Mutually orthogonal Latin squares from the inner products of vectors in mutually unbiased bases

2010 J. Phys. A: Math. Theor. 43 135302

(http://iopscience.iop.org/1751-8121/43/13/135302)

IOP PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL

J. Phys. A: Math. Theor. **43** (2010) 135302 (12pp) doi:10.1088/1751-8113/43/13/135302

Mutually orthogonal Latin squares from the inner products of vectors in mutually unbiased bases

Joanne L Hall and Asha Rao

School of Mathematical and Geospatial Sciences, RMIT University, Melbourne 3001, Australia

E-mail: joanne.hall@rmit.edu.au and asha@rmit.edu.au

Received 7 July 2009, in final form 20 January 2010
Published 10 March 2010
Online at stacks.iop.org/JPhysA/43/135302

Abstract

Mutually unbiased bases (MUBs) are important in quantum information theory. While constructions of complete sets of $d + 1$ MUBs in $\mathbb{C}^d$ are known when d is a prime power, it is unknown if such complete sets exist in non-prime power dimensions. It has been conjectured that complete sets of MUBs only exist in $\mathbb{C}^d$ if a maximal set of mutually orthogonal Latin squares (MOLS) of side length d also exists. There are several constructions (Roy and Scott 2007 *J. Math. Phys.* **48** 072110; Paterek, Dakić and Brukner 2009 *Phys. Rev.* A **79** 012109) of complete sets of MUBs from specific types of MOLS, which use Galois fields to construct the vectors of the MUBs. In this paper, two known constructions of MUBs (Alltop 1980 *IEEE Trans. Inf. Theory* **26** 350–354; Wootters and Fields 1989 *Ann. Phys.* **191** 363–381), both of which use polynomials over a Galois field, are used to construct complete sets of MOLS in the odd prime case. The MOLS come from the inner products of pairs of vectors in the MUBs.

PACS numbers: 03.65.Fd, 02.10.Ox

1. Introduction

Mutually unbiased bases (MUBs) are an important tool in quantum physics. It is conjectured that the existence of a complete set of MUBs in $\mathbb{C}^d$ is linked to the existence of a complete set of mutually orthogonal Latin squares (MOLS) of side length d [1]. While there are several constructions of complete sets of MUBs from complete sets of specific types of MOLS [12, 13], no one seems to have gone from MUBs to MOLS. In this paper we show a way to construct MOLS from MUBs in odd prime dimensions, using the inner product vectors in the MUBs.

A basis for $\mathbb{C}^d$ is *orthonormal* if all basis vectors are orthogonal and of unit length. Two orthonormal bases $\mathcal{B}$ and $\mathcal{B}'$ in $\mathbb{C}^d$ are called *mutually unbiased* if and only if $|\langle\phi|\psi\rangle|^2 = 1/d$ for all $\phi \in \mathcal{B}$ and $\psi \in \mathcal{B}'$.

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 exploited in a cryptographic protocol [2] to securely distribute secret keys over a public channel. Thus MUBs may be a key feature in quantum cryptography in the future. MUBs are also used in quantum state determination—they provide a way to design the optimal set of measurements for determining an ensemble's state [3]. Sets of $d + 1$ MUBs in $\mathbb{C}^d$ are called *complete* and are known to exist if d is a prime power. In the non-prime power case, it is not known if complete sets of MUBs exist—the question is open even in the case $d = 6$.

Much work has been done investigating the structure and constructing sets of MUBs using various mathematical objects. Constructions of complete sets of MUBs from the early 1980s used complex periodic sequences [5] and commutative subsets of Hermitian matrices [6]. Weil sums over Galois fields and Galois rings were used in [3, 7] to generalize these constructions to all prime powers. More recent constructions use orthogonal unitary matrices [8] and discrete phase space [9]. However, the aforementioned constructions rely on the properties of primes and prime powers and hence do not generalize to constructions in non-prime power dimensions [10].

There can be a maximum of $d - 1$ mutually orthogonal Latin squares (MOLS) of side length d [4, section 3.2, theorem 3.25]. Sets of $d - 1$ MOLS of side length d are said to be *complete* and are known to exist if d is a prime power. In the case of MOLS of side length 6, it can be shown that there is no complete set—in fact only one Latin square of side length 6 exits [4, theorem 3.39].

Complete sets of MOLS are equivalent to finite affine planes. There has been a complete classification of Affine planes into the seven Lenz–Bartolli groups [11] but not all of these groups have known examples. The Desarguesian planes are constructed from cosets in a vector space over a finite field. Paterek *et al* [12] use MOLS equivalent to the Desarguesian planes to construct MUBs and claim that given a complete set of MOLS, a complete set of MUBs can be constructed. All known constructions of complete sets of MOLS (and therefore affine planes) use Galois fields in some way [11, p 219]. For further information on constructions of planes and MOLS we refer to [11]. As there is much more known about Latin squares than MUBs, there has been a greater focus on constructing sets of MUBs from sets of MOLS. We take the opposite approach and construct complete sets of MOLS from complete sets of MUBs in the case d an odd prime.

Roy and Scott [13, theorem 4.2] show that given a planar function a complete set of MUBs can be constructed. The planar functions are used to construct the vectors of the set of MUBs. Our construction of MOLS from MUBs could be considered a converse of the [13] construction, in that it relies on planar functions. However, our construction does not rely on planar functions having generated the vectors in the set of MUBs, but on planar functions generating the inner products between these vectors. Furthermore, in this paper we also construct MOLS from a set of MUBs, where the set of MUBs are not generated by planar functions.

Here we show a way to construct MOLS from MUBs in the odd prime case. We conjecture that this construction will work for any MUBs constructed using characters of polynomials. In section 2, we detail the necessary definitions and preliminary results. Section 3 contains two examples constructing complete sets of MOLS from complete sets of MUBs. Section 4 gives a proof that this construction works for the two different MUBs' constructions for all odd prime dimensions.

2. Preliminaries

2.1. Mutually unbiased bases (MUBs)

A basis for $\mathbb{C}^d$ is *orthonormal* if all basis vectors are orthogonal and of unit length.

Definition 1. *Two orthonormal bases $\mathcal{B}$ and $\mathcal{B}'$ of the space $\mathbb{C}^d$ are mutually unbiased if and only if they satisfy*

$$|\langle\phi|\psi\rangle|^2 = \frac{1}{d} \tag{1}$$

for all $\phi \in \mathcal{B}$ and $\psi \in \mathcal{B}'$.

Let $N(d)$ be the maximum number of MUBs in $\mathbb{C}^d$.

Theorem 1 [3, equation (9)]**.** $N(d) \leqslant d + 1$.

Thus we call a set of $d + 1$ MUBs in $\mathbb{C}^d$ a complete set of MUBs.

Theorem 2 [7, lemma 3]**.** *Let $d = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ be the prime power decomposition of d. Then*

$$N(d) \geqslant \min\left\{N\left(p_1^{a_1}\right), N\left(p_2^{a_2}\right), \dots, N\left(p_r^{a_r}\right)\right\}. \tag{2}$$

This is referred to as the 'reduce to prime powers' construction.

2.2. Mutually orthogonal Latin squares (MOLS)

A *Latin square* is an $n \times n$ array, with each of n symbols appearing exactly once in each row and each column. A *striation* is a partition of a set of points into a set of d lines which are parallel. Two striations A and B of the set X are *unbiased* if each line of partition A contains exactly one element in common with each line of partition B. We are working with a set of n^2 cells, which have been arranged into an $n \times n$ array. A Latin square represents three *mutually unbiased striations*, the set of rows (the row striation), the set of columns (the column striation) and the sets of cells which contain the same symbol (the Latin striation).

Two Latin squares A and B of the same order are *orthogonal* if the Latin striations of the squares are unbiased. Mutually orthogonal Latin squares (MOLS) are pairwise orthogonal. A set of s MOLS is equivalent to $s + 2$ mutually unbiased striations: the row striation, column striation and s Latin striations. Each Latin square represents the same row and column striations, as they have the same arrangement of cells. Each of the s MOLS have a different arrangement of symbols within the cells, and hence represent different Latin striations.

Many of the counting theorems for MOLS are similar to those for MUBs. Let $M(d)$ be the maximum number of MOLS of side length d.

Theorem 3 ([4, theorem 3.25])**.** *For $d > 1$, $M(d) \leqslant d - 1$.*

Thus if we are counting striations instead of MOLS, theorem 3 would be entirely analogous to theorem 1.

Theorem 4 ([4, theorem 3.28])**.** *For $d = p^n$ a complete set of MOLS exists.*

The following is analogous to theorem 2.

Theorem 5 ([4, theorem 3.26]). $M(xy) \geqslant \min\{M(x), M(y)\}$.

The combinatorial similarities between projective planes and complete sets of MUBs have been noted in the conjecture in [1] and since there exist (projective and affine) planes of order n if and only if there exist $n-1$ MOLS of side length n [11], we can reframe the conjecture in [1] as follows:

Conjecture 1. *The non-existence of a complete set of MOLS of side length d implies the non-existence of a complete set of MUBs in* $\mathbb{C}^d$.

In addition, the Bruck–Ryser–Chowla theorem [14] shows that complete sets of MOLS cannot exist for a certain set of composite sizes, in particular the small values of 6, 14, 21. It has also been shown through exhaustive computation that there is no complete set of MOLS of side length 10 [15]. Thus, if there is a concrete connection between MOLS and MUBs, then results such as the Bruck–Ryser–Chowla theorem could be used to show non-existence of complete sets of MUBs in certain dimensions.

3. Two examples of constructing MOLS from MUBs

Given a complete set of MUBs we can construct a complete set of MOLS in odd prime dimensions. This construction will be shown to work for two known constructions of MUBs (theorems 6 and 7). This could be considered the converse of known constructions which have focused on constructing MUBs from MOLS [12, 13, 16]. Our construction exploits the properties of the polynomials which generate the MUBs. We illustrate the construction using an example in $\mathbb{C}^3$.

The following result is obvious and important in the construction.

Lemma 1. *Let* $\omega_p = \mathrm{e}^{\frac{2i\pi}{p}}$.

$$\sum_{k=1}^{np} \omega_p^k = 0, \qquad n \in \mathbb{N}. \tag{3}$$

When p is a prime, this summation is unique.

We begin with a known construction of complete sets of MUBs.

3.1. Wootters and Fields type MUBs

Let $\mathbb{F}_q$ be the Galois field of order q.

Theorem 6 ([3] extended in [7, theorem 2]). *Let p be an odd prime with* $p^n = q$. *For* $a, b \in \mathbb{F}_q$, *the set of vectors given by*

$$w_{ab} = \frac{1}{\sqrt{q}}\left(\omega_p^{\mathrm{tr}(ax^2+bx)}\right)_{x\in\mathbb{F}_q} \tag{4}$$

and the standard basis form a complete set of MUBs in $\mathbb{C}^q$.

In the case $q = 3$ the complete set of MUBs is

S	W_0	W_1	W_2
$s_0 = \begin{pmatrix}1\\0\\0\end{pmatrix}$	$w_{00} = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\1\end{pmatrix}$	$w_{10} = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega\\\omega\end{pmatrix}$	$w_{20} = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega^2\\\omega^2\end{pmatrix}$
$s_1 = \begin{pmatrix}0\\1\\0\end{pmatrix}$	$w_{01} = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega\\\omega^2\end{pmatrix}$	$w_{11} = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega^2\\1\end{pmatrix}$	$w_{21} = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\\omega\end{pmatrix}$
$s_2 = \begin{pmatrix}0\\0\\1\end{pmatrix}$	$w_{02} = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega^2\\\omega\end{pmatrix}$	$w_{12} = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\\omega^2\end{pmatrix}$	$w_{22} = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega\\1\end{pmatrix}$

We call S the standard basis, and W_0, W_1, W_2 the non-standard bases where $\omega = \mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}$. Using lemma 1, the first standard basis vector may be written as

$$s_0 = \begin{pmatrix}1\\0\\0\end{pmatrix} = \frac{1}{3}\begin{pmatrix}1+1+1\\1+\omega+\omega^2\\1+\omega^2+\omega\end{pmatrix}. \tag{5}$$

This can be written as a linear combination of various non-standard bases vectors, e.g.

$$\begin{aligned} s_0 &= \frac{1}{\sqrt{3}}\left(\frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\1\end{pmatrix} + \frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega\\\omega^2\end{pmatrix} + \frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega^2\\\omega\end{pmatrix}\right) \\ &= \frac{1}{\sqrt{3}}(w_{00} + w_{01} + w_{02}). \end{aligned} \tag{6}$$

In all s_0 can be written as six different linear combinations of non-standard bases vectors:

$$s_0 = \frac{1}{\sqrt{3}}(w_{00} + w_{01} + w_{02}) \tag{7}$$

$$= \frac{1}{\sqrt{3}}(w_{10} + w_{11} + w_{12}) \tag{8}$$

$$= \frac{1}{\sqrt{3}}(w_{20} + w_{21} + w_{22}). \tag{9}$$

$$s_0 = \frac{1}{\sqrt{3}}(w_{00} + w_{10} + w_{20}) \tag{10}$$

$$= \frac{1}{\sqrt{3}}(w_{01} + w_{11} + w_{21}) \tag{11}$$

$$= \frac{1}{\sqrt{3}}(w_{02} + w_{12} + w_{22}). \tag{12}$$

Then ignoring the scalar $\frac{1}{\sqrt{3}}$, the vectors may be arranged in an array (13), with the row striation representing the vectors which appear in linear combinations of (7)–(9), and the column striation representing the vectors which appear in the linear combinations of (10)–(12).

w_{00}	w_{01}	w_{02}
w_{10}	w_{11}	w_{12}
w_{20}	w_{21}	w_{22}

(13)

This array (13) is the structure we will use to build Latin squares. Since we have the row and column striations, we now require a further striation to give the symbols for the Latin square.

Finding three representations of s_1 requires using weights. Note that we have used ω_3 to clearly differentiate ω from w:

$$s_1 = \tfrac{1}{3}\left(w_{00} + \omega_3^2 w_{01} + \omega_3 w_{02}\right) \tag{14}$$

$$= \tfrac{1}{3}\left(\omega_3^2 w_{10} + \omega_3 w_{11} + w_{12}\right) \tag{15}$$

$$= \tfrac{1}{3}\left(\omega_3 w_{20} + w_{21} + \omega_3^2 w_{22}\right). \tag{16}$$

Here we get the same vectors in each of the linear combinations as in (7)–(9) which represent the rows striation. This is unsurprising as any vector may be written as a linear combination of the vectors in each base. This time there are weights, which when arranged according the array (13), gives an interesting pattern, in this case of a Latin square:

Weights

1	ω^2	ω
ω^2	ω	1
ω	1	ω^2

(17)

The next three representations of s_1 give us another mutually unbiased striation:

$$s_1 = \tfrac{1}{3}\left(w_{00} + \omega_3 w_{11} + \omega_3^2 w_{22}\right) \tag{18}$$

$$= \tfrac{1}{3}\left(\omega_3^2 w_{01} + w_{12} + \omega_3 w_{20}\right) \tag{19}$$

$$= \tfrac{1}{3}\left(\omega_3 w_{02} + \omega_3^2 w_{10} + w_{21}\right). \tag{20}$$

The groupings according to (18)–(20) can be organized into the Latin square below (21). The vectors used in (18) are represented by ♡, the vectors used in (19) are represented by ♢ and the vectors used in (20) are represented by ♣. This gives us a Latin square in the vectors. The weights form the same arrangement as (14)–(16), which can be seen in (17). The weights Latin square and vectors Latin square are orthogonal to each other:

Vectors

♡	♢	♣
♣	♡	♢
♢	♣	♡

(21)

Repeating this for a further standard basis vector we get another three equations which form the row striations and three equations which form a Latin striation in the vectors, and in the weights. The two vector Latin striations are orthogonal, as are the two weights Latin striations:

	Vectors			Weights		
s_1	♡	♢	♣	1	ω^2	ω
	♣	♡	♢	ω^2	ω	1
	♢	♣	♡	ω	1	ω^2
s_2	♡	♢	♣	1	ω	ω^2
	♢	♣	♡	ω^2	1	ω
	♣	♡	♢	ω	ω^2	1

(22)

By using the linear combinations of the vectors for the MUBs construction of theorem 6 we have constructed a complete set of MOLS. This construction also yields a complete set of MOLS in the weights.

3.2. Alltop type MUBs

There are other constructions of complete sets of MUBs. The following construction has been shown to be unitarily equivalent to theorem 6 [17]. However, it behaves slightly differently with our linear combinations.

Theorem 7 ([5] extended in [7, theorem 1]). *Let p be an odd prime $\geqslant 5$, with $p^n = q$. For $a, b \in \mathbb{F}_q$, the set of vectors given by*

$$v_{ab} = \frac{1}{\sqrt{q}}\left(\omega_p^{\mathrm{tr}((x+a)^3+b(x+a))}\right)_{x\in\mathbb{F}_q} \tag{23}$$

and the standard basis form a complete set of MUBs in $\mathbb{C}^q$.

When using the construction of theorem 7, a complete set of MOLS is constructed in the vectors of the linear combinations, but the weights form Butson Hadamard Matrices (see [18, section 4]). For example for $q = 5$, we get the following set of MOLS and Butson Hadamard matrices:

	Vectors					Weights				
s_1	♡	◇	♣	♠	△	ω^4	ω^3	ω^2	ω	1
	◇	♣	♠	△	♡	ω^3	ω	ω^4	ω^2	1
	♣	♠	△	♡	◇	ω^4	ω	ω^3	1	ω^2
	♠	△	♡	◇	♣	ω^4	1	ω	ω^2	ω^3
	△	♡	◇	♣	♠	1	1	1	1	1
s_2	♡	◇	♣	♠	△	ω^2	1	ω^3	ω	ω^4
	♣	♠	△	♡	◇	ω^2	ω^4	ω	ω^3	1
	△	♡	◇	♣	♠	ω^4	1	ω	ω^2	ω^3
	◇	♣	♠	△	♡	1	1	1	1	1
	♠	△	♡	◇	♣	ω^2	ω	1	ω^4	ω^3
s_3	♡	◇	♣	♠	△	ω^3	1	ω^2	ω^4	ω
	♠	△	♡	◇	♣	ω^3	ω^4	1	ω	ω^2
	◇	♣	♠	△	♡	1	1	1	1	1
	△	♡	◇	♣	♠	ω	1	ω^4	ω^3	ω^2
	♣	♠	△	♡	◇	ω^3	ω	ω^4	ω^2	1
s_4	♡	◇	♣	♠	△	ω	ω^2	ω^3	ω^4	1
	△	♡	◇	♣	♠	1	1	1	1	1
	♠	△	♡	◇	♣	ω	1	ω^4	ω^3	ω^2
	♣	♠	△	♡	◇	ω	ω^4	ω^2	1	ω^3
	◇	♣	♠	△	♡	ω^2	ω^4	ω	ω^3	1

(24)

Again we have exploited the linear combinations of the vectors in a complete set of MUBs to produce a complete set of MOLS. In the next section, we prove that the complete set of MOLS will always be generated for the theorem 6 and theorem 7 constructions in odd prime dimensions.

4. Algebraic construction of MOLS

4.1. MOLS from planar functions

The construction of theorem 6 uses planar functions to construct the vectors of the set of MUBs. Let G and H be arbitrary finite groups, written additively, but not necessarily commutative. A function $f : G \to H$ is called a planar function if for every non-identity $a \in G$ the functions $\Delta_{f,a} : x \mapsto f(a+x) - f(x)$ and $\nabla_{f,a} : x \mapsto f(x) + f(x+a)$ are bijections [20].

Planar functions [11] can be used to construct complete sets of MOLS (see theorem 8 below). However, there are MOLS that cannot be constructed via a planar function, for example see the construction of affine planes [21]. Planar functions have also been used to construct complete sets of MUBs [13]. Note that quadratic functions are planar for all finite fields [19].

The vectors of theorem 7 are not constructed using planar functions. However, the inner product between any two (non-standard basis) vectors in the set of MUBs in theorem 7 can be calculated using a quadratic function, which is planar. Both the vectors and the inner product vectors (definition 2) of the theorem 6 construction are from quadratic functions. The key to our construction is the functions which describe the inner products.

Definition 2. *The inner product vector, $IPV[u, w]$, of two vectors u, w can be generated by $IPV[u, w]_i = v_i = u_i\overline{w_i}$ where $v = (v_1, v_2, \ldots, v_n)$, $u = (u_1, u_2, \ldots, u_n)$ and $w = (w_1, w_2, \ldots, w_n)$.*

In both the theorems 6 and 7 constructions, vector u is constructed from a function f_u by $u = \left(\omega_p^{\mathrm{tr}(f_u(x))}\right)_{x\in\mathbb{F}_p}$. Hence we may call f_u the function of u, and consequently, the inner product vector can be constructed from the function $f_v(x) = f_u(x) - f_w(x)$ by

$$IPV[u, w] = \left(\omega_p^{\mathrm{tr}(f_u(x)-f_w(x))}\right)_{x\in\mathbb{F}_p}. \tag{25}$$

The inner product is easily recovered from the inner product vector by summing the entries in the inner product vector.

Given that we are only working with prime dimensions, the trace map is an identity function, and we are really looking at features of the polynomials.

Theorem 8 ([20, theorem 5.3])**.** *Let f be a planar function on the group G, and let $a \in G^* = G\backslash 0$. Then $L_a(x, y) = f(x) - f(x-a) + y$, $a \neq 0$ constructs a Latin square. The set $L_a : a \in G^*$ forms a complete set of MOLS.*

We can take a variation on this, interchanging rows and columns (hence $L_a(y, x)$) and permuting the symbols by multiplication by 3. For $d = 5$, let $f(x) = x^2$. Then $L_a(y, x) = 3(f(x) - f(x-a) + y)$ generates the MOLS constructed from the theorem 6 construction (array (22)), and $L_a(y, x) = f(x) - f(x-a) + y$ for the theorem 7 construction (array (24)). However, this is not how they have been constructed in the previous section.

Theorem 9 ([20, theorem 5.2])**.** *The MOLS generated from $f(x)$ and $f(ax + b) + c$ are equivalent.*

Therefore any MOLS generated from any quadratic equations are equivalent. The MUBs generated from the theorem 6 and theorem 7 constructions have equivalent sets of inner product vectors. Thus, they form the same set of MOLS. The two constructions are equivalent as their sets of inner product vectors are equivalent. This is not surprising given the result of [17] that the two constructions are equivalent. Reference [17] shows this by providing a unitary mapping for the vectors in theorem 7 to the vectors in theorem 6. Looking at inner product vectors may yield a more general way of determining equivalences of sets of MUBs.

4.2. Proof of our construction of MOLS

There are p standard basis vectors; hence for each $z \in \mathbb{F}_p$ there is a standard basis vector s_z. Any vector may be written as a linear combination of other vectors. Thus,

$$s_z = \sum_{i \in P} m_{iz} v_i \tag{26}$$

where P is some set of vector labels, v_i is the vector and m_{iz} is the weight assigned to that vector in linear combinations which sum to s_z.

The outline of the construction and proof: for each $z \in \mathbb{F}_p$ we choose the weight that will be assigned to each vector. We then choose the vectors that will (with their weights) form a linear combination that represents s_z. We show that for each z we produce the same 'row' striation. For each z we also produce another striation. These striations are unbiased to the 'row' striation and to each other. We call the striation associated with $z = 0$ the 'column' striation and the ones associated with $1 \leqslant z \leqslant p-1$ the Latin striations. Each of the Latin striations from each of the non-zero values of z are orthogonal to each other giving $p-1$ Latin squares.

Let

$$v_{ab} = \frac{1}{\sqrt{q}} (\omega^{\mathrm{tr}(f_{ab}(x))})_{x \in \mathbb{F}_q}. \tag{27}$$

Any vector can be expressed as a linear combination of the vectors of a base. This grouping of vectors into bases gives the row striation. For each $z \in \mathbb{F}_p$, the weight m_{abz} is assigned to v_{ab}. We want to represent s_z, in a linear combination, where all summands have the same magnitude. Thus we are most interested in the phase of the summands. We want the zth component of $m_{abz} v_{ab}$ to be $\frac{1}{q}$, and hence

$$m_{abz} = \frac{1}{\sqrt{q}} \omega^{-\mathrm{tr}(f_{ab}(z))}. \tag{28}$$

Thus, the elements in the linear combinations representing s_z are

$$m_{abz} v_{ab} = \frac{1}{q} (\omega^{\mathrm{tr}[f_{ab}(x) - f_{ab}(z)]})_{x \in \mathbb{F}_q} \tag{29}$$

By choosing the vectors to be all from the same base we fix a. We find that for each choice of a and each choice of z

$$\sum_{b \in \mathbb{F}_p} m_{abz} v_{ab} = s_z. \tag{30}$$

This gives us p copies of the row striation. For example, equations (7)–(9) and (14)–(16) show two copies of the row striation, the third copy has been omitted as a repetitious calculation.

In the theorem 6 construction f_{ab} is a planar function, so it is no surprise that the arrays of weights are Latin squares (as in (17)). In the theorem 7 construction f_{ab} is not a planar function, and so the arrays of weights are not Latin squares (see (24)).

Next we create the non-row striations using the same weights assigned to each vector, but different groupings of vectors. Note that in (14)–(16) and (18)–(20) each vector has the same weight assigned. In order to create a linear combination involving $m_{abz} v_{ab}$ which contains vectors not in the same basis, we first choose one vector e.g. v_{0c}, and see which elements can form the appropriate summation. To sum to s_z, we need $(m_{abz} v_{ab})_z = 1$ and $(m_{abz} v_{ab})_x \neq (m_{0cz} v_{0c})_x$ for all $x \neq z$. Hence, we need

$$\omega^{\mathrm{tr}[f_{ab}(x) - f_{ab}(z)]} \neq \omega^{\mathrm{tr}[f_{0c}(x) - f_{0c}(z)]} \qquad \forall z \neq x, \quad a \neq 0. \tag{31}$$

Thus, if (31) is satisfied for $z = 0$ then this grouping forms the column striation and we prepare an array e.g. (13). If (31) is satisfied for $z \neq 0$ then the cell in the prepared array corresponding to v_{ab} shall contain the cth symbol. For example in array (21), ♡ is the 0th symbol, ◇ is the 1st symbol and ♣ is the 2nd symbol.

In our simplified situation we only deal with prime fields and hence the trace function is equivalent to the identity function. Thus without loss of generality (31) may also be simplified to

$$[f_{ab}(x) - f_{0c}(x)] - [f_{ab}(z) - f_{0c}(z)] \neq 0 \qquad \forall z \neq x, \quad a \neq 0. \tag{32}$$

In (32), $[f_{ab}(x) - f_{0c}(x)]$ is the function of the inner product vector $IPV[v_{ab}, v_{0c}]$. $[f_{ab}(z) - f_{0c}(z)]$ represents the zth position of the inner product vector. It is the functions of the inner product vectors that create the MOLS, not the functions of the vectors themselves.

Theorem 10. *Let f_{ab} be as in theorem 6 or theorem 7 with $a, b \in \mathbb{F}_p$, p a prime. The set of 4-tuples $(a, b, c, z) \in \mathbb{F}_p^4$ that satisfy equation (32) (with an appropriate permutation $\sigma(b) = b'$) form a complete set of MOLS, where a is the row number, b' is the column number, c is the symbol number and z is the striation number.*

Permutations are not required for the theorem 6 construction. A permutation on b is required for the theorem 7 construction. A more general proof may be developed to include further classes of polynomials, with more general permutations.

Proof. Let $f_{ab} = ax^2 + bx$ as in theorem 6. Let $g_{ab} = (x + a)^3 + b(x + a)$ as in theorem 7; then

$$[f_{ab}(x) - f_{0c}(x)] - [f_{ab}(z) - f_{0c}(z)] = a(x^2 - z^2) + (b - c)(x - z) \tag{33}$$

$$= (x - z)[a(x + z) + b - c] \tag{34}$$

and

$$[g_{ab}(x) - g_{0c}(x)] - [g_{ab}(z) - g_{ab}(z)] = 3a(x^2 - z^2) + (3a^2 + b - c)(x - z) \tag{35}$$

$$= (x - z)[3a(x + z) + 3a^2 + b - c]. \tag{36}$$

(1) Given a suitable permutation $\sigma(b) = b'$, for each (b', z) there are exactly p valid (a, c) with no two of the valid (a, c) containing the same a or the same c. This ensures that each column of each square contains every symbol only once.

For the construction of theorem 6 the identity permutation $b' = b$ is used. Fixing b and z, and letting $x = z$ we solve (34). Inequation (32) requires inequality, so we seek to solve the statement for equality, knowing that the values which solve for equality will not solve the inequation:

$$a(2z) + b - c = 0. \tag{37}$$

For each a there is a unique c that solves this equation and hence there are p pairs (a, c). If $x \neq z$, then none of those pairs (a, c) will be solutions to (37), and hence satisfy (32).

For the construction of theorem 7 the permutation $b' = b + 3a^2$ is required. Fixing b and z and setting $x = z$ we solve (36)

$$3a(2z) + 3a^2 + b - c = 3a(2z) + b' - c = 0. \tag{38}$$

For each a there is a unique c that solves (38) and hence there are p pairs (a, c). If $x \neq z$ then none of these pairs (a, c) will be solutions to (38), and hence satisfy (32).

Note that in (32) we require $a \neq 0$, as this yields the solution $b = c$ giving one of the pairs that solve (34) and (36). This shows that the first row of every square is in standard form.

(2) For each (a, z) there are exactly p valid pairs (b', c). No two of the valid pairs (b', c) contain the same b' nor the same c. This ensures that each row of each square contains every symbol exactly once.

If we fix a and z and set $x = z$, then we solve equations (37) and (38). In the theorem 6 construction $c = 2az - b'$, and in the theorem 7 construction $c = 6az - b'$. Thus for each b' there is a unique c. There are p values of b' and hence p valid pairs (b', c) for each (a, z).

(3) For each (a, b'), $a \neq 0$ there are exactly p valid pairs (c, z). No two of the valid pairs (c, z) contain the same c, nor the same z. This shows that each cell (other than cells in the first row) has a different symbol in each square, which ensures that all of the squares are mutually orthogonal. There are $p - 1$ Latin striations, and 1 column striation.

For the construction of theorem 6 we try to solve

$$(x - z)[a(x + z) + b - c] = 0 \tag{39}$$

Assuming $x \neq z$ we require a solution to (37). If we fix $c \neq b$, then for each x there is a unique z that solves (39). There are p combinations of x and z that solve equation (39). One of these combinations will be of the form $x = z$. If we select this z to fill in the 4-tuple (a, b', c, z), then (32) is satisfied. If we allow $c = b$, then either $a = 0$, which represents the symbol in the b'th column, 0th row of each square; or $z = 0$, which creates a column striation. Hence there are p pairs (c, z).

For the construction of theorem 7 we try to solve

$$(x - z)[3a(x + z) + b' - c] = 0 \tag{40}$$

Then follow the argument for the theorem 6 case.

Properties 1, 2 and 3 combine to show that the set of 4-tuples (a, b', c, z) represents a complete set of MOLS. □

Conjecture 2. *Let f be a set of functions $f : \mathbb{F}_p \mapsto \mathbb{F}_p$, which construct a complete set of MUBs in dimension p. The set of 4-tuples (a, b, c, z) that satisfy equation (32), with an appropriate permutation $\sigma_a(a) = a'$, $\sigma_b(b) = b'$, $\sigma_c(c) = c'$, $\sigma_z(z) = z'$ form a complete set of MOLS, where a' is the row number, b' is the column number, c' is the symbol number and z' is the striation number.*

That is, any two IPV from vectors in different bases have exactly one position where their entries are the same.

5. Conclusion

The research in this paper points to subtleties within the construction of MUBs—the need for planar functions, but only in the inner products. It also gives valuable insight into the connection between MUBs and MOLS and suggests the possibility of MOLS giving rise to more MUBs in non-prime dimensions than the product construction does—see for example the conclusion in the paper by Wocjan and Beth [22].

Both of the constructions presented generate the same set of MOLS, showing that multiple sets of MUBs can be associated with each set of MOLS. Also the MUBs constructed in theorem 6 are obtained via characters of the polynomial x^2, and since this is a planar function which gives a Desarguesian plane (see [20]), the MUBs obtained could be considered to be connected to the same. The polynomial in the case of theorem 7 is not a quadratic and is non-planar. Perhaps there are new constructions of MUBs which use non-planar functions, which however have planar functions hidden in the structure.

The main question yet unanswered is whether this construction can be extended to all prime powers, odd and even, and to other constructions of MUBs, e.g. [13]. The authors are currently working on the odd prime power case, and also hope to extend the construction to the even prime powers. It should be noted that the known construction of MUBs in the even power case [7] is different from the construction in the odd prime power case, since it is based on Galois rings and not Galois fields. A summary of open question can be found in [23].

Acknowledgments

JH is supported by the Australian Postgraduate Awards Scheme. The authors would like to thank the anonymous referees for their very helpful comments, both on this paper and on possible future research.

References

[1] Saniga M, Planat M and Rosu H 2004 *J. Opt. B: Quantum Semiclass. Opt.* **6** L19–20
[2] Bennett C H and Brassard G 1984 *Proc. IEEE, Int. Conf. Computers, Systems and Signal Processing (Bangalore)* pp 175–9
[3] Wootters W K and Fields B D 1989 *Ann. Phys.* **191** 363–81
[4] Colbourn C J and Dinitz J H (eds) 2007 *Handbook of Combinatorial Designs* 2nd edn (Boca Raton FL: Taylor and Francis)
[5] Alltop T O 1980 *IEEE Trans. Inf. Theory* **26** 350–4
[6] Ivanovic I D 1981 *J. Phys. A: Math. Gen.* **14** 3241–5
[7] Klappenecker A and Rötteler M 2003 *Lect. Notes Comput. Sci.* **2948** 137–44
[8] Bandyopadhyay S, Boykin O P, Roychowdhury V and Vatan F 2002 *Algorithmica* **34** 512–28
[9] Šulc P and Tolar J 2007 *J. Phys. A: Math. Theor.* **40** 15099–112
[10] Archer C 2005 *J. Math. Phys.* **46** 022106
[11] Dembowski P 1997 *Finite Geometries (Classics in Mathematics)* (Berlin: Springer) (reprint of the 1968 edition)
[12] Paterek T, Dakić B and Brukner Č 2009 *Phys. Rev.* A **79** 012109
[13] Roy A and Scott A J 2007 *J. Math. Phys.* **48** 072110
[14] Bruck R H and Ryser H J 1949 *Can. J. Math.* **1** 88–93
[15] Lam C W H 1991 *Am. Math. Month.* **98** 305–18
[16] Gibbons K S, Hoffman M J and Wootters W K 2004 *Phys. Rev.* A **70** 062101
[17] Godsil C and Roy A 2009 *Eur. J. Combin.* **30** 246–62
[18] Horadam K J 2007 *Hadamard Matrices and their Applications* (Princeton, NJ: Princeton University Press)
[19] Dembowski P and Ostrom T G 1968 *Math. Z.* **103** 239–58
[20] Coulter R S and Matthews R W 1997 *Design. Code. Cryptogr.* **10** 167–84
[21] Johnson N L 2009 *Discrete Math.* **309** 430–61
[22] Wocjan P and Beth T 2005 *Quantum Inf. Comput.* **5** 93–101
[23] Rosu H C, Planat M and Saniga M 2004 *Quantum Commun., Meas. Comput.* **734** 315–8