Uniqueness of Sets of Mutually Unbiased Bases of Order 5

Daniel P. May*
University of Wyoming

G. Eric Moorhouse
University of Wyoming

16 April, 2009

Abstract

It is known that a set of k mutually unbiased bases of order d is unique (to within equivalence) for $d \in \{2, 3, 4\}$; in particular this is true for complete sets of mutually unbiased bases (the case $k = d + 1$). Here we show this conclusion holds also for $d = 5$. Our proof uses Haagerup's result [4] that any two complex Hadamard matrices of order 5 are are equivalent. We also use techniques borrowed from the study of nets of arbitrary prime order.

1 Introduction

Denote by $\mathbb{C}^d$ the complex vector space consisting of all column vectors of length d, endowed with the standard inner product

$$u^*v = \sum_j \overline{u_j}v_j$$

where $u, v \in \mathbb{C}^d$. Here, and throughout, the asterisk (*) denotes the conjugate-transpose map. A set $\mathfrak{B} = \{\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_k\}$ of k orthonormal bases of $\mathbb{C}^d$ is *mutually unbiased* if $|u^*v| = \frac{1}{\sqrt{d}}$ for all $u \in \mathcal{B}_i$ and $v \in \mathcal{B}_j$ with $i \neq j$. It is well known [5, 13] that every such collection $\mathfrak{B}$ consists of $k \leqslant d + 1$

*This work will appear as a portion of the first author's Ph.D. dissertation at the University of Wyoming.

members. A *complete set of MUB's* (mutually unbiased bases) is a set of $d+1$ MUB's of order d. The required conditions on the bases $\mathcal{B}_i$ depend only on the corresponding *orthonormal frames* $\mathcal{F}_i = \{\langle u\rangle : u \in \mathcal{B}_i\}$ where $\langle u\rangle \leqslant \mathbb{C}^d$ denotes the $\mathbb{C}$-subspace spanned by u. Let $\mathfrak{B}$ and $\mathfrak{B}'$ be two sets of k MUB's in $\mathbb{C}^d$, with corresponding orthonormal frames $\mathfrak{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_k\}$ and $\mathfrak{F}' = \{\mathcal{F}'_1, \ldots, \mathcal{F}'_k\}$ respectively. An *equivalence from* $\mathfrak{B}$ *to* $\mathfrak{B}'$ is a unitary transformation $U \in U_d(\mathbb{C})$ mapping $\mathfrak{F} \mapsto \mathfrak{F}'$. In Section 3 we restate this definition of equivalence in terms of matrix representations of the MUB's $\mathfrak{B}$ and $\mathfrak{B}'$.

Complete sets of MUB's of order d are known to exist when d is a prime power; see e.g. [7]. In Section 3 we recall the construction of the known MUB's of prime order. No complete sets are known when d is not a prime power; even in the case $d = 6$ the question of existence remains open, as no more than three MUB's of order 6 have been constructed to date; see [2, 3]. Our main result, which concerns the case $d = 5$, is

Theorem 1.1 *Every complete set of MUB's of order 5 is equivalent to the known construction. More generally, every set of MUB's of order 5 is equivalent to a subset of the known complete set.*

In Sections 2 and 3 we outline the connection between MUB's and complex Hadamard matrices, stating Haagerup's classification [4] of complex Hadamard matrices of order 5, upon which our proof of Theorem 1.1 relies. We also require results from the theory of exponential sums, as found in Section 4. This material, motivated largely by Gluck's result [6] on permutation polynomials, is valid much more generally than the case $p = 5$ considered here. Its emergence in this context further illustrates the ties between the study of MUB's and the study of nets, already observed in the literature; see e.g. [1, 12]. Finally in Section 5 we pull these tools together to prove our main Theorem 1.1.

2 Complex Hadamard Matrices

A *complex Hadamard matrix of order* $d \geqslant 1$ is a $d \times d$ matrix H, whose entries are complex numbers of modulus 1, such that

$$H^*H = dI.$$

As before, the asterisk (*) denotes the conjugate-transpose map. Every complex Hadamard matrix H of order d gives rise to a unitary matrix $A = \frac{1}{\sqrt{d}}H \in U_d(\mathbb{C})$.

A matrix $M \in U_d(\mathbb{C})$ is *(unitary) monomial* if it has exactly one nonzero entry (of modulus 1) in each row and column. The set of all $d \times d$ unitary monomial matrices form a subgroup, denoted here by $\mathbb{M}_d \leqslant U_d(\mathbb{C})$. If H is complex Hadamard of order d, then so is MHN whenever $M, N \in \mathbb{M}_d$. Similarly, if A is a normalized complex Hadamard matrix of order d, then so is MAN. We say two complex Hadamard matrices H, H' of order d are *equivalent* if $H' = MHN$ for some $M, N \in \mathbb{M}_d$. Similarly, two normalized complex Hadamard matrices A, A' of order d are *equivalent* if $A' = MAN$ for some $M, N \in \mathbb{M}_d$.

For every $d \geqslant 1$, there exists a complex Hadamard matrix of order d; for example, consider the character table of any abelian group of order d. In particular, the cyclic group of order d has character table $H = (\zeta^{jk})$ with row and column indices $j, k \in \mathbb{Z}/d\mathbb{Z}$, where ζ is a primitive complex d-th root of 1. We call this construction the *standard complex Hadamard matrix of order d.* (This construction appears in the literature under other names, including the *generalized Sylvester matrix* or *Fourier matrix* of order d.) For $d \in \{1, 2, 3, 5\}$, every complex Hadamard matrix of order d is equivalent to the standard one. For $d = 5$, this result is due to Haagerup [4]:

Theorem 2.1 *[Haagerup [4]] Every complex Hadamard matrix of order 5 is equivalent to the standard example $H_5 = (\zeta^{ij})_{i,j\in\mathbb{Z}/5\mathbb{Z}}$ where ζ is a complex primitive fifth root of 1.*

For a survey of known complex Hadamard matrices of other small orders, see [13].

In the study of complex Hadamard matrices, one sometimes uses a coarser equivalence relation, by allowing transposes, and possibly also field automorphisms (applied to matrix entries) as equivalences. This issue will not concern us here, since for $d \in \{1, 2, 3, 5\}$, any two complex Hadamard matrices of order d are already equivalent under the group $\mathbb{M}_d \times \mathbb{M}_d$ acting on the left and right.

A complex Hadamard matrix H is *normalized* if its first row and column consist of 1's. It is clear that every complex Hadamard matrix is equivalent to one in normalized form. In Section 5 we will use the following consequence of 2.1, whose proof is left as an easy exercise:

Corollary 2.1 *Let $H = (h_{i,j})_{i,j\in\mathbb{F}_5}$ be a* normalized *complex Hadamard matrix of order 5. Then all entries of H are complex fifth roots of 1. Moreover in any given row or column of H, the product of all five entries is 1.*

3 Matrix Representations of MUB's

Let $\mathfrak{B} = \{\mathcal{B}_1, \ldots, \mathcal{B}_k\}$ be a set of MUB's in $\mathbb{C}^d$. For each $i \in \{1, 2, \ldots, k\}$, let A_i be a $d \times d$ matrix with columns given by the members of the orthonormal basis $\mathcal{B}_i$. Since B_i is an orthonormal basis, we have $A_i^* A_i = I$; and since $\mathfrak{B}$ is mutually unbiased, every entry of $A_i^* A_j$ has modulus $\frac{1}{\sqrt{d}}$ for $i \neq j$. We call $\{A_1, A_2, \ldots, A_k\}$ a *matrix representation of* $\mathfrak{B}$. We similarly take $\{A_1', A_2', \ldots, A_k'\}$ to be a matrix representation of $\mathfrak{B}'$. Then $\mathfrak{B}$ and $\mathfrak{B}'$ are equivalent (as defined above) iff there exists a unitary matrix $U \in U_n(\mathbb{C})$, and monomial unitary matrices $M_i \in \mathbb{M}_d$ such that

$$\{A_1', A_2', \ldots, A_k'\} = \{UA_1M_1,\ UA_2M_2,\ \ldots,\ UA_kM_k\}.$$

Note that the k matrices may be listed in a different order in the two sets. Also note that the monomial matrix M_i permutes the vectors of $\mathcal{B}_i$ and scales them by complex numbers of modulus 1, while preserving the corresponding frame $\mathcal{F}_i$.

Now let $\mathfrak{B} = \{\mathcal{B}_1, \ldots, \mathcal{B}_k\}$ be a set of $k \geqslant 2$ MUB's, with matrix representation $\mathfrak{A} = \{A_1, A_2, \ldots, A_k\}$. Without loss of generality, $A_1 = I$ and $\mathcal{B}_1$ is the standard basis of $\mathbb{C}^d$; otherwise left-multiply all matrices in $\mathfrak{A}$ by the unitary matrix A_1^* to obtain an equivalent set whose matrix representation contains I. Thus $\mathfrak{A} = \{I, A_2, \ldots, A_k\}$ where each of the matrices $A_2, \ldots, A_k$ is complex Hadamard; moreover whenever $2 \leqslant i < j \leqslant k$, every entry of $A_i^* A_j$ has modulus $\frac{1}{\sqrt{d}}$.

The standard construction of a complete set of MUB's of odd prime order p is as follows, described in terms of its matrix representation. We take $A_\infty = I$ and for each $i \in \mathbb{F}_p$, we set

$$A_i = \tfrac{1}{\sqrt{p}} \big(\zeta^{ij^2+kj}\big)_{j,k\in\mathbb{F}_p}\,. \tag{1}$$

This is a special case of the standard construction of a complete set of MUB's of order q for every prime power q; see e.g. [7].

4 Exponential Sums

Our proof of Theorem 1.1, which follows in Section 5, makes use of the following results. Here $\mathbb{F}_p$ is a finite field of prime order p, and ζ is a complex primitive p-th root of 1. We define the *exponential sum* of an arbitrary function $f : \mathbb{F}_p \to \mathbb{F}_p$ by

$$S_f = \sum_{x \in \mathbb{F}_p} \zeta^{f(x)} \in \mathbb{Z}[\zeta].$$

The following result is inspired by Gluck's proof [6] that a transitive affine plane of prime order is necessarily classical (i.e. isomorphic to $AG_2(\mathbb{F}_p)$).

Theorem 4.1 *A function $f : \mathbb{F}_p \to \mathbb{F}_p$ is represented by a quadratic polynomial in $\mathbb{F}_p[x]$, iff $|S_{f(x)+cx}| = \sqrt{p}$ for all $c \in \mathbb{F}_p$.*

Proof. It is well-known that $|S_{f(x)+cx}| = \sqrt{p}$ for all $c \in \mathbb{F}_p$. To prove the converse, assume that $|S_{f(x)+cx}| = \sqrt{p}$ for all $c \in \mathbb{F}_p$. This implies that for all $c \in \mathbb{F}_p$, the function $x \mapsto f(x) + cx$ assumes no value more than twice as x ranges over $\mathbb{F}_p$; see [6]. In the classical projective plane $PG_2(\mathbb{F}_p)$, we consider the point set

$$\mathcal{O} = \{(x, f(x), 1) : x \in \mathbb{F}_p\} \cup \{(0, 1, 0)\}.$$

Note that $|\mathcal{O}| = p+1$. We will show that no three points of $\mathcal{O}$ are collinear. Let (X, Y, Z) be homogeneous coordinates for the plane, and suppose that three points of $\mathcal{O}$ lie on a line $aX + bY + cZ = 0$ where the coefficients $a, b, c \in \mathbb{F}_p$ are not all zero. We cannot have $b = 0$, since the line $aX + cZ = 0$ meets $\mathcal{O}$ in just two points, including $(0, 1, 0)$. We may therefore assume that $b = 1$ and the line $aX + Y + cZ = 0$ meets $\mathcal{O}$ in three points $(x_i, f(x_i), 1)$ for $i = 1, 2, 3$. This means that $f(x) + ax$ attains the value $-c \in \mathbb{F}_p$ at least three times, a contradiction.

Thus no three points of $\mathcal{O}$ are collinear. By Segre's Theorem [10], $\mathcal{O}$ is a conic: its points are the solutions of a homogeneous polynomial equation of degree 2. From this it is not hard to see that f is itself given by a polynomial of degree 2. $\square$

The following technical result will also be used.

Lemma 4.1 *Let $f : \mathbb{F}_p \to \mathbb{F}_p$ and let $a \in \mathbb{F}_p$ be a nonzero constant. Suppose that $|S_{ax^2+bx+cf(x)}| = \sqrt{p}$ for all $b, c \in \mathbb{F}_p$. Then $f(x) = mx + d$ for some $m, d \in \mathbb{F}_p$.*

Proof. The hypothesis implies that

$$\begin{aligned} p &= \Big| \sum_{x \in \mathbb{F}_p} \zeta^{ax^2+bx+cf(x)} \Big|^2 \\ &= \sum_{x,y \in \mathbb{F}_p} \zeta^{a(x^2-y^2)+b(x-y)+c(f(x)-f(y))} \\ &= \sum_{y,t \in \mathbb{F}_p} \zeta^{2aty+at^2+bt+c(f(y+t)-f(y))} \end{aligned}$$

for all $b, c \in \mathbb{F}_p$. Multiply both sides by ζ^{-b} and sum over $b \in \mathbb{F}_p$ to obtain

$$\sum_{y \in \mathbb{F}_p} \zeta^{2ay+a+c(f(y+1)-f(y))} = 0 \tag{2}$$

for all $c \in \mathbb{F}_p$. Now suppose the desired conclusion fails, i.e. f is not representable as a polynomial of degree $\leqslant 1$; we seek a contradiction. Then the first-order difference of f is not constant, so there exists $x \in \mathbb{F}_p$ such that

$$f(x+1) - f(x) \neq m$$

where $m = f(1) - f(0)$. Clearly $x \neq 0$. Set

$$c = \frac{2ax}{m - [f(x+1) - f(x)]}$$

and check that the general term in (2) takes the same value for $y = 0$ and for $y = x$. However the only way for the exponential sum (2) to vanish is for the exponent to have distinct values as y varies over $\mathbb{F}_p$, which is the desired contradiction. $\square$

5 Order $d = 5$

We proceed to prove Theorem 1.1. Consider a set $\mathfrak{B}$ of k MUB's of order $d = 5$, with $k \geqslant 2$. Rather than indexing the members of $\mathfrak{B}$ using $\{1, 2, \ldots, k\}$ as in Section 3, it is convenient to use subscripts $\{\infty, 0, 1, 2, \ldots, k-2\}$. Let ζ be a primitive complex fifth root of 1, and denote $H_5 = (\zeta^{ij})_{i,j \in \mathbb{F}_5}$ as in Theorem 2.1.

Lemma 5.1 *To within equivalence,* $\mathfrak{B} = \{\mathcal{B}_\infty, \mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{k-2}\}$ *has matrix representation of the form*

$$A_\infty = I, \quad A_i = \tfrac{1}{\sqrt{5}} L_i H_5$$

where $L_i \in \mathbb{M}_5$ *for* $i = 0, 1, \ldots, k-2$*. Moreover we may assume that* $L_0 = I$ *and each of the matrices* $L_0, L_1, \ldots, L_{k-2}$ *has 1 as the nonzero entry in its first column.*

Proof. As explained in Section 3, we may assume that $A_\infty = I$. By Theorem 2.1, we have $A_i = \frac{1}{\sqrt{5}} L_i H_5 R_i$ for some $L_i, R_i \in \mathbb{M}_5$. We may in fact assume that $A_i = \frac{1}{\sqrt{5}} L_i H_5$ where $L_i \in \mathbb{M}_5$ for $i = 0, 1, \ldots, k-2$ and $L_0 = I$; otherwise replace $\mathfrak{A}$ by the equivalent set of matrices

$$\begin{aligned} \{L_0^* A_\infty L_0 {=} I, \qquad & L_0^* A_0 R_0^* {=} \tfrac{1}{\sqrt{5}} H_5\,, \\ L_0^* A_i R_i^* {=} \tfrac{1}{\sqrt{5}} (L_0^* L_i) H_5\,, \quad & 1 \leqslant i \leqslant k-2\}. \end{aligned}$$

Now

$$L_i = (\lambda_{i,j} \delta_{\sigma_i(j),\ell})_{j,\ell \in \mathbb{F}_5} \quad \text{for } i = 0, 1, \ldots, k-2$$

where $\lambda_{i,j} \in \mathbb{C}$ with $|\lambda_{i,j}| = 1$, $\lambda_{0,j} = 1$ and $\sigma_i \in \operatorname{Sym} \mathbb{F}_5$ with $\sigma_0 = id$. Finally, we may assume that $\lambda_{i,0} = 1$ for $i = 0, 1, \ldots, k-2$; otherwise we again replace the current matrix representation by the equivalent set

$$\begin{aligned} \{A_\infty {=} I, \qquad & A_0 {=} \tfrac{1}{\sqrt{5}} H_5\,, \\ A_i (\overline{\lambda_{i,0}} I) {=} \tfrac{1}{\sqrt{5}} (\overline{\lambda_{i,0}} L_i) H_5\,, \quad & 1 \leqslant i \leqslant k-2\} \end{aligned}$$

which has the desired form. $\square$

As in the proof of 5.1, we write

$$L_i = (\lambda_{i,j} \delta_{\sigma_i(j),\ell})_{j,\ell \in \mathbb{F}_5} \tag{3}$$

for $i = 0, 1, \ldots, k-2$, where $|\lambda_{i,j}| = 1$, $\lambda_{i,0} = \lambda_{0,j} = 1$, and $\sigma_i \in \operatorname{Sym} \mathbb{F}_5$, and $\sigma_0 = id$. The (r,s)-entry of $A_i^* A_j$ has modulus

$$\tfrac{1}{5} \left| \sum_{x \in \mathbb{F}_5} \overline{\lambda_{i,x}} \lambda_{j,x} \zeta^{s\sigma_j(x) - r\sigma_i(x)} \right| = \tfrac{1}{\sqrt{5}} \tag{4}$$

for all $r, s \in \mathbb{F}_5$ and *distinct* $i, j \in \{0, 1, \ldots, k-2\}$. In particular for $r = 0$, we have

$$\left| \sum_{x \in \mathbb{F}_5} \overline{\lambda_{i,x}} \lambda_{j,x} \zeta^{s\sigma_j(x)} \right| = \sqrt{5}. \tag{5}$$

Specializing further to the case $j = 0 \neq i$, and using the fact that $\sigma_0 = id \in \operatorname{Sym} \mathbb{F}_5$ and $\lambda_{i,0} = 1$, we have

$$\begin{aligned} \sum_{a,x \in \mathbb{F}_5} \overline{\lambda_{i,x}} \lambda_{i,x-a} \zeta^{sa} &= \textstyle\sum_{x,y \in \mathbb{F}_5} \overline{\lambda_{i,x}} \lambda_{i,y} \zeta^{s(x-y)} \\ &= \left| \textstyle\sum_{x \in \mathbb{F}_5} \overline{\lambda_{i,x}} \zeta^{sx} \right|^2 = 5. \end{aligned} \tag{6}$$

Now multiply both sides of (6) by ζ^{su} where $s, u \in \mathbb{F}_5$, and sum over $s \in \mathbb{F}_5$ to obtain

$$\sum_{x \in \mathbb{F}_5} \overline{\lambda_{i,x}} \lambda_{i,x+u} = 5\delta_{u,0} \,.$$

This means that the matrix $(\lambda_{i,x+y})_{x,y \in \mathbb{F}_5}$ is complex Hadamard. It is a routine matter to normalize this matrix (see Section 2) and apply Corollary 5.1, together with the fact that $\lambda_{i,0} = 1$, to conclude that each of the values $\lambda_{i,j}$ is a complex fifth root of unity. In (6) we write $\overline{\lambda_{i,x}} = \zeta^{f_i(x)}$ for some function $f_i : \mathbb{F}_5 \to \mathbb{F}_5$ to obtain

$$\left| \sum_{x \in \mathbb{F}_5} \zeta^{f_i(x)+sx} \right| = \sqrt{5}$$

for all $s \in \mathbb{F}_5$. By Theorem 4.1, the function $f_i : \mathbb{F}_5 \to \mathbb{F}_5$ is quadratic. We have

$$f_i(x) = a_i x^2 + b_i x$$

for some $a_i, b_i \in \mathbb{F}_5$ with $a_i \neq 0$; the constant term of f_i is zero since $\zeta^{f_i(0)} = \overline{\lambda_{i,0}} = 1$. Substitute into (4) with $j = 0$ to obtain

$$\left| \sum_{x \in \mathbb{F}_5} \zeta^{a_i x^2 + (b_i+s)x - r\sigma_i(x)} \right| = \sqrt{5}$$

for all $r, s \in \mathbb{F}_5$. By Lemma 4.1, we have $\sigma_i(x) = m_i x + d_i$ for some $m_i, d_i \in \mathbb{F}_5$. Note that $m_i \neq 0$ since $\sigma_i : \mathbb{F}_5 \to \mathbb{F}_5$ is a permutation. Now

$$A_i = \tfrac{1}{\sqrt{5}} L_i H_{[0]} = \tfrac{1}{\sqrt{5}} H_{[-a_i]} R_i$$

where the complex Hadamard matrix

$$H_{[a]} = \left(\zeta^{aj^2+\ell j}\right)_{j,\ell \in \mathbb{F}_p}$$

arises from the standard construction (1), and the monomial matrices L_i and R_i are given by

$$\begin{aligned} L_i &= (\lambda_{i,j}\delta_{\sigma_i(j),\ell})_{j,\ell\in\mathbb{F}_5} = (\delta_{m_ij+d_i,\ell}\zeta^{-a_ij^2-b_ij})_{j,\ell\in\mathbb{F}_5}\,; \\ R_i &= (\delta_{j,m_i\ell-b_i}\zeta^{d_i\ell})_{j,\ell\in\mathbb{F}_5}\,. \end{aligned}$$

The monomial matrices R_i disappear after replacing the matrices A_i with yet another equivalent set, and so we obtain

$$A_\infty = I, \quad A_i = \tfrac{1}{\sqrt{5}}H_{[-a_i]}$$

for $i = 0, 1, \ldots, k-2$ where $a_0{=}0, a_1, \ldots, a_{k-2} \in \mathbb{F}_5$ are distinct. This concludes the proof of Theorem 1.1.

References

[1] M. Aschbacher, A. M. Childs and P. Wocjan, 'The limitations of nice mutually unbiased bases', *Journal of Algebraic Combinatorics* **25** (2007), 111–123. arXiv:quant-ph/0412066

[2] I. Bengtsson, W. Bruzda, Â. Ericsson, J.-Â. Larsson, W. Tadej and K. Życzkowski, 'Mutually unbiased bases and Hadamard matrices of order 6', *J. Math. Phys.* **48** (2007), 052106.

[3] S. Brierley and S. Weigert, 'Maximal sets of mutually unbiased quantum states in dimension 6', *Phys. Rev. A* **78** (2008), 042312.

[4] U. Haagerup, 'Orthogonal maximal abelian *-subalgebras of the $n \times n$ matrices and cyclic n-roots', in *Operator Algebras and Quantum Field Theory* (Rome), Cambridge, MA: International Press, 1996, pp.296–322.

[5] I. D. Ivanović, 'Geometrical description of quantal state determination', *J. Phys. A: Math. Gen.* **14** (1981), 3241–3245.

[6] D. Gluck, 'A note on permutation polynomials and finite geometries', *Discrete Math.* **80** (1990), 97–100.

[7] A. Klappenecker and M. Rötteler, 'Constructions of mutually unbiased bases', in *Proc. International Conference on Finite Fields and Applications, Toulouse, France,* May 5–9, 2003, pp.137–144. arXiv:quant-ph/0309120

[8] G. E. Moorhouse, 'Ranks of nets and webs', preliminary draft, 2005. http://www.uwyo.edu/moorhouse/pub/ranks_webs.pdf

[9] G. E. Moorhouse, 'Ranks of nets', *Quasigroups and Related Systems* **14** (2006), 61–72. http://www.uwyo.edu/moorhouse/pub/qrs.pdf

[10] B. Segre, 'Ovals in a finite projective plane', *Canad. J. Math.* **7** (1955), 414–416.

[11] W. Tadej and K. Życzkowski, 'A concise guide to complex Hadamard matrices', arXiv:quant-ph/0512154

[12] P. Wocjan and T. Beth, 'New construction of mutually unbiased bases in square dimensions', *Quantum Information and Computation* **5** (2005), 93–101. arXiv:quant-ph/0407081

[13] W. K. Wooters and B. D. Fields, 'Optimal state determination by mutually unbiased measurements', *Ann. Phys.* **191** (1989), 363–381.