generated from a set of orthogonal Latin squares.

Then using Theoram 3.2 from [7]: "If there is a set of orthogonal unitary matrices, which can be partitioned into M subsets of d commuting operators," the eigenbases of the commuting matrices are MUBs.

In Sec. IV of [1] Paterek, Dakić, and Brukner, state "the orthogonal Latin square and the net are generated by the formula." Thus the construction uses a particular set of MOLS for each d. However there exist several nonequivalent complete sets of MOLS of many orders, see [8].

The construction of MOLS and proof of commuting operators in [1] is entirely dependent on properties of Galois fields. Operators S_{mn} and $S_{m'n'}$ commute if and only if they are from the same row of the first column of the net. This property is given algebraically: S_{mn} and $S_{m'n'}$ commute if and only if

$$\vec{m}\cdot\vec{n}' - \vec{m}'\cdot\vec{n} = 0 \bmod p. \tag{8}$$

Using Eq. (8) in [1]

$$\mathrm{tr}(m \odot n') - \mathrm{tr}(m' \odot n) = 0. \tag{9}$$

While this condition may be met by sets of OLS which are not defined by Eq. (3), the arguments presented in [1] fail to show this. Galois fields are used to construct both the orthogonal Latin squares and the mutually unbiased bases. The construction of the OLS is an unnecessary step in constructing this set of MUBs.

Commutation is shown in [6] using only properties of fields. Gibbons, Hoffman, and Wootters [6] use the term discrete phase space and make no mention of MOLS or any other combinatorial object, though they do give the axioms for an affine plane as "the usual rules governing lines."

Subsequent work has been done assuming that this construction is based on MOLS. Paterek, Pawlowski, Grassl, and Brukner show two MOLS of order 10, which when using the previously mentioned construction produce operators which do not commute (Sec. IV in [9]). Given the presented finding this is not surprising as there is no Galois field of size 10 (see, e.g., [10]).

IV. CONCLUSION

The construction as described in [1] is therefore based on Galois fields, and not MOLS.

This construction is not without interest as it is not equivalent to other constructions. For instance, the constructions based on Galois fields given in [4] only work for odd prime powers. A Galois ring is then required for powers of 2. The construction as presented in [1] constructs complete set of MUBs in both odd and even prime power dimensions using a Galois field.

The construction of complete sets of MUBs as presented in [1] is interesting and an important idea in the theory of MUBs. It should be noted that it is a simpler presentation of a previously published result. The construction is based on Galois fields, not MOLS, and therefore has no bearing on the conjectured connection between MUBs and MOLS.

[1] T. Paterek, B. Dakić, and Č. Brukner, Phys. Rev. A **79**, 012109 (2009).
[2] W. Wootters and B. Fields, Ann. Phys. **191**, 363 (1989).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] A. Klappenecker and M. Rötteler, Lecture Notes Comput. Sci. **2948**, 137 (2003).
[5] M. Saniga, M. Planat, and H. Rosu, J. Opt. B **6**(9), L19 (2004).
[6] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters, Phys. Rev. A **70**, 062101 (2004).
[7] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
[8] C. J. Colbourn and J. H. Dinitz, J. Stat. Planning Inference **95**, 9 (2001).
[9] T. Paterek, M. Pawlowski, M. Grassl, and Č. Brukner, Phys. Scr. T **140**, 014031 (2010).
[10] J. B. Fraleigh, *A First Course in Abstract Algebra*, 6th ed. (Addison-Wesley, Reading, MA, 1999).