Mutually unbiased triplets from non-affine families of complex Hadamard matrices in dimension 6

D Goyeneche

Departamento de Física, Universidad de Concepción, Casilla 160-C, Concepción, Chile
Center for Optics and Photonics, Universidad de Concepción, Casilla 4016, Concepción, Chile

E-mail: dgoyeneche@cefop.udec.cl

Received 5 October 2012, in final form 29 January 2013
Published 21 February 2013
Online at stacks.iop.org/JPhysA/46/105301

Abstract

We study the problem of constructing mutually unbiased bases in dimension 6. This approach is based on an efficient numerical method designed to find solutions to the quantum state reconstruction problem in finite dimensions. Our technique suggests the existence of previously unknown symmetries in Karlsson’s non-affine family $K_6^{(5)}$ which we confirm analytically. Also, we obtain strong evidence that not more than three mutually unbiased bases can be constructed from pairs which contain members of some non-affine families of complex Hadamard matrices.

PACS numbers: 03.67.-a, 03.65.-w, 03.65.Aa

1. Introduction

The existence of maximal sets of mutually unbiased (MU) bases in every dimension is a very important open problem in foundations of quantum mechanics. Two orthogonal bases are MU if they are as different as possible in Hilbert space, in the sense that the projection of each element of the first base onto each element of the second one has the same absolute value. These kinds of bases have several applications in quantum information theory: quantum key distribution protocols [1–3], entanglement detection [4], dense coding, teleportation, entanglement swapping, covariant cloning and state tomography (see [5] and references therein). They are also interesting in mathematics because of their connection with affine planes [6] and finite geometries [7]. Additionally, they are useful in solving the Mean King problem [8]. In a Hilbert space of dimension $d$, we can construct maximal sets of $d + 1$ MU bases when $d$ is prime or prime power. Otherwise, analytical [9–12] and numerical [13–17] efforts to construct $d + 1$ MU bases fail and it is suspected that they do not exist. The lowest dimension where this problem remains open is 6, where most of the previously mentioned works have tried to find a solution. This paper presents a new method that numerically solves the problem to find the maximal set of MU bases that can be obtained from a given pair of MU bases. The most important advantage of our method is that the computational cost is...
independent of the pair of MU bases considered. Our method is not an algorithm because it does not stop with a definite answer but converges very quickly even in higher dimensions. This work is organized as follows. In section 2, we briefly introduce complex Hadamard matrices and MU bases. In section 3, we present the method to find MU vectors and discuss its convergence. We successfully test our approach in section 4 by searching the known 48 vectors MU to the identity and the Fourier matrices in dimension 6, and we obtain known triplets containing the identity and the Diţă matrices. Section 5 contains our main results: we could not find triplets of MU bases from considering a complex Hadamard matrix belonging to the non-affine families $K_6^{(2)}$ and $K_6^{(3)}$ existing in dimension 6 as well as other families contained in them. This study has allowed us to find new symmetries for the family $K_6^{(2)}$.

2. Complex Hadamard matrices and mutually unbiased bases

This section contains the minimal information about complex Hadamard matrices and MU bases required to make the paper self-contained; more details can be found in [14] and [18], for example. Two orthonormal bases $\{|\psi_k\rangle\}$ and $\{|\phi_l\rangle\}$ defined on a $d$-dimensional Hilbert space are MU if they satisfy the property

$$\langle \psi_k | \phi_l \rangle^2 = \frac{1}{d},$$

for every $k, l = 0, \ldots, d - 1$.

A square matrix is a complex Hadamard matrix if it has unimodular entries and orthonormal columns. Such matrices exist in every dimension and the Fourier matrices represent the simplest proof of their existence. For example, in dimension 4 the Fourier matrix is given by

$$F_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & -1 & \omega^3 \\ 1 & \omega^2 & 1 & \omega^2 \\ 1 & \omega^3 & -1 & \omega \end{pmatrix},$$

where $\omega = e^{2\pi i/4}$. Also, the tensor product of complex Hadamard matrices is a complex Hadamard matrix. The simplest example is given by the tensor product of two Fourier matrices defined in dimension 2:

$$F_2 \otimes F_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

which gives us a real Hadamard matrix. Complex Hadamard matrices have been extensively studied in recent years and they are very hard to find when $d > 5$ [15]. We say that two complex Hadamard matrices $H_1$ and $H_2$ are equivalent ($H_1 \sim H_2$) if there exist unitary diagonal operators $D_1, D_2$ and permutation operators $P_1, P_2$, such that

$$H_1 = P_1 D_1 H_2 D_2 P_2.$$
A complex Hadamard matrix may belong to a continuous set of inequivalent complex Hadamard matrices called a family. A family of complex Hadamard matrices $H(x)$ is affine if it can be cast in the form

$$H(x) = H(0) \circ \text{Exp}(iR(x)),$$

where $R(x)$ is a real matrix for all value of the real parameter $x = (x_1, \ldots, x_s)$ and $\text{Exp}$ is the entry-wise exponential function given by

$$\text{Exp}(iR(x))_{lm} = \exp(iR(x)_{lm}),$$

and the symbol $\circ$ denotes the Hadamard product $(A \circ B)_{lm} = A_{lm}B_{lm}$. The number $s$ of independent parameters corresponds to the dimension of the family. If a continuous family of inequivalent complex Hadamard matrices is not affine we say it is non-affine. For example, the families stemming from the Fourier matrix in dimension 6 ($F_6^{(2)}$) and the Ditâ family ($D_6^{(1)}$) are affine families, whereas the Karlsson families $K_6^{(2)}$ and $K_6^{(3)}$ are non-affine. The notation considered here is consistent with the catalogue of complex Hadamard matrices presented by Bruzda–Tadej–Życzkowski [22]. In this notation, the upper index denotes the dimension of the family and the lower index the dimension of the space where it is defined. If a complex Hadamard matrix $H$ belongs neither to an affine nor to a non-affine family we call it isolated.

In other words, it is impossible to obtain a complex Hadamard matrix inequivalent to $H$ from infinitesimal perturbations to its entries. A set of MU bases is inextensible if no further orthonormal basis MU to each base of the set exists. A well-known fact is that any set of $d+1$ MU bases is inextensible, and it is conjectured that every triplet of MU bases in dimension 6 is inextensible. We mention that the complete set of inextensible MU bases in dimensions $d \leq 5$ has been found in [23] by considering Buchberger’s algorithm [24]. This algorithm is a generalization of Gaussian elimination to nonlinear multivariate polynomial equations. Also, a characterization of triplets of MU bases in $d = 6$ have been given if the second MU basis belongs to an affine family of Hadamard matrices [16]. In a recent paper, it has been analytically proven that given any triplet of MU product bases in dimension 6 it is not possible to find even a single vector MU to the triplet [25].

From definition of MU bases, it is easy to show that any pair $\{b_1, b_2\}$ of MU bases is unitary equivalent to a pair $\{I, H\}$, where $I$ is the identity matrix and $H$ is a complex Hadamard matrix. Therefore, the existence and classification of MU bases is closely related to the existence of the maximal set of complex Hadamard matrices. Given a pair of MU bases $\{I, H\}$ the problem of finding the complete set of vectors MU to both of them can, in principle, be solved by considering Buchberger’s algorithm. However, when $H$ belongs to a special kind of family of complex Hadamard matrices, known as non-affine, even 16 GB was not enough memory for the algorithm to terminate and identify the solutions [18]. In the following section, we will present a method to find the complete set of MU vectors to a given pair of the form $\{I, H\}$ whose efficiency does not decrease for non-affine families.

### 3. MU vectors as fixed points

#### 3.1. The physical imposition operator

In this section, we present a method that allows the numerical construction of all of vectors MU to a given pair of MU bases $\{I, H\}$. The iterative method used here allows us to efficiently generate highly accurate approximations to the solutions of the defining set of equations. The desired states are attractive fixed points of the physical imposition operator [26] which has been used previously to find those quantum states known as Pauli partners [27]. The problem has a unique answer if the given probability distributions are informationally complete; otherwise a
finite or infinite number of solutions may exist. The physical imposition operator is useful for the problem studied here because the search for MU bases is a particular case of the quantum state reconstruction problem, namely to determine the quantum state of a physical system compatible with probability distributions obtained from actual measurements.

To illustrate the concept of the imposition operator, let us assume that \{\ket{\psi_k}\} and \{\ket{\phi_l}\} are the eigenvectors bases of two observables acting in \( \mathbb{C}^d \) say, \( A \) and \( B \), respectively. We suppose that two probability distributions \{\rho_k^{(A)}\} and \{\rho_l^{(B)}\} have been obtained by measuring the observables \( A \) and \( B \), respectively. For simplicity, the distributions are assumed to be given exactly, which is only possible when the ensemble of quantum states is infinite. To reconstruct a pure state \( \ket{\Phi} \in \mathbb{C}^d \) compatible with the measurements, we need to find all solutions \{\ket{\Phi}\} of the following set of coupled nonlinear equations:

\[
|\braket{\psi_k|\Phi}|^2 = \rho_k^{(A)}, \quad (7)
\]

\[
|\braket{\phi_l|\Phi}|^2 = \rho_l^{(B)}, \quad (8)
\]

where \( k, l = 0, \ldots, d-1 \). In order to find a solution we perform the following steps.

1. Choose a quantum state \( \ket{\Psi_0} \) at random, which will be called the seed.
2. Decompose the state \( \ket{\Psi_0} \) in the basis \{\ket{\psi_k}\},

\[
\ket{\Psi_0} = \sum_{k=0}^{d-1} c_k \ket{\psi_k}. \quad (9)
\]

3. Modify the amplitudes of the expansion coefficients \( c_k \) in order to impose the information about \( A \),

\[
c_k \rightarrow \sqrt{\rho_k^{(A)}} \frac{c_k}{|c_k|}. \quad (10)
\]

In the last step, we have replaced the amplitudes of the coefficients \( \{c_k\} \) compatible with those of the observable \( A \); note that we did not modify the phase factors \( c_k/|c_k| \) because we cannot draw any conditions about them from the data \{\rho_k^{(A)}\}. The physical imposition operator implements the transformations just described in one operation,

\[
T_{A, \rho^{(A)}} \ket{\Psi_0} = \sum_{k=0}^{d-1} \sqrt{\rho_k^{(A)}} \frac{\braket{\psi_k|\Psi_0}}{|\braket{\psi_k|\Psi_0}|} \ket{\psi_k}; \quad (11)
\]

when \( \ket{\Psi_0} \) happens to be orthogonal to the state \( \ket{\psi_k} \), for any \( k = 0, \ldots, d-1 \), we define

\[
\braket{\psi_k|\Psi_0}/|\braket{\psi_k|\Psi_0}| \rightarrow 1. \quad (12)
\]

This operator is nonlinear and its action on every quantum state is well defined. The action of this operator on a randomly chosen state \( \ket{\Psi_0} \) can be interpreted as incorporating, what we learn about the unknown state when the observable \( A \) is measured. In other words, the initial state \( \ket{\Psi_0} \) has no information about the quantum system considered, while the state \( T_{A, \rho^{(A)}} \ket{\Psi_0} \) contains all the information we have acquired by measuring \( A \) in the unknown state. Note that \( T_{A, \rho^{(A)}} \) is idempotent because applying it once exhausts the information available about \( A \).

Next, we proceed in a similar way with the second observable \( B \) in order to try to find a solution of the set of equations (7), (8), defining the physical imposition operator associated with the observable \( B \),

\[
T_{B, \rho^{(B)}} \ket{\Psi_0} = \sum_{r=0}^{d-1} \sqrt{\rho_r^{(B)}} \frac{\braket{\phi_r|\Psi_0}}{|\braket{\phi_r|\Psi_0}|} \ket{\phi_r}. \quad (13)
\]
In order to analyze the convergence of the sequence \( |\Psi_n\rangle = (T_{B,p^n}T_{A,p^n})^n |\Psi_0\rangle \), generally does not contain the complete information about both \( A \) and \( B \); some of the information about \( A \) is destroyed when \( T_{B,p^n} \) is imposed, which is a consequence of the commutation rule \([A,B] \neq 0\). If \( A \) and \( B \) commute, it is trivial to find a solution to equations (7), (8), namely

\[
S = \{|\Psi \rangle \in \mathcal{H} / |\Psi \rangle = T_{A,p^n} |\Psi_0\rangle, \forall |\Psi_0\rangle \in \mathcal{H}\} \tag{15}
\]

\[
= \{|\Psi \rangle \in \mathcal{H} / |\Psi \rangle = T_{B,p^n} |\Psi_0\rangle, \forall |\Psi_0\rangle \in \mathcal{H}\}. \tag{16}
\]

In general, the state \( |\Psi_1\rangle \) has the complete information about \( B \) and only partial information about \( A \), so the composite operator \( T_{B,p^n}T_{A,p^n} \) is not idempotent. Therefore, we can iterate the procedure just described and analyze the convergence of the sequence

\[
|\Psi_n\rangle = (T_{B,p^n}T_{A,p^n})^n |\Psi_0\rangle, \quad n \in \mathbb{N}. \tag{17}
\]

It has been proven [27] that each solution of the system of coupled equations (7), (8) is an attractive fixed point of \( T_{B,p^n}T_{A,p^n} \). Moreover, this property also holds for a general set of observables \( A, B, C, \ldots \) and probability distributions \( p^{(A)}, p^{(B)}, p^{(C)}, \ldots \). The iterations are robust under adding redundant information, and the sequences converge if and only if the probability distributions are compatible, in the sense that the Heisenberg uncertainty principle is not violated.

The problem of constructing MU vectors is a particular case of the quantum state reconstruction problem just described. Let \( A \) and \( B \) be two observables with a pair of MU eigenbases \( B_A \) and \( B_B \). A vector is MU to the pair \( \{B_A, B_B\} \) if it has equally weighted probability distributions with respect to both observables, that is,

\[
p_k^{(A)} = \frac{1}{d} \quad \text{and} \quad p_l^{(B)} = \frac{1}{d}. \tag{18}
\]

for every \( k, l = 0, \ldots, d - 1 \). Interestingly, when the eigenvectors bases are MU, every basin of attraction is found to be of the same size, verified numerically in every prime dimension \( 2 \leq d \leq 37 \) [27], as well as in every simulation reported below for \( d = 6 \). This property indicates that the efficiency of the algorithm is maximal when the eigenvector bases of the observables are MU, because the number of randomly chosen seed states needed to find all solutions is minimized. This observation conforms with the idea that the redundancy of information is minimal when the observables have MU eigenvector bases.

### 3.2. Convergence

In order to analyze the convergence of the sequence \( |\Psi_n\rangle \) defined in equation (17), we need to define a metric for quantum states. We want to determine when a solution given by our method is a solution of the coupled system of equations given by equations (7), (8). Let \( A \) be an observable having the eigenvectors base \( \{|\psi_k\rangle\}_{k=0,...,d-1} \) and let \( |\phi\rangle \) and \( |\psi\rangle \) be two arbitrary quantum states. The distance between the probability distributions associated with the observable \( A \) in the states \( |\phi\rangle \) and \( |\psi\rangle \) can be defined by means of Hellinger’s metric [28],

\[
D_A^2(|\phi\rangle, |\psi\rangle) = \sum_{k=0}^{d-1} \left( |\langle \psi_k | \phi \rangle| - |\langle \phi_k | \psi \rangle| \right)^2. \tag{19}
\]

This metric compares two probability distributions of the eigenvalues of a single observable and it is important to realize that this is a metric for probability distributions, not for states.
In the present context, we need to consider more than one observable and the corresponding probability distributions. Therefore, we introduce the Hellinger metric for \( m \) observables, the so-called distributional metric [27],

\[
D^2_{A_1,\ldots,A_m}(|\phi\rangle,|\psi\rangle) = \frac{1}{m} \sum_{j=1}^{m} D^2_{A_j}(|\phi\rangle,|\psi\rangle),
\]

where \( D_{A_j}(|\phi\rangle,|\psi\rangle) \) is the Hellinger distance of the observable \( A_j \), defined in equation (19).

In our study of MU bases, we will always start from a pair of bases \( B_1 = \{|\psi_k\rangle, k = 0, \ldots, d - 1\} \) and \( B_2 = \{|\phi_l\rangle, l = 0, \ldots, d - 1\} \). Now, assuming that \(|\Phi\rangle \in \mathbb{C}^d\) is a vector MU to these bases, the expression

\[
D_{A,B}(|\Psi_n\rangle,|\Phi\rangle) = \sqrt{\frac{1}{2} D^2_A(|\Psi_n\rangle,|\Phi\rangle) + \frac{1}{2} D^2_B(|\Psi_n\rangle,|\Phi\rangle)}
\]

\[
= \sqrt{\frac{1}{2} \sum_{k=0}^{d-1} |\langle \psi_k | \Psi_n \rangle|^2 - \sqrt{\frac{1}{d}} + \frac{1}{2} \sum_{l=0}^{d-1} |\langle \phi_l | \Psi_n \rangle|^2 - \sqrt{\frac{1}{d}}}
\]

\[
= \sqrt{2 - \frac{1}{\sqrt{d}} \left( \sum_{k=0}^{d-1} |\langle \psi_k | \Psi_n \rangle|^2 + \sum_{l=0}^{d-1} |\langle \phi_l | \Psi_n \rangle|^2 \right)}
\]

(21)

tells us how close the state \(|\Psi_n\rangle\) is to being MU to \( B_1 \) and \( B_2 \). We will say that a sequence has converged when

\[
D_{A,B}(|\Psi_n\rangle,|\Phi\rangle) < 0.01,
\]

which means that the absolute error of the amplitudes is less than \( 8 \times 10^{-4} \) on average. Numerical simulations suggest that the absolute error of every amplitude of a solution is very close to the averaged error just mentioned. Given that the desired solutions are (stable) attractive fixed points, our approximations must be close to the exact solutions of the problem. In the following section, we test our method by constructing known sets of states MU to a number of pairs consisting of the identity and a complex Hadamard matrix of order 6.

4. Testing the method: Tao, Fourier and Ditā matrices

In this section, we apply the approach described above to four cases which have been studied before, reproducing successfully known results. We will (i) search for states simultaneously MU to the identity matrix \( I \) and Tao’s matrix \( S_6^{(0)} \), the only known isolated Hadamard matrix of order 6; (ii) we will derive the complete set of vectors MU to the pair \([I, F_6]\) with the numerical results being, in fact, so accurate that we are able to deduce an interesting analytic result about this set; (iii) we are able to confirm that there are no quadruples containing members of the Fourier family \( F_6(a, b) \), and (iv) we will search for states MU to the standard basis and members of the one-parameter Ditā family \( D_6^{(1)}(c) \). The results presented in this section are summarized in the first three rows of table 1 in section 6.

(i) Tao’s matrix \( S_6 \). The pair \([I, S_6^{(0)}]\) cannot be complemented by six orthogonal vectors to form a triplet of MU bases [29]. We are able to confirm this result by unsuccessfully searching for a third basis by means of the imposition operator. We found 90 vectors MU to the pair \([I, S_6^{(0)}]\), but a third MU base cannot be constructed from them.

(ii) Fourier matrix \( F_6 \). It is impossible to construct four MU bases which contain the pair \([I, F_6]\) [12, 18, 30, 31]. More specifically, it is known that 48 vectors exist which are MU to this pair of bases, giving rise to 16 different ways to construct a triplet of MU bases.
We have been able to unambiguously identify 48 vectors MU to $\{I, F_6\}$, and they agree with the known solutions [12, 14, 29–31]. A careful analysis of the numerical expressions revealed that the components of 12 of the vectors can be expressed solely in terms of sixth roots of unity, while the remaining 36 vectors also depend on Björck’s number,

$$a = \frac{1 - \sqrt{3}}{2} + i \sqrt{3} \frac{1}{2},$$

(23)

which is unimodular, and occurs as $a, a^*, a^2, (a^3)^*$, where $*$ means complex conjugation. The analytic expression for the number $a$ has been found from the numerical results by imposing the unbiasedness of a solution to the pair $\{I, F_6\}$.

It turns out that the 48 vectors can be grouped into three sets, each corresponding to one orbit under the Weyl–Heisenberg group. To see this, let us first define the displacement operators $D_p$ by

$$D_p = \tau^{p_1} X^{p_2} Z^{p_2},$$

(24)

with $p \equiv (p_1, p_2) \in \mathbb{Z}_d^2$, where $X$ and $Z$ are the shift and phase operators, respectively, defined by their actions on the states of the canonical basis,

$$X \vert \phi_k \rangle = \vert \phi_k + 1 \rangle, \quad \text{and} \quad Z \vert \phi_k \rangle = \omega^k \vert \phi_k \rangle.$$  

(25)

Three vectors generating the mentioned orbits under Weyl–Heisenberg group are given by

$$v_1 = \frac{1}{\sqrt{6}} (1, i, \omega^3, i, 1, i\omega^5),$$

(26)

$$v_2 = \frac{1}{\sqrt{6}} (1, -i, \omega^3, -i, 1, -i\omega^5),$$

(27)

$$v_3 = \frac{1}{\sqrt{6}} (1, ia, a^2, -ia^2, -a, -i),$$

(28)

with $\omega = e^{\pi i/6}$; we noted that $v_1$ and $v_2$ are eigenvectors of $D_{(\mu, 0)}$ and $D_{(\mu, 5\mu)}$, respectively, for every $\mu = 0, \ldots, d - 1$. Consequently, the two orbits generated by $v_1$ and $v_2$ each have six elements only consisting of the so-called Gaussian states [14] which, in fact, can be written as product vectors if we swap components 2 and 5 [32]. We understand the origin of the Gaussian vectors very well: the eigenvectors of the operators $\{D_{(1,0)}, D_{(0,1)}, D_{(1,1)}\}$—that is, the bases consisting of the eigenvectors of $X, Z$ and $XZ$—form a triplet of MU bases in any dimension [33]. Every eigenvector of $XZ$ in dimension 6 is a member of the orbit generated by $v_1$, whereas the orbit generated by $v_2$ is its complex conjugated orbit, in agreement with the fact that $v_2 = v_1^*$. Given an MU vector of the pair $\{I, F_6\}$ it is well known that its complex conjugate is also an MU vector in any finite dimension. Moreover, this is also valid in infinite dimension and it is related to Perelomov’s conjecture about the existence of Pauli partners [34]. The origin of the vector $v_3$, however, is not clear to us; it is not an eigenvector of any displacement operator, and it gives rise to an orbit with 36 different states.

Finally, in condensed form, the 48 MU vectors can be written as

$$\{D_{(\mu, 0)} v_1\}_{\mu \in \mathbb{Z}_d}$$

(29)

$$\{D_{(\mu, 0)} v_2\}_{\mu \in \mathbb{Z}_d}$$

(30)

$$\{D_{(\mu, \mu)} v_3\}_{\mu, \nu \in \mathbb{Z}_d}.$$  

(31)

Both the first and second set define a circulant matrix each, while the last set give rise to six circulant matrices. These observations generalize to other dimensions $d$ as follows.
Proposition 4.1. Let \(|\psi\rangle\) be a state MU to the pair \([I, F_d]\), where \(F_d\) is the Fourier matrix defined in dimension \(d\). Then, the set \([D_p|\psi\rangle\}_{p=2}^{d^2}\) defines an orbit of MU vectors which has \(d\) elements if \(|\psi\rangle\) is an eigenvector of any operator \(D_p\) and it has \(d^2\) elements if \(|\psi\rangle\) is not an eigenvector of any \(D_p\).

The proof of the proposition is trivial because the pair of bases of \(C^d\) defined by \([I, F_d]\) is invariant under the action of the displacement operators. Also, the eigenvectors of \(D_{(u,\mu,\nu)}\) are shifted cyclically under the action of \(D_{(\mu',\nu',v')}\) for every \(\mu'=0, \ldots, d-1\) and \(v' \neq v\) [35].

(iii) Fourier family \(F^{(2)}_6(a, b)\). We have attempted to extend pairs of the form \([I, F^{(2)}_6(a, b)]\) for \(10^5\) randomly chosen values of \(a\) and \(b\), taken from the entire parameter range. In each case, we found a triplet of MU bases and we could not find a single additional vector MU to it.

(iv) Dîţă family \(D^{(1)}_6(c)\). The Dîţă family \(D^{(1)}_6(c)\) [36] is an affine one-parameter family of complex Hadamard matrices in dimension 6 which is closely related to the Fourier family. Bengtsson et al [14] found two triplets of MU bases which extend the pair \([\mathbb{I}, D^{(1)}_6(0)]\).

To do so, they used a modified ‘24th-roots program’ which lists all orthonormal bases whose vectors have 24th roots of unity as well as the number \(b_2 = (-1 + 2i)/\sqrt{5}\) (and its complex conjugate) as components.

In the numerical simulations realized with the physical imposition operator, we have considered \(10^4\) random choices of the parameter \(c\). We found ten triplets of MU bases containing the pair \([\mathbb{I}, D(0)]\), but only two of them are inequivalent, in agreement with [14]. It is not difficult to find the analytic form of the triplets by an educated guess. The exact value of the number \(b_2\) was found again by imposing the unbiasedness of a solution to the pair \([\mathbb{I}, D(0)]\).

Explicitly, the inequivalent triplets we find are \([\mathbb{I}, D(0), H_m]\), \(m = 1, 2\), where

\[
H_1 = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
-i & -i & \omega^2 & \omega^{10} & \omega^{10} & \omega^2 \\
-ib_2 & ib_2 & \omega^9 & \omega^{21} & \omega^9 & \omega^{21} \\
-i & -i & \omega^{10} & \omega^2 & \omega^2 & \omega^{10} \\
ib_2 & -ib_2 & \omega^{13} & \omega^{17} & \omega^5 & \omega \\
ib_2 & -ib_2 & \omega^5 & \omega & \omega^{13} & \omega^{17}
\end{pmatrix},
\]

(32)

\[
H_2 = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
ib_2^* & -ib_2^* & \omega^{19} & \omega^7 & \omega^{23} & \omega^{11} \\
ib_2^* & ib_2^* & \omega^5 & \omega^7 & \omega^3 & \omega^{15} \\
ib_2^* & -ib_2^* & \omega^{11} & \omega^3 & \omega^7 & \omega^{19} \\
i & i & \omega^{22} & \omega^{22} & \omega^{14} & \omega^{14} \\
i & i & \omega^{14} & \omega^{14} & \omega^{22} & \omega^{22}
\end{pmatrix},
\]

(33)

and \(\omega = e^{2\pi i/24}\). The MU vectors are given by the columns of the matrices \(H_1\) and \(H_2\). Interestingly, both of them are equivalent to a member of the Fourier family. We have verified that these analytical expressions are indeed solutions of the problem.

The two inequivalent triplets were found among the first three triplets obtained numerically, and no other inequivalent triplet was found in the next 100 runs of our program. This represents strong numerical evidence that no more than two inequivalent triplets exist which contain the pair \([\mathbb{I}, D(0)]\). Moreover, both triplets occur with nearly equal frequency: we found \([\mathbb{I}, D(0), H_1]\) 48 times, while \([\mathbb{I}, D(0), H_2]\) occurred 52 times, an observation which can be explained if one assumes that the basin of attraction of every MU vector has the same size. This apparent symmetry has been noted so far in each imposition-operator search for MU bases, whatever the dimension \(d\) [26, 27].
Triplets of MU bases containing the pair \([\mathbb{I}, D_6^{(1)}(c)]\) have also been found for many other values of the parameter \(c\); none of the resulting triplets seems to allow for even a single further MU vector.

5. Karlson’s non-affine families

The most interesting property of the method defined in section 3 is that its computational costs do not increase when we consider non-affine families. This advantage can be used to analyze the construction of triplets from a pair of the form \([\mathbb{I}, H]\), where \(H\) belongs to a non-affine family of complex Hadamard matrices. Little seems to be known about extending such triplets, so that the method presented here is the first efficient way to study them over the entire parameter range of the families. We have performed computations for pairs of the form \([\mathbb{I}, K_6^{(2)}]\) and \([\mathbb{I}, K_6^{(3)}]\), and it seems that they cannot be extended to four MU bases (up to a possible null measure set of the parameters). Moreover, many pairs can be extended to a triplet only for a non-trivial subset of parameters. Let us start with the family \(K_6^{(2)}\).

5.1. Karlsson’s biparametric family

Karlsson has found a two-parameter non-affine family of complex Hadamard matrices \(K_6^{(2)}\) in dimension 6 [37], which contains the families \(D_6^{(1)}, M_6^{(1)}\) and two subfamilies of the Fourier family. The Diţă family \(D_6^{(1)}(t)\) is equivalent to the four corners \(K_6^{(2)}(\pm \pi/2, \pm \pi/2)\), whereas \(K_6^{(2)}(x, 0) \sim F_6^{(2)}(x, x)\) and \(K_6^{(2)}(0, x) \sim (F_6^{(2)}(x, x))^t\). Also, Matolcsi family determines one of the diagonals, that is, \(K_6^{(2)}(x, x) \sim M_6^{(1)}(x)\). All these subfamilies are explicitly obtained from \(K_6^{(2)}\) in Karlsson’s paper [37]. Note that a subset of the Fourier family and its transpose define the horizontal and vertical axes, respectively, of the parameter space of \(K_6^{(2)}\). Also, the Fourier matrix \(F_6^{(2)}(0, 0)\) is equivalent to the center \(K_6^{(2)}(0, 0)\).

The results of our attempts to extend pairs of the form \([\mathbb{I}, K_6^{(2)}(x_1, x_2)]\) to triplets are presented in figure 1. In this figure, a black dot at the point \((x_1, x_2)\) means that a triplet has been found. Previously known results about affine families indicate that a triplet of MU bases can be obtained in the full range of the family [5, 14, 17, 38], as far as we know. The evidence presented in figure 1 shows that triplets of MU bases only exist for a subset of parameters if the family is non-affine. In these simulations, we have considered the convergence of the sequences according to the upper bound 0.01 established in equation (22) and we have also considered the bounds 0.03, 0.05 and 0.08. In all cases, we found the same results, which are evidence for the stability of the solutions.

Furthermore, figure 1 clearly suggests the existence of new symmetries. The Fourier matrix \(F_6\) and the Diţă family \(D_6^{(1)}(t)\) seem to be privileged in the problem of constructing triplets from a pair of the form \([\mathbb{I}, K_6^{(2)}(x_1, x_2)]\): both of them are centers of symmetries in figure 1. Let us prove all symmetries existing in the family \(K_6^{(2)}\), defined as

\[
K_6^{(2)}(x_1, x_2) = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & z_1 & -z_1 & z_1 & -z_1 \\
1 & z_2 & -f_1 & -z_2 f_2 & -f_3 & -z_2 f_4^* \\
1 & -z_2 & -z_1 f_2^* & z_1 z_2 f_1^* & -z_1 f_4 & z_1 z_2 f_3 \\
1 & z_2 & -f_3^* & -z_2 f_4^* & f_1 & -z_2 f_2 \\
1 & -z_2 & -z_1 f_4 & z_1 z_2 f_3 & -z_1 f_2^* & z_1 z_2 f_1^* \\
\end{pmatrix}, \quad (34)
\]
where \( z_1 = e^{i x_1} \) and \( z_2 = e^{i x_2}, -\pi/2 \leq x_1, x_2 \leq \pi/2 \) and the four functions

\[
\begin{align*}
    f_1 &= f(+x_1, +x_2), \\
    f_2 &= f(+x_1, -x_2), \\
    f_3 &= f(-x_1, -x_2), \\
    f_4 &= f(-x_1, +x_2),
\end{align*}
\]  

are defined in terms of a single function, namely

\[
f(x_1, x_2) = e^{i(x_1+x_2)/2} \left( \cos \left( \frac{x_1 - x_2}{2} \right) - i \sin \left( \frac{x_1 + x_2}{2} \right) \right) \times \left( \frac{1}{2} + i \sqrt{\frac{1}{1 + \sin(x_1) \sin(x_2)} - \frac{1}{4}} \right).
\]  

Karlsson has shown that

\[
f(x_1 + \pi, x_2) = z_2 f(x_1, -x_2),
\]  

\[
f(x_1, x_2 + \pi) = z_1 f(-x_1, x_2),
\]  

meaning that

\[
K_6^{(2)}(x_1 + \pi, x_2) = K_6^{(2)}(x_1, x_2) P_{34} P_{56},
\]  

and

\[
K_6^{(2)}(x_1, x_2 + \pi) = P_{36} P_{43} K_6^{(2)}(x_1, x_2),
\]

where \( P_{34} \) and \( P_{56} \) are permutations matrices. Consequently, one may restrict both parameters \( x_1 \) and \( x_2 \) to the interval \([-\pi/2, \pi/2]\).
Figure 2. Karlsson’s family $K^{(2)}_6(x_1, x_2)$ is equivalent to the gray triangle; note that $-\frac{\pi}{2} \leq x_j \leq \frac{\pi}{2}$, $j = 1, 2$.

Inspired by the symmetries of the graph shown in figure 1 and taking into account equations (35) and (36), we note that

$$K^{(2)}_6(x_1, x_2) = P_{36}P_{45}K^{(2)}_6(x_1, x_2), \quad \text{(41)}$$

$$K^{(2)}_6(-x_1, x_2) = P_{36}P_{45}K^{(2)}_6(x_1, x_2); \quad \text{(42)}$$

using the symmetry $f(x_1, x_2) = f(x_2, x_1)$, we also obtain

$$K^{(2)}_6(x_1, x_2) = K^{(2)}_6(x_2, x_1). \quad \text{(43)}$$

Equations (41)–(43) reveal the symmetry apparent in figure 1, and we consider it unlikely that any further symmetries exist. The family $K^{(2)}_6(x_1, x_2)$ with $-\pi/2 \leq x_1, x_2 \leq \pi/2$ is divided into eight triangles of the same area, each of them containing one copy of the complete family. Therefore, it is sufficient to consider values in the triangle $x_1 \in [0, \pi/2]$, $x_2 \leq x_1$, i.e. the shaded area in figure 2. In this figure, we show that Matolcsi’s family $M^{(1)}_6$ is located on the both diagonals of the square. As we will show later, we can construct triplets of MU bases from $M^{(1)}_6$, which means that it should appear in figure 1. However, the set $\{M^{(1)}_6 \times \}$ is of measure zero within the family $K^{(2)}_6(x_1, x_2)$; since the parameters $(x_1, x_2)$ are chosen at random, the probability of observe it vanishes.

5.2. Karlsson’s tri-parametric family

A tri-parametric non-affine family of complex Hadamard matrices has been recently found by Karlsson [39], reading explicitly:

$$K^{(3)}_6(\theta, \phi, \psi) = \begin{pmatrix} F_2 & Z_1 & Z_2 \\ Z_3 & \frac{1}{2}Z_3AZ_1 & \frac{1}{2}Z_3BZ_2 \\ \frac{1}{2}Z_4BZ_1 & \frac{1}{2}Z_4AZ_2 \end{pmatrix}, \quad \text{(44)}$$
where
\[ F_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad A = \begin{pmatrix} A_{11} & A_{12} \\ A_{12}^* & -A_{11}^* \end{pmatrix}, \quad B = -F_2 - A, \] (45)
and
\[ Z_i = \begin{pmatrix} 1 & 1 \\ z_i & -z_i \end{pmatrix}, \quad i = 1, 2; \quad Z_i = \begin{pmatrix} 1 & z_i \\ 1 & -z_i \end{pmatrix}, \quad i = 3, 4. \] (46)
The entries of \( A \) are given by
\[ A_{11} = -\frac{1}{2} + i \frac{\sqrt{3}}{2} (\cos(\theta) + e^{-i\phi} \sin(\theta)), \] (47)
\[ A_{12} = -\frac{1}{2} + i \frac{\sqrt{3}}{2} (-\cos(\theta) + e^{i\phi} \sin(\theta)), \] (48)
and the entries of \( Z_i \) are
\[ z_1 = e^{i\psi}, \] (49)
\[ z_2^2 = M_A^{-1}(M_B(z_1^2)), \] (50)
\[ z_3^2 = M_A(z_1^2), \] (51)
\[ z_4^2 = M_B(z_1^2). \] (52)
Here, \( M \) denotes the Möbius transformation, defined by
\[ M(z) = \frac{\alpha z - \beta}{\beta z - \alpha^*}, \] (53)
with \( \alpha_A = A_{12}, \beta_A = A_{11}, \) and \( \alpha_B = B_{12}, \beta_B = B_{11}, \) and \( \theta, \phi, \psi \in [0, \pi). \)

This family contains the non-affine family \( K_6^{(2)} \) and it also contains the complete set of the so-called \( H_2 \)-reducible matrices. In dimension 6, a complex Hadamard matrix is \( H_2 \)-reducible if it contains nine \( 2 \times 2 \) submatrices that are Hadamard matrices. Let us analyze an interesting particular case. It follows from equations (47) and (48) that the subfamily \( K_6^{(3)}(0, \phi, \psi) \) does not depend on the parameter \( \phi \). In this case, the Möbius transformations in equations (50)–(52) turn into the identity irrespective of the value of \( z \). Therefore, we obtain an affine one-parameter family
\[ K_6^{(3)}(0, \phi, \psi) = (P_{46} F_2 \otimes F_1) \circ \text{Exp}(iR(\psi)), \] (54)
which is contained in the Fourier family \( F_6^{(2)} \). Here, the matrix \( R(\psi) \) is defined by
\[ R(\psi) = \begin{pmatrix} \bullet & \bullet & \bullet & \psi & \psi & \bullet \\ \bullet & \bullet & \bullet & \psi & \psi & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \psi & \psi & \psi & \psi & \psi & \bullet \end{pmatrix}, \] (55)
where \( \bullet \) means a null entry. The permutation matrix \( P_{46} \) interchanges rows 4 and 6. This subfamily allows a triplet for any \( \psi \in [0, \pi) \), because it is contained in the Fourier family \( F_6^{(2)}(a, b) \), which admits a triplet for any value of \( a \) and \( b \).

Numerical simulations from considering the family \( K_6^{(3)} \) are shown in figures 3(a)–(d). As we can see, these figures strongly suggest the existence of reflection symmetries in the three variables \( \theta, \phi \) and \( \psi \). However, we have not been able to find them analytically even in the simplest case \( \psi = 0 \). There are highly non-trivial diagonal matrices and row permutations which do not allow us to reveal the hidden symmetries. On the other hand, if a random value of \( \psi \) is considered we always obtain the same kind of two-dimensional objects. No fractal structures have been detected for any value of the parameters. Consequently, we have a representative description of the general case, in the sense that the evolution of the parameter \( \psi \) gives us a smooth connection between these four figures (figures 3(a)–(d)).
Figure 3. Triplets in Karlsson’s family $K_{6}^{(3)}(\theta, \phi, \psi)$ for some fixed values of $\psi$. (a) Triplets for $K_{6}^{(3)}(\theta, \phi, 0)$. (b) Triplets for $K_{6}^{(3)}(\theta, \phi, \pi/4)$. (c) Triplets for $K_{6}^{(3)}(\theta, \phi, \pi/2)$. (d) Triplets for $K_{6}^{(3)}(\theta, \phi, 3\pi/4)$.

6. Summary and conclusions

We have presented an efficient numerical method to construct sets of mutually unbiased (MU) bases in a finite dimension. The main advantage of our method appears when non-affine families of complex Hadamard matrices are considered, where the standard method to solve coupled polynomial equations (Buchberger’s algorithm) often stalls due to excessive memory requirements. Our method numerically solves the problem for non-affine families with the same computational cost as for affine families.

To test our approach we first used it to determine the well-known 48 MU vectors to the pair $\{I, F_6\}$. We have been able to prove that they determine three orbits under the Weyl–Heisenberg group. Also, considering the Dîța matrix we found two triplets that agree with a result obtained previously [14].

Table 1 summarizes the results obtained in this paper, indicating the maximal set of MU bases that can be constructed from pairs of MU bases associated with various families in dimension 6. In the cases of affine families and the non-affine family $B_{6}^{(1)}$, we found triplets in the entire range of the parameters, whereas the isolated matrix $S_{6}^{(0)}$ does not allow a triplet. This property of $S_{6}^{(0)}$ has been previously found by Brierley and Weigert [29].
Table 1. Maximal set of MU bases for some families. The last four cases are new results.

| Pair                        | Kind            | Maximal set of MU bases                                                                 |
|-----------------------------|-----------------|----------------------------------------------------------------------------------------|
| \{I, S_{6}^{(0)}\}         | Isolated        | 2                                                                                      |
| \{I, D_{6}^{(1)}(c)\}      | Affine          | 3, \forall c \in \left[ -\frac{1}{2}, \frac{1}{2} \right]                          |
| \{I, F_{6}^{(2)}(a, b)\}   | Affine          | 3, \forall a, b \in [0, 2\pi)                                                        |
| \{I, B_{6}^{(1)}(s)\}      | Non-affine      | 3, \forall s \in \left[ -\pi, \arccos\left(\frac{-1+\sqrt{3}}{2}\right) \right] \cup \left[ \arccos\left(\frac{-1+\sqrt{3}}{2}\right), -\pi \right] |
| \{I, M_{6}^{(1)}(t)\}      | Non-affine      | \begin{cases} 3 & \text{if } t \in [0.5309\pi, 0.9157\pi] \\ 2 & \text{otherwise} \end{cases} |
| \{I, K_{6}^{(2)}(s_{1}, s_{2})\} | Non-affine   | \begin{cases} 3 & \text{in black regions of figure 1} \\ 2 & \text{in white regions of figure 1} \end{cases} |
| \{I, K_{6}^{(3)}(\theta, \phi, \psi)\} | Non-affine   | \begin{cases} 3 & \text{in black regions from figures 3 (a)-(d)} \\ 2 & \text{in white regions from figures 3 (a)-(d)} \end{cases} |

In the simulation realized for the non-affine family \(B_{6}^{(1)}\), we have considered 10,000 random choices of its parameter, and we obtained a triplet in each case. This is the only non-affine family where we found a triplet for each value. The non-affine family \(M_{6}^{(1)}\) defined in the range \(t \in (\pi/2, \pi] \cup (3\pi/2, 2\pi]\) does not allow a triplet in its full range. We have realized three simulations considering 1000, 10,000 and 100,000 random choices of the parameter \(t\) and we obtain the same results. That is, a part of the family \(M_{6}^{(1)}\) does not allow us to construct a triplet of MU bases (see Table 1).

In the cases of Karlsson’s families \(K_{6}^{(2)}\) and \(K_{6}^{(3)}\), we have considered two million and eight million random choices, respectively, sampling the entire parameter ranges of both families. We have shown that these two families extend to triplets at most. The property that a triplet of MU bases can be found only for a reduced set of parameters of a family is a new result presented here for the first time. In addition, we identified new symmetries that reduce the range of the parameters of the family \(K_{6}^{(2)}\).

Finally, in our investigation of more than ten million complex Hadamard matrices belonging to non-affine families we could not find a single vector being MU to a triplet. This evidence supports the conjecture that no more than three MU bases can be constructed in dimension 6.

Acknowledgments

I specially thank Stefan Weigert for his invaluable help in order to make this paper possible. This work is supported by Grants FONDECyT No 3120066 and MSI P10-030-F.

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing pp 175–9
[2] Bruß D 1998 Optimal eavesdropping in quantum cryptography with six states Phys. Rev. Lett. 81 3018–21
[3] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 Security of quantum key distribution using d-level systems Phys. Rev. Lett. 88 127902
[4] Spengler C et al 2012 Entanglement detection via mutually unbiased bases Phys. Rev. A 86 022311
[5] Durt T, Englert B, Bengtsson I and Życzkowski K 2010 On mutually unbiased bases Int. J. Quantum Inform. 8 535–640
[6] Gibbons K S, Hoffman M J and Wootters W K 2004 Discrete phase space based on finite fields Phys. Rev. A 70 1–23
[7] Bengtsson I 2005 Mubs, polytopes and finite geometries AIP Conf. Proc. 750 63–69
[8] Aharonov Y and Englert B G 2001 The mean king’s problem: spin 1 Z. Naturf. A 56 16–9
[9] Zauner G 1999 PhD Thesis University of Wien
[10] Archer C 2005 There is no generalization of known formulas for mutually unbiased bases J. Math. Phys. 46 022106
[11] Jaming P, Matolcsi M and Móra P 2010 The problem of mutually unbiased bases in dimension 6 Cryptogr. Commun. 2 211–20
[12] Grassl M 2004 On SIC-POVMs and MUBs in dimension 6 EQUIP: ERATO Conf. on Quantum Information Science pp 60–1
[13] Butterley P and Hall W 2007 Numerical evidence for the maximum number of mutually unbiased bases in dimension six Phys. Lett. A 369 5–8
[14] Bengtsson I, Bruzda W, Ericsson A, Larsson J, Tadej W and Życzkowski K 2007 MUBs and Hadamards of order six J. Math. Phys. 48 052106
[15] Brierley S and Weigert S 2008 Maximal sets of mutually unbiased quantum states in dimension six Phys. Rev. A 78 042312
[16] Brierley S and Weigert S 2010a Mutually unbiased bases and semi-definite programming J. Phys.: Conf. Ser. 254 012008
[17] Jaming P et al 2009 A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6 J. Phys. A: Math. Theor. 42 245305
[18] Brierley S 2009a Mutually unbiased bases in low dimensions PhD Thesis University of York
[19] Ivanovic I 1981 Geometrical description of quanlitative state determination J. Phys. A: Math. Gen. 14 3241
[20] Wootters W and Fields B 1989 Optimal state-determination by mutually unbiased measurements Ann. Phys. 191 363
[21] Bengtsson I 2007 Three ways to look at mutually unbiased bases AIP Conf. Proc. 889 40–51
[22] http://chaos.if.uj.edu.pl/karol/hadamard
[23] Brierley S, Weigert S and Bengtsson O 2010 All mutually unbiased bases in dimensions two to five Quantum Inform. Comp. 10 0803–20
[24] Buchberger B 1965 An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal PhD Dissertation University of Innsbruck
[25] McNulty D and Weigert S 2012 On the impossibility to extend triples of mutually unbiased product bases in dimension six Int. J. Quantum Inform. 10 5
[26] Goyeneche D M and de la Torre A C 2008 State determination: an iterative algorithm Phys. Rev. A 77 042116
[27] Goyeneche D and de la Torre A 2011 Quantum state reconstruction from dynamical systems theory arXiv:1103.3213
[28] Hellinger E 1907 Die Orthogonalinvarianten quadratischer Formen von unendlich vielen Variablen Dissertation Göttingen
[29] Brierley S and Weigert S 2009 Constructing mutually unbiased bases in dimension six Phys. Rev. A 79 052316
[30] Björck G and Fröberg R 1991 A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots J. Symb. Comput. 12 329
[31] Björck G and Saffari B 1995 New classes of finite unimodular sequences with unimodular Fourier transforms. Circulant Hadamard matrices with complex entries C. R. Acad. Sci., Paris I 320 319–24
[32] McNulty D and Weigert S 2012 All mutually unbiased product-bases in dimension 6 J. Phys. A: Math. Theor. 45 135307
[33] de la Torre A and Goyeneche D 2003 Quantum mechanics in finite-dimensional Hilbert space Am. J. Phys. 71 49–54
[34] Moroz B Z and Perelomov A M 1994 On a problem posed by Pauli Theor. Math. Phys. 101 1200–4
[35] Bandyopadhyay S et al 2002 A new proof of the existence of mutually unbiased bases Algorithmica 34 512–28
[36] Ditt P 2004 Some results on the parameterization of complex Hadamard matrices J. Phys. A: Math. Gen. 37 5355
[37] Karlsson B 2009 Two-parameter complex Hadamard matrices for N = 6 J. Math. Phys. 50 082104
[38] Szőlösi F 2011 Construction, classification and parametrization of complex Hadamard matrices PhD Thesis arXiv:1110.5590
[39] Karlsson B 2011 Three-parameter complex Hadamard matrices of order 6 Linear Algebra Appl. 434 247