A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6

2009 J. Phys. A: Math. Theor. 42 245305

(http://iopscience.iop.org/1751-8121/42/24/245305)

J. Phys. A: Math. Theor. **42** (2009) 245305 (25pp) doi:10.1088/1751-8113/42/24/245305

A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6

Philippe Jaming[1], **Máté Matolcsi**[2,3], **Péter Móra**[3], **Ferenc Szöllősi**[4] **and Mihály Weiner**[2]

[1] Université d'Orléans, Faculté des Sciences, MAPMO - Fédération Denis Poisson, BP 6759, F 45067 Orléans Cedex 2, France
[2] Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences POB 127 H-1364 Budapest, Hungary
[3] BME Department of Analysis, Egry J. u. 1, H-1111 Budapest, Hungary
[4] Institute of Mathematics and its Applications, Central European University (CEU), H-1051, Nádor u. 9., Budapest, Hungary

E-mail: philippe.jaming@univ-orleans.fr, matomate@renyi.hu, morapeter@gmail.com, szoferi@gmail.com and mweiner@renyi.hu

Received 26 February 2009, in final form 29 April 2009
Published 28 May 2009
Online at stacks.iop.org/JPhysA/42/245305

Abstract

We exhibit an infinite family of *triplets* of mutually unbiased bases (MUBs) in dimension 6. These triplets involve the Fourier family of Hadamard matrices, $F(a, b)$. However, in the main result of this paper we also prove that for any values of the parameters (a, b), the standard basis and $F(a, b)$ *cannot be extended to a MUB-quartet*. The main novelty lies in the *method* of proof which may successfully be applied in the future to prove that the maximal number of MUBs in dimension 6 is three.

PACS numbers: 03.67.−a, 02.10.Ud

1. Introduction

The notion of mutually unbiased bases (MUBs) emerged in the literature of quantum mechanics in 1960 in the works of Schwinger [27]. It now constitutes a basic concept of quantum information theory and plays an essential role in quantum tomography [20, 31], quantum cryptography [4, 6, 26], the mean king problem [1] as well as in constructions of teleportation and dense coding schemes [30].

Recall that two orthonormal bases of $\mathbb{C}^d$, $\mathcal{A} = \{\mathbf{e}_1, \dots, \mathbf{e}_d\}$ and $\mathcal{B} = \{\mathbf{f}_1, \dots, \mathbf{f}_d\}$ are said to be *unbiased* if, for every $1 \leqslant j, k \leqslant d$, $|\langle \mathbf{e}_j, \mathbf{f}_k\rangle| = \frac{1}{\sqrt{d}}$. A set $\mathcal{B}_0, \dots, \mathcal{B}_m$ of orthonormal bases is said to be *mutually unbiased* if any two of them are unbiased. It is well known (see, e.g., [2, 5, 16, 19, 22, 31]) that the number of mutually unbiased bases in $\mathbb{C}^d$ cannot exceed $d + 1$. It is also known that $d + 1$ such bases can be constructed if the dimension d is a prime or a prime power (see, e.g., [2, 12–14, 20, 23, 31]). Apart from this, very little is known except for the fact that there are always $p + 1$ mutually unbiased bases in $\mathbb{C}^d$ where p is the smallest prime divisor of d. Thus, the first case where the largest number of mutually unbiased bases is unknown is $d = 6$.

Problem 1.1. *What is the maximal number of pairwise mutually unbiased bases in* $\mathbb{C}^6$?

Although this famous open problem has received considerable attention over the past few years (see [5, 9, 10, 25, 28]), it remains wide open. Since $6 = 2 \times 3$, we know that there are at least three mutually unbiased bases in $\mathbb{C}^6$, but so far tentative numerical evidence [9, 10, 11, 32] suggests that there are no more than three, a fact apparently first conjectured by Zauner [32].

One reason for the slow progress is that mutually unbiased bases are naturally related to *complex Hadamard matrices* (and the classification of such matrices in dimension 6 seems to be very difficult). Indeed, if the bases $\mathcal{B}_0, \ldots, \mathcal{B}_m$ are mutually unbiased, we may identify each $\mathcal{B}_l = \left\{\mathbf{e}_1^{(l)}, \ldots, \mathbf{e}_d^{(l)}\right\}$ with the *unitary* matrix $U_j = \left[\left\langle \mathbf{e}_k^{(l)}, \mathbf{e}_j^{(1)}\right\rangle\right]_{1\leqslant j,k\leqslant d}$, i.e., the kth column consists of the coordinates of the kth vector of $\mathcal{B}_j$ in the bases $\mathcal{B}_0$. (Throughout this paper the scalar product $\langle ., .\rangle$ of $\mathbb{C}^d$ is linear in the first variable and conjugate-linear in the second.) With this convention, $U_1 = Id$, the identity matrix and all other matrices are unitary and have entries of modulus $1/\sqrt{d}$. Such matrices are called *complex Hadamard matrices*. It is clear that the existence of a family of mutually unbiased bases $\mathcal{B}_0, \ldots, \mathcal{B}_m$ is thus equivalent to the existence of a family of complex Hadamard matrices $H_1, \ldots, H_m$ such that for all $1 \leqslant j \neq k \leqslant m$, $H_j^* H_k$ is again a complex Hadamard matrix. In such a case, we will say that these complex Hadamard matrices are *mutually unbiased*.

A complete classification of complex Hadamard matrices is only available up to dimension 5 (see [18]). The classification in dimension 6 is still out of reach despite recent efforts [3, 25, 28]. This is one of the reasons for problem 1.1 to be difficult.

A natural question that arises in this context is that given two unbiased orthonormal bases, does there always exist a third orthonormal basis that is unbiased to the first two? Or, equivalently, given a complex Hadamard matrix H, does there always exist another one G that is unbiased to H? The answer is negative in such generality. It has recently been proved in [10] that for the matrix S_6 (cf [29] for the notation) there exists no complex Hadamard matrix unbiased to it. A less restrictive question is the following.

Problem 1.2. *Given a Hadamard matrix H, does there always exist some unbiased vectors to H?*

At this stage, it may be worth recalling some invariants of this problem. Assume $H_1, \ldots, H_m$ are mutually unbiased $n \times n$ Hadamard matrices, and let $D, D_1, \ldots, D_m$ be unitary $n \times n$ diagonal matrices $P, P_1, \ldots, P_m$ be $n \times n$ permutation matrices. Then $DPH_iP_iD_i$ are still Hadamard matrices and are still mutually unbiased. We will say that $DPH_i^{(*)}P_iD_i$ is *equivalent* to H_i where the superscript $(*)$ is a choice (the same for all matrices) between complex conjugation or nothing. Note that the effect of this operation is that we may assume that the first *row* of each Hadamard matrix is $d^{-1/2}[1, \ldots, 1]$ and that the first *column of* H_1 is $d^{-1/2}[1, \ldots, 1]$. We may further *order* the remaining rows *and* columns of H_1.

Further, note that if an n-dimensional vector

$$\mathbf{u} = \frac{1}{\sqrt{6}}(1, \mathrm{e}^{2\mathrm{i}\pi\phi_1}, \mathrm{e}^{2\mathrm{i}\pi\phi_2}, \mathrm{e}^{2\mathrm{i}\pi\phi_3}, \mathrm{e}^{2\mathrm{i}\pi\phi_4}, \mathrm{e}^{2\mathrm{i}\pi\phi_5}) \tag{1}$$

is unbiased to the standard basis and to the $n - 1$ first columns of a Hadamard matrix, then it is automatically unbiased to the last one. Hence, we have $n - 1$ unbiased-criteria to be satisfied for the $n-1$ parameters ϕ_j. In generic situations, we therefore expect a finite number of solutions to arise. We know of a non-generic example (in dimension 4) where infinitely many unbiased vectors arise, but of no examples where the number of such vectors is *zero*.

Moving back to the six-dimensional case, we note the significance of problem 1.2. If for a certain complex Hadamard matrix H the number of unbiased vectors is less than 30, then the MUB-pair $\{Id, H\}$ can obviously not be extended to a full set of 7-MUBs (because we would need at least 30 vectors to form another five bases).

Further, it is easy to see that a vector $\mathbf{u}$ of the form (1) is unbiased to the columns of Id and of H if and only if the mapping

$$\mathcal{H}(\phi_1,\phi_2,\phi_3,\phi_4,\phi_5)=\sum_{j=1}^{6}|\langle\mathbf{u},\mathbf{h_j}\rangle| \tag{2}$$

(where $\mathbf{h_j}$ denote the columns of H) has a global maximum at the point $(\phi_1,\phi_2,\phi_3,\phi_4,\phi_5)$ in $\mathbb{T}^5$.

Therefore, a natural way to search numerically for unbiased vectors $\mathbf{u}$ is to start from a random point of the parameter space $(\phi_1,\phi_2,\phi_3,\phi_4,\phi_5)$ in $\mathbb{T}^5$ and find local maxima of $\mathcal{H}$ defined in (2). It is plausible to expect that if we run our numerical search many times, we will find most, or indeed all, unbiased vectors $\mathbf{u}$ in this manner (as well as finding possible other local maxima which we simply discard). There is no guarantee, of course, and we will need to back up our numerical evidence with rigorous mathematical statements.

In most of this paper, we will focus on H belonging to the 'Fourier family'. Let us recall (cf [29]) that this is the two-parameter family of complex Hadamard matrices $F(a,b)$ defined by

$$F(a,b)=\frac{1}{\sqrt{6}}\begin{bmatrix}1&1&1&1&1&1\\1&-\omega^2x&\omega&-x&\omega^2&-\omega x\\1&\omega y&\omega^2&y&\omega&\omega^2y\\1&-1&1&-1&1&-1\\1&\omega^2x&\omega&x&\omega^2&\omega x\\1&-\omega y&\omega^2&-y&\omega&-\omega^2y\end{bmatrix}, \tag{3}$$

where $x=\mathrm{e}^{2\mathrm{i}\pi a}$, $y=\mathrm{e}^{2\mathrm{i}\pi b}$ and $\omega=\mathrm{e}^{2\mathrm{i}\pi/3}$.

Note that $F(0,0)=\mathcal{F}_6$ is the standard Fourier matrix. We may thus see the task of finding unbiased vectors to the standard and the $F(a,b)$ bases as a perturbation of the so-called Pauli problem. Recall that Pauli asked whether a function f in $L^2(\mathbb{R}^d)$ is uniquely determined by its modulus $|f|$ and the modulus of its Fourier Transform $|\widehat{f}|$ (see, e.g., [21] or [15] for some results and further references). The discrete analog of this problem, i.e., the problem of finding finite sequences of complex numbers of modulus one (a_j) such that their Fourier transforms have also modulus 1 (such sequences are called *biunimodular sequences*) has been considered, e.g., in [7, 8]. Our problem can thus be seen as a perturbation of the discrete case in dimension 6.

For the particular case of $H=\mathcal{F}_6$, a full analytical solution of problem 1.2 is actually known [7, 17]: there are exactly 48 vectors, normalized as in (1), that are unbiased with respect to $\{Id,\mathcal{F}_6\}$ and one can form 16 different orthonormal bases $C_1,\ldots,C_{16}$ out of them. However, no pair of bases (C_i,C_j) are unbiased with respect to each other, which means that no triplet $\{I,\mathcal{F}_6,C\}$ can be extended to a mutually unbiased quartet $\{I,\mathcal{F}_6,C,D\}$ (see [17, 10]). What happens if we set $H=F_6(a,b)$ for some generic values a,b? We heuristically expected that in such a case significantly less than 48 unbiased vectors $\mathbf{u}$ should arise. We also expected that only in exceptional cases should there exist a basis C built from these unbiased vectors. These heuristics turned out to be false[5].

We ran the numeric search of finding local maxima of expression (2) for several values of a, b. The results were both surprising and overwhelmingly convincing.

Numeric Evidence 1.3. *For any values of the parameters* (a, b)*, the number of vectors unbiased to the identity matrix and* $F(a, b)$ *is 48. For generic values* (a, b)*, there are eight different orthonormal bases* $C_1(a, b), \ldots, C_8(a, b)$ *that can be formed out of these 48 vectors. For some exceptional values of* (a, b)*, there are more such bases: for* $(a, b) = (0, 0)$ *there are 16, while for* $(a, b) = (1/6, 0)$ *there are 70 such bases*[6]*. However, no mutually unbiased triplet of the form* $(Id, F(a, b), C)$ *can be extended by a further basis to form a mutually unbiased quartet* $(Id, F(a, b), C, D)$*.*

We will back up most of these numerical data by *rigorous analytic results* in subsequent sections[7].

In section 2, we construct an *infinite family of MUB-triplets in the analytic form* involving the Fourier family of Hadamard matrices $F(a, b)$, with $a = 0$ (and some restrictions on b). We have recently been informed by G Zauner that his work [32] also includes an infinite family of MUB-triplets, although the formulae are not made explicit. As the beautiful construction of [32] is scarcely known and is originally written in German, we decided to provide an English version of it in appendix B. We will show, however, that Zauner's family is not equivalent to ours.

One may think that the emergence of an infinite family of MUB-triplets is a major step toward finding a MUB-quartet in dimension 6. In contrast, we prove the following:

Theorem 1.4. *None of the pairs* $(Id, F(a, b))$ *of mutually unbiased orthonormal bases can be extended to a quartet* $(Id, F(a, b), C, D)$ *of mutually unbiased orthonormal bases.*

While this can be disappointing for some, we believe that this is a *breakthrough result* of the paper in that the method we apply here may later be generalized to *settle problem 1.1* and prove that the maximal number of mutually unbiased orthonormal bases in dimension 6 is three.

This paper is organized as follows. Section 2 is devoted to characterizing vectors unbiased to the standard basis and $F(a, b)$, and the construction of an infinite one-parameter family of MUB-triplets. In section 3, we prove theorem 1.4. Finally, in section 4 we attempt to offer some general theoretical reasons behind our results, other than just the sheer numbers and formulae.

This paper is supplemented by two appendices. In appendix A, we provide the computations that lead to theorem 2.4 and that the reader might skip at first reading and in appendix B we give Zauner's construction [32] of another one-parameter family of MUB-triplets.

[5] The authors are grateful for W Bruzda for making the first computer search, with a method other than maximizing expression (2), which indicated that the number of unbiased vectors is more than 40 on average.

[6] The exact number 70 is given in [10].

[7] The authors of [10] have used the technique of Gröbner bases to prove that the number of unbiased vectors is indeed 48 for several (but *finitely many*) tested values of (a, b). In fact, in [10] several members of *all* known Hadamard families are tested, not only the Fourier family. However, the techniques of this paper have the advantage that they enable us to reach rigorous conclusions about the *whole family* $F(a, b)$ and not just the tested values of the parameters.

2. An infinite family of MUB-triplets involving $F(a, b)$

In this section, we first describe a reduced system of equations for any vector $\mathbf{u}$ unbiased to the bases $A = Id$ and $B = F(a, b)$. However, we can only obtain some particular solutions in the closed analytic form in the special case $a = 0$. Nevertheless, these explicit formulae give a *rigorous proof of the existence of an infinite one-parameter family of MUB-triplets* involving $A = Id$ and $B = F(0, b)$. Recall that the numerical evidence actually suggests the existence of MUB-triplets for *all* a, b, with $A = Id$ and $B = F(a, b)$, i.e., a *two-parameter family*. We cannot give a rigorous argument in such generality.

2.1. A reduced system of equations for unbiased vectors

We begin with a useful lemma about vectors unbiased with the Fourier basis in $\mathbb{C}^3$.

Lemma 2.1. *Let* $\omega = \mathrm{e}^{2\mathrm{i}\pi/3}$ *and let* $\alpha, \beta, \gamma \in \mathbb{C}$. *Then*

$$\begin{cases} |\alpha + \beta + \gamma|^2 = 6 \\ |\alpha + \beta\omega + \gamma\omega^2|^2 = 6 \\ |\alpha + \beta\omega^2 + \gamma\omega|^2 = 6 \end{cases} \tag{4}$$

if and only if

$$\begin{cases} |\alpha|^2 + |\beta|^2 + |\gamma|^2 = 6 \\ \alpha\bar{\beta} + \beta\bar{\gamma} + \gamma\bar{\alpha} = 0. \end{cases}$$

Proof. One easily sees that (4) is equivalent to

$$\begin{cases} |\alpha|^2 + |\beta|^2 + |\gamma|^2 + 2\,\mathrm{Re}(\alpha\bar{\beta} + \beta\bar{\gamma} + \gamma\bar{\alpha}) = 6 \\ |\alpha|^2 + |\beta|^2 + |\gamma|^2 + 2\,\mathrm{Re}(\omega^2\alpha\bar{\beta} + \omega^2\beta\bar{\gamma} + \omega^2\gamma\bar{\alpha}) = 6 \\ |\alpha|^2 + |\beta|^2 + |\gamma|^2 + 2\,\mathrm{Re}(\omega\alpha\bar{\beta} + \omega\beta\bar{\gamma} + \omega\gamma\bar{\alpha}) = 6. \end{cases}$$

Then, using the fact that $1 + \omega + \omega^2 = 0$ and adding all three equations, we see that this is equivalent to

$$\begin{cases} |\alpha|^2 + |\beta|^2 + |\gamma|^2 = 6 \\ \mathrm{Re}(\alpha\bar{\beta} + \beta\bar{\gamma} + \gamma\bar{\alpha}) = 0 \\ \mathrm{Re}(\omega\alpha\bar{\beta} + \omega\beta\bar{\gamma} + \omega\gamma\bar{\alpha}) = 0. \end{cases}$$

We conclude by noting that $\mathrm{Re}(z) = 0$ and $\mathrm{Re}(\omega z) = 0$ if and only if $z = 0$. □

Let us now assume that $\mathbf{u} \in \mathbb{C}^6$ is a unit-norm vector that is unbiased to the standard basis:

$$\mathbf{u} = \frac{1}{\sqrt{6}}(1, \bar{c}_1, \bar{c}_2, \bar{c}_3, \bar{c}_4, \bar{c}_5), \qquad |c_1| = |c_2| = |c_3| = |c_4| = |c_5| = 1,$$

where the conjugate signs are introduced for later convenience of calculations.

Recalling the notation $x = \mathrm{e}^{2\mathrm{i}\pi a}$, $y = \mathrm{e}^{2\mathrm{i}\pi b}$, the vector $\mathbf{u}$ is further unbiased with respect to the generalized Fourier basis $F(a, b)$, if and only if

$$|1 + c_1 + c_2 + c_3 + c_4 + c_5| = \sqrt{6} \tag{5}$$

$$|1 - \omega^2 x c_1 + \omega y c_2 - c_3 + \omega^2 x c_4 - \omega y c_5| = \sqrt{6} \tag{6}$$

$$|1 + \omega c_1 + \omega^2 c_2 + c_3 + \omega c_4 + \omega^2 c_5| = \sqrt{6} \tag{7}$$

$$|1 - x c_1 + y c_2 - c_3 + x c_4 - y c_5| = \sqrt{6} \tag{8}$$

$$|1 + \omega^2 c_1 + \omega c_2 + c_3 + \omega^2 c_4 + \omega c_5| = \sqrt{6} \tag{9}$$

$$|1 - \omega x c_1 + \omega^2 y c_2 - c_3 + \omega x c_4 - \omega^2 y c_5| = \sqrt{6}. \tag{10}$$

Applying lemma 2.1 to equations (5), (7) and (9), we obtain

$$|1 + c_3|^2 + |c_1 + c_4|^2 + |c_2 + c_5|^2 = 6 \tag{11}$$

$$(1 + c_3)\overline{(c_1 + c_4)} + (c_1 + c_4)\overline{(c_2 + c_5)} + (c_2 + c_5)\overline{(1 + c_3)} = 0 \tag{12}$$

while applying it to equations (6), (8) and (10), we obtain the following:

$$|1 - c_3|^2 + |x(-c_1 + c_4)|^2 + |y(c_2 - c_5)|^2 = 6 \tag{13}$$

$$(1 - c_3)\overline{x(c_4 - c_1)} + x(c_4 - c_1)\overline{y(c_2 - c_5)} + y(c_2 - c_5)\overline{(1 - c_3)} = 0. \tag{14}$$

But, using the fact that $c_1, \ldots, c_5$ are all of modulus 1, we see that equation (11) is equivalent to

$$\mathrm{Re}(c_3 + c_1\overline{c_4} + c_5\overline{c_2}) = 0. \tag{15}$$

Similarly, as $|x| = |y| = 1$, (13) reads $|1 - c_3|^2 + |c_4 - c_1|^2 + |c_2 - c_5|^2 = 6$ which also reduces to (15).

We have thus proved the following lemma:

Lemma 2.2. *A vector* $\mathbf{u} = \frac{1}{\sqrt{6}}(1, \overline{c}_1, \overline{c}_2, \overline{c}_3, \overline{c}_4, \overline{c}_5))$ *is unbiased to both the standard basis and the generalized Fourier basis* $F(a, b)$ *if and only if all* c_j *have absolute value 1, and the following conditions are fulfilled*

$$\begin{cases} \mathrm{Re}(c_3 + c_1\overline{c_4} + c_5\overline{c_2}) = 0 & (15) \\ (1 + c_3)\overline{(c_1 + c_4)} + (c_1 + c_4)\overline{(c_2 + c_5)} & \\ \quad + (c_2 + c_5)\overline{(1 + c_3)} = 0 & (12) \\ (1 - c_3)\overline{x(c_4 - c_1)} + x(c_4 - c_1)\overline{y(c_2 - c_5)} & \\ \quad + y(c_2 - c_5)\overline{(1 - c_3)} = 0 & (14). \end{cases}$$

Remark 2.3. The most natural way to prove all statements indicated by section 1.3 would be to *solve this system of equations* and show that there are exactly 48 solution vectors for any choice of a, b. This would provide an *exhaustive list of MUB-triplets* involving the generalized Fourier matrices $F(a, b)$. Unfortunately, we have been unable to fulfill this task in this generality and we are not able to give *all* solutions in the closed analytic form.

2.2. An infinite family of MUB-triplets involving $F(0, b)$

In order to obtain analytic formulae for *some* of the arising MUB-triplets, we need to restrict our attention to the case $a = 0$. Even in this case the calculations are rather long and cumbersome, and not very instructive. The full details are presented in appendix A, and we only include the final result here. Note that all emerging formulae are *explicit* so that the correctness of the result can be checked (most conveniently by computer algebra) without going through the detailed calculations.

Theorem 2.4. *Assume that* $\frac{1}{2}\arcsin\frac{\sqrt{5}}{3} \leqslant t \leqslant \frac{\pi}{2} - \frac{1}{2}\arcsin\frac{\sqrt{5}}{3}$. *Introduce the following variables:*

$$\psi = \arccos\frac{\sqrt{2 + \cos 2t}}{2}, \qquad c_3 = -\frac{\cos 2t}{2} + \mathrm{i}\left(1 - \frac{\cos^2 2t}{4}\right)^{1/2} \tag{16}$$

$$\beta = \arccos \frac{\sqrt{3+\sin^2 2t} + 3\sqrt{9\sin^2 2t - 5}}{8 \sin 2t}. \tag{17}$$

Then define φ and $\tilde{\varphi}$ by the equations

$$\cos\varphi = \frac{-\cos^2\psi \cos t + \cos(\beta+\psi)\sin\psi \sin t}{\sin\beta \sin 2t}, \tag{18}$$

$$\sin\varphi = \frac{\sin\psi\cos\psi\cos t - \sin(\beta+\psi)\sin\psi\sin t}{\sin\beta\sin 2t} \tag{19}$$

and

$$\cos\tilde{\varphi} = \frac{-\sin t\sin^2\psi + \cos\psi\cos t\sin(\beta+\psi)}{\sin\beta\sin 2t}, \tag{20}$$

$$\sin\tilde{\varphi} = \frac{\cos\psi\cos(\beta+\psi)\cos t - \cos\psi\sin t\sin\psi}{\sin\beta\sin 2t}. \tag{21}$$

Write $\eta = \mathrm{e}^{\mathrm{i}t}$, $\nu = \mathrm{e}^{\mathrm{i}\varphi}$, $\xi = \mathrm{e}^{\mathrm{i}\tilde{\varphi}}$ and $b = \frac{1}{2\pi}\beta$. Finally define $C(t)$ to be the orthonormal basis given by columns of the matrix

$$\frac{1}{\sqrt{6}}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \bar{c}_3 & \bar{c}_3\omega^2 & \bar{c}_3\omega & -\bar{c}_3 & -\bar{c}_3\omega^2 & -\bar{c}_3\omega \\ \bar{\nu}\eta & \bar{\nu}\eta\omega & \bar{\nu}\eta\omega^2 & \mathrm{i}\bar{\xi}\eta & \mathrm{i}\bar{\xi}\eta\omega & \mathrm{i}\bar{\xi}\eta\omega^2 \\ \bar{c}_3 & \bar{c}_3 & \bar{c}_3 & -\bar{c}_3 & -\bar{c}_3 & -\bar{c}_3 \\ 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\ \bar{\nu}\bar{\eta} & \bar{\nu}\bar{\eta}\omega & \bar{\nu}\bar{\eta}\omega^2 & -\mathrm{i}\bar{\xi}\bar{\eta} & -\mathrm{i}\bar{\xi}\bar{\eta}\omega & -\mathrm{i}\bar{\xi}\bar{\eta}\omega^2 \end{bmatrix}.$$

Then the standard basis, the generalized Fourier basis $F\big(0, b(t)\big)$ and the basis given by $C(t)$ are mutually unbiased.

Remark 2.5. This theorem exhibits an infinite family of MUB-triplets in terms of a parameter t. Each member of the family contains the standard basis and one member of the family $F(0, b(t))$. However, the dependence of t on b is only implicit and seems unsolvable in the closed form. Note also that $b(t)$ does not take the value 0.

We do not claim that we have found all MUB-triplets containing the standard basis and $F(0, b(t))$, but only one such triplet. Actually, section 1.3 shows that there exist other solutions, but we have been unable to describe them all analytically.

Note also that the family of MUB-triplets above is different from that presented in [32]. This fact is shown in appendix B.

Remark 2.6. It is natural to ask whether $C(t)$ provides a new family of complex Hadamard matrices of order 6. This is not the case as $C(t)$ also belongs to the generalized Fourier family $F(a, b)$. This can easily be seen by dephasing the first column and properly reordering the remaining ones.

3. No quartet of mutually unbiased bases involving the identity and $F(a, b)$

In this section, we prove theorem 1.4, i.e., the *non-existence* of quartets of mutually unbiased bases of the form $(Id, F(a, b), C, D)$ for any values of a, b. This will be done via a discretization scheme and an exhaustive computer search after establishing proper estimates of the error terms. We believe that the method can be *generalized* in the future to prove that the maximal number of MUBs in dimension 6 is three.

Proof of theorem 1.4. Let us briefly describe the basic idea and turn to the details later. The proof proceeds by contradiction: assume there exists a MUB-quartet $(Id, F(a,b), C, D)$. First, as described in the introduction, we may take advantage of the equivalence relations of Hadamard matrices to reduce the range of parameters. *A priori*, (a, b) is any point in the square $[0, 1)^2$. But, due to the equivalences described in [5], we can assume without loss of generality that (a, b) lies in the triangle T with vertices $(0, 0)$, $(1/6, 0)$ and $(1/6, 1/12)$ which is a *fundamental region* (see [5] for details).

Next, $\mathrm{e}^{2\mathrm{i}\pi a}$, $\mathrm{e}^{2\mathrm{i}\pi b}$ and all entries of $\sqrt{6}C$ and $\sqrt{6}D$ are unimodular complex numbers. We will thus approximate them by Nth roots of unity and replace the matrix $F(a, b)$ by a matrix $F(\tilde{a}, \tilde{b})$ and $\sqrt{6}C$, $\sqrt{6}D$ by matrices $\sqrt{6}\tilde{C}$, $\sqrt{6}\tilde{D}$ with entries exclusively Nth roots of unity. Of course, in doing so, we will destroy the main features of C, D: namely, $\tilde{C}$ and $\tilde{D}$ are neither unitary nor unbiased to $F(\tilde{a}, \tilde{b})$ (or to each other) anymore. However, if N is large enough, then $(Id, F(\tilde{a}, \tilde{b}), \tilde{C}, \tilde{D})$ will still *approximately* be a MUB-quartet. Moreover, the bounds in these approximations can be precisely controlled. It turns out that if N is large enough, an *exhaustive* computer search shows that no quartet of matrices satisfies the prescribed bounds. This means that the hypothetical quartet $(Id, F(a, b), C, D)$ cannot exist. The code of the computer algorithm and the full documentation of the results are available at the webpage [33]. The running time of the code was about 6 h on a computer with a 3,2 GHz CPU.

Let us now describe the details. Let N be an integer. We partition the interval $[0, 1)$ into N subintervals $I_0^{(N)}, I_1^{(N)}, \ldots, I_{N-1}^{(N)}$ of equal length, i.e., $I_j^{(N)} = [j/N, (j+1)/N)$, and denote by $r_j^{(N)} = (j + 1/2)/N$ the midpoint of $I_j^{(N)}$. Now, if a (resp. b) fall in some interval $I_j^{(N)}$ (resp. $I_m^{(N)}$), we then replace a by $\tilde{a} = r_j^{(N)}$ (resp. b by $\tilde{b} = r_m^{(N)}$). When doing so we must keep in mind that the actual value of a (resp. b) can lie anywhere in the *interval* $I_j^{(N)}$ (resp. $I_m^{(N)}$).

Next, recall that there is no loss of generality in assuming that all vectors in all appearing bases have first coordinate $1/\sqrt{6}$. All other entries have modulus $1/\sqrt{6}$. This has the consequence that all appearing scalar products throughout this section have the form $\langle \mathbf{u}, \mathbf{v}\rangle = \frac{1}{6}\left(1 + \sum_{k=1}^{5} \mathrm{e}^{2\mathrm{i}\pi(\phi_k - \psi_k)}\right)$.

Denote the entries of $\sqrt{6}C$, $\sqrt{6}D$ as $c_{k,j} = \mathrm{e}^{2\mathrm{i}\pi\gamma_{k,j}}$ and $d_{k,j} = \mathrm{e}^{2\mathrm{i}\pi\rho_{k,j}}$ with $\gamma_{k,j}, \rho_{k,j} \in [0, 1)$, and the indexing being set as $0 \leqslant k, j \leqslant 5$. Thus, for $k = 0$ we have $\gamma_{k,j} = \rho_{k,j} = 0$ and for $k \geqslant 1$ each $\gamma_{k,j}, \rho_{k,j}$ falls into some interval $I_\ell^{(N')}$, where N' is another integer (for clarity of notation the dependence of ℓ on $\gamma_{k,j}, \rho_{k,j}$ has been dropped). We define $\sqrt{6}\tilde{C}$, $\sqrt{6}\tilde{D}$ by replacing these entries by $r_\ell^{(N')}$. It turns out that we can take N' smaller than N, which saves a lot of computing time. Actually, our search was carried out with $N = 180$ and $N' = 19$.

Finally, the algorithm runs in two steps. In the first one, we seek all vectors $\tilde{\mathbf{u}}$ of the form

$$\tilde{\mathbf{u}} = \frac{1}{\sqrt{6}}(1, \mathrm{e}^{2\mathrm{i}\pi(j_1+1/2)/N'}, \ldots, \mathrm{e}^{2\mathrm{i}\pi(j_5+1/2)/N'}) \tag{22}$$

that are 'almost' unbiased to $F(\tilde{a}, \tilde{b})$. These vectors are the candidates for the columns of $\tilde{C}$, $\tilde{D}$. The second step then consists of constructing 'almost' orthonormal bases $\tilde{C}$, $\tilde{D}$ out of these vectors and checking whether those can possibly be 'almost' unbiased to each other. Of course, all the 'almost' terms above need to be properly quantified.

Let us now turn to the error term. We want to approximate a column vector of C or D,

$$\mathbf{u} = \frac{1}{\sqrt{6}}(1, \mathrm{e}^{2\mathrm{i}\pi\phi_1}, \mathrm{e}^{2\mathrm{i}\pi\phi_2}, \mathrm{e}^{2\mathrm{i}\pi\phi_3}, \mathrm{e}^{2\mathrm{i}\pi\phi_4}, \mathrm{e}^{2\mathrm{i}\pi\phi_5}) \tag{23}$$

by a vector $\tilde{\mathbf{u}}$ of the form (22), where each ϕ_k has been approximated by some $(j_k+1/2)/N' = r_k^{(N')}$. We must keep in mind that ϕ_k can lie anywhere in the *interval* $[j_k/N', (j_k+1)/N')$. Let us denote by $\mathbf{f}_0, \ldots, \mathbf{f}_5$ the columns of $F(a, b)$ and by $\tilde{\mathbf{f}}_0, \ldots, \tilde{\mathbf{f}}_5$ those of $F(\tilde{a}, \tilde{b})$. By construction $\tilde{\mathbf{u}}$ and $\tilde{\mathbf{f}}_0, \ldots, \tilde{\mathbf{f}}_5$ have the *following property*: there exist numbers ϕ_k in $[j_k/N', (j_k+1)/N')$, and numbers a, b in $\left[\tilde{a} - \frac{1}{2N}, \tilde{a} + \frac{1}{2N}\right)$, $\left[\tilde{b} - \frac{1}{2N}, \tilde{b} + \frac{1}{2N}\right)$ such that the corresponding vectors $\mathbf{u}$ (as in (23)) and $\mathbf{f}_0, \ldots \mathbf{f}_5$ (as in the columns of (3)) are unbiased to each other, i.e., $|\langle \mathbf{u}, \mathbf{f}_k\rangle| = 1/\sqrt{6}$. For a fixed pair of discretization parameters N, N' and a fixed pair of $\tilde{a}, \tilde{b}$, the vectors $\tilde{\mathbf{u}}$ of the form (22) which have the above property will be called *quasi-unbiased to* $F(\tilde{a}, \tilde{b})$, and their set will be denoted by $\mathrm{FUB}_{N,N'}^{\tilde{a},\tilde{b}}$. Our first aim is to find the vectors belonging to $\mathrm{FUB}_{N,N'}^{\tilde{a},\tilde{b}}$ out of all vectors $\tilde{\mathbf{u}}$ of the form (22). Despite having N'^5 possible vectors $\tilde{\mathbf{u}}$, we will see that the set $\mathrm{FUB}_{N,N'}^{\tilde{a},\tilde{b}}$ will be of reasonably small size.

We will need the following lemma which we will refer to as the *trivial error bound*.

Lemma 3.1. *Let I_k and J_k ($1 \leqslant k \leqslant 5$) be closed intervals (possibly degenerate) contained in* $[0, 1]$. *Let L_k and T_k denote the lengths, while m_k and s_k the midpoints of the intervals I_k and J_k, respectively.*

Consider the midpoint sum $S = \frac{1}{6}\left(1 + \sum_{k=1}^{5} \mathrm{e}^{2\mathrm{i}\pi(m_k - s_k)}\right)$. The following two statements hold:

- *if it is possible to select points ϕ_k and ψ_k from the intervals I_k and J_k, such that $\left|\frac{1}{6}\left(1 + \sum_{k=1}^{5} \mathrm{e}^{2\mathrm{i}\pi(\phi_k - \psi_k)}\right)\right| = \frac{1}{\sqrt{6}}$, then*

$$\frac{\pi}{6}\sum_{k=1}^{5}(L_k + T_k) \geqslant \left| |S| - \frac{1}{\sqrt{6}} \right|, \tag{24}$$

- *if it is possible to select points ϕ_k and ψ_k from the intervals I_k and J_k, such that $\frac{1}{6}\left(1 + \sum_{k=1}^{5} \mathrm{e}^{2\mathrm{i}\pi(\phi_k - \psi_k)}\right) = 0$, then*

$$\frac{\pi}{6}\sum_{k=1}^{5}(L_k + T_k) \geqslant |S|. \tag{25}$$

Proof. Let us introduce the 'error function' $E(\underline{x}, \underline{y}) = S - \frac{1}{6}(1 + \sum_{k=1}^{5} \mathrm{e}^{2\mathrm{i}\pi(x_k - y_k)})$, where x_k, y_k are in I_k and J_k, respectively. Note that $|(m_k - s_k) - (x_k - y_k)| \leqslant \frac{1}{2}(L_k + T_k)$ for each $1 \leqslant k \leqslant 5$. The trivial estimate $|\mathrm{e}^{2\mathrm{i}\pi(m_k - s_k)} - \mathrm{e}^{2\mathrm{i}\pi(x_k - y_k)}| \leqslant \pi(L_k + T_k)$ yields $|E(\underline{x}, \underline{y})| \leqslant \frac{\pi}{6}\sum_{k=1}^{5}(L_k + T_k)$. Therefore, the values of the function $\frac{1}{6}\left(1 + \sum_{k=1}^{5} \mathrm{e}^{2\mathrm{i}\pi(\phi_k - \psi_k)}\right)$ stay within a disk of radius $\frac{\pi}{6}\sum_{k=1}^{5}(L_k + T_k)$ around S. In the first statement of the lemma, we thus conclude that the distance of S from the circle of radius $1/\sqrt{6}$ (centered at the origin) is not greater than $\frac{\pi}{6}\sum_{k=1}^{5}(L_k + T_k)$. In the second statement, we conclude that the distance of S from the origin is not greater than $\frac{\pi}{6}\sum_{k=1}^{5}(L_k + T_k)$. These are equivalent to (24) and (25). □

Let us apply this lemma to our particular case. The last five coordinates of $\tilde{\mathbf{u}}$ represent *intervals* of length $1/N'$. For $j = 0, 2, 4$ the columns $\tilde{\mathbf{f}}_j$ do not contain the parameters a, b so that all coordinates are known *exactly*, which means that the corresponding intervals are degenerate (of length zero). For $j = 1, 3, 5$ the columns $\tilde{\mathbf{f}}_j$ contain parameters at four different coordinates, each representing *intervals* of type $\left[\tilde{a} - \frac{1}{2N}, \tilde{a} + \frac{1}{2N}\right)$ and $\left[\tilde{b} - \frac{1}{2N}, \tilde{b} + \frac{1}{2N}\right)$, of length $1/N$. Therefore lemma 3.1 yields

$$\left| |\langle \tilde{\mathbf{u}}, \tilde{\mathbf{f}}_j\rangle| - \frac{1}{\sqrt{6}} \right| \leqslant \frac{5\pi}{6N'} \qquad j = 0, 2, 4 \tag{26}$$

$$\left| |\langle \tilde{\mathbf{u}}, \tilde{\mathbf{f}}_j \rangle| - \frac{1}{\sqrt{6}} \right| \leqslant \frac{5\pi}{6N'} + \frac{4\pi}{6N} \qquad j = 1, 3, 5. \tag{27}$$

However, these bounds turn out to be too crude, and we will need the following *improved error bound.* The technical lemma below establishes the simple fact that 'maximal error always occurs at the endpoints of the intervals'.

Lemma 3.2. *Let I_k and J_k ($1 \leqslant k \leqslant 5$) be closed intervals (possibly degenerate) contained in* $[0, 1]$. *Let L_k and T_k denote the lengths, m_k and s_k the midpoints, and i_k^-, i_k^+ and j_k^-, j_k^+ the endpoints of the intervals I_k and J_k, respectively. Assume that $\sum_{k=1}^5 (L_k + T_k) < \frac{1}{\pi}$.*

Consider the midpoint sum $S = \frac{1}{6}\big(1 + \sum_{k=1}^5 \mathrm{e}^{2\mathrm{i}\pi(m_k - s_k)}\big)$ and all the 32 endpoint sums $S_{\underline{\epsilon}} = \frac{1}{6}\big(1 + \sum_{k=1}^5 \mathrm{e}^{2\mathrm{i}\pi(i_k^{\epsilon_k} - j_k^{-\epsilon_k})}\big)$ (where $\underline{\epsilon}$ denotes any vector of $\pm$ signs; note that $-\epsilon_k$ appears at the upper index of j_k). The following two statements hold:

- *if it is possible to select points ϕ_k and ψ_k from the intervals I_k and J_k, such that $\big|\frac{1}{6}\big(1 + \sum_{k=1}^5 \mathrm{e}^{2\mathrm{i}\pi(\phi_k - \psi_k)}\big)\big| = \frac{1}{\sqrt{6}}$, then*
$$\max\{|S - S_{\underline{\epsilon}}|\} \geqslant \big||S| - \tfrac{1}{\sqrt{6}}\big|, \tag{28}$$
- *if it is possible to select points ϕ_k and ψ_k from the intervals I_k and J_k, such that $\frac{1}{6}\big(1 + \sum_{k=1}^5 \mathrm{e}^{2\mathrm{i}\pi(\phi_k - \psi_k)}\big) = 0$, then*
$$\max\{|S - S_{\underline{\epsilon}}|\} \geqslant |S|. \tag{29}$$

Proof. Let $r = \max\{|S - S_{\underline{\epsilon}}|\}$. Let us use again the 'error function' $E(\underline{x}, \underline{y}) = S - \frac{1}{6}\big(1 + \sum_{k=1}^5 \mathrm{e}^{2\mathrm{i}\pi(x_k - y_k)}\big)$, where x_k, y_k are in I_k and J_k, respectively. Apply for each $1 \leqslant k \leqslant 5$ the trivial estimate $|\mathrm{e}^{2\mathrm{i}\pi(m_k - s_k)} - \mathrm{e}^{2\mathrm{i}\pi(x_k - y_k)}| \leqslant \pi(L_k + T_k)$ to obtain $|E(\underline{x}, \underline{y})| \leqslant \frac{1}{6}\pi \sum_{k=1}^5 (L_k + T_k) < \frac{1}{6}$, by assumption. Also, $|E(\underline{x}, \underline{y})|$ is a continuous function on a compact space, so it achieves its maximum. We claim that the maximum is achieved where all coordinates x_k, y_k are opposite endpoints of I_k and J_k (i.e., if x_k is the lower endpoint of I_k then y_k is the upper endpoint of J_k, and vice versa). Assume by contradiction that this is not so for, say, x_1, y_1. Then $x_1 - y_1$ lies in the *interior* of the interval $I_1 - J_1$. This means that for t small enough we can move x_1 and/or y_1 to x_1', y_1' within the intervals I_1, J_1 so that $x_1' - y_1' = x_1 - y_1 + t$. This yields

$$|E(\underline{x}', \underline{y}')| = \left| S - \frac{1}{6} - \frac{1}{6}\,\mathrm{e}^{2\mathrm{i}\pi(x_1 - y_1 + t)} - \frac{1}{6}\sum_{k=2}^5 \mathrm{e}^{2\mathrm{i}\pi(x_k - y_k)} \right| \tag{30}$$

$$= \left| E(\underline{x}, \underline{y}) + \frac{1}{6}(1 - \mathrm{e}^{2t\mathrm{i}\pi})\,\mathrm{e}^{2\mathrm{i}\pi(x_1 - y_1)} \right|. \tag{31}$$

As t varies in the neighborhood of zero, the locus of the points $E(\underline{x}, \underline{y}) + \frac{1}{6}(\mathrm{e}^{2t\mathrm{i}\pi} - 1)\,\mathrm{e}^{2\mathrm{i}\pi(x_1 - y_1)}$ is a small arc of a circle of radius $\frac{1}{6}$ with center $E(\underline{x}, \underline{y}) - \frac{1}{6}\,\mathrm{e}^{2\mathrm{i}\pi(x_1 - y_1)}$. This arc goes through $E(\underline{x}, \underline{y})$ at $t = 0$. Combining this with the fact that $|E(\underline{x}, \underline{y})| < \frac{1}{6}$, it results from easy plane geometry that one can move along this circle in one way or the other so that $|E(\underline{x'}, \underline{y'})|$ becomes larger than $|E(\underline{x}, \underline{y})|$. The same argument applies to any of the variables x_k, y_k, so we conclude that $|E(\underline{x}, \underline{y})|$ indeed achieves its maximum when all x_k, y_k are at some opposite endpoints of the intervals I_k and J_k. This means that r is the maximum of $|E(\underline{x}, \underline{y})|$. Therefore, the values of the function $\frac{1}{6}\big(1 + \sum_{k=1}^5 \mathrm{e}^{2\mathrm{i}\pi(\phi_k - \psi_k)}\big)$ stay within a disk of radius r around S. In the first statement of the lemma, we thus conclude that the distance of S from the circle of radius

$1/\sqrt{6}$ (centered at the origin) is not greater than r. In the second statement, we conclude that the distance of S from the origin is not greater than r. These are equivalent to (28) and (29). □

We are now ready to search for vectors $\tilde{\mathbf{u}} \in \mathrm{FUB}^{\tilde{a},\tilde{b}}_{N,N'}$. For each fixed pair[8] $\tilde{a}, \tilde{b} = 1/2N, 3/2N, \ldots, (2N-1)/2N$ we simply take all possible values of $j_1, \ldots, j_5$ from 0 to $N'-1$ and check if the vector $\tilde{\mathbf{u}}$ given by (22) satisfies the bound (28) for all $\tilde{\mathbf{f}}_j$, $(0 \leqslant j \leqslant 5)$. Recall that the coordinates of $\tilde{\mathbf{u}}$ and $\tilde{\mathbf{f}}_j$ represent *intervals* in which the actual coordinates of $\mathbf{u}$ and $\mathbf{f}_j$ might lie. The sum of the lengths of these intervals is either $\frac{5}{N'}$ or $\frac{5}{N'} + \frac{4}{N}$ (see equations (26) and (27)), which are less than $\frac{1}{\pi}$ due to our choices $N = 180$, $N' = 19$, so that lemma 3.2 can indeed be applied.

It turns out, however, that the number of vectors $\tilde{\mathbf{u}}$ satisfying the improved error bound (28) is still too high. Therefore we need to use the following *multiscale* strategy. We subdivide each interval $I_j^{(N')}$ into two equal subintervals $I_{j,-}^{(N')} = \left[r_j^{(N')} - 1/(2N'), r_j^{(N')}\right)$ and $I_{j,+}^{(N')} = \left[r_j^{(N')}, r_j^{(N')} + 1/(2N')\right)$. Let $r_{j,-}$ and $r_{j,+}$ denote the midpoints of these subintervals. Clearly, each ϕ_k—defined in (23)—must fall into one of these intervals. This means that we can better approximate $\mathbf{u}$ by

$$\tilde{\mathbf{u}}_{\underline{\epsilon}} = \frac{1}{\sqrt{6}}(1, \mathrm{e}^{2\mathrm{i}\pi r_{j_1,\epsilon_1}}, \ldots, \mathrm{e}^{2\mathrm{i}\pi r_{j_5,\epsilon_5}}),$$

where $\underline{\epsilon}$ is a ± vector with the signs being chosen according to which subintervals ϕ_k fall. Then $\tilde{\mathbf{u}}_{\underline{\epsilon}}$ is a better approximation of $\mathbf{u}$ and needs to satisfy (28) for all $\tilde{\mathbf{f}}_j$, $(0 \leqslant j \leqslant 5)$, with the *smaller* intervals corresponding to $\tilde{\mathbf{u}}_{\underline{\epsilon}}$. The 2^5 vectors $\tilde{\mathbf{u}}_{\underline{\epsilon}}$ will be called the *daughters* of $\tilde{\mathbf{u}}$ (called their *mother*). Clearly, if none of the daughters satisfies the bound (28) then we can discard the mother. The point is that it often happens that the mother satisfies the bound (28) (corresponding to her own intervals), but none of her daughters do. In such a situation, we must keep the mother at the first level of checking, but can discard her at the level of daughters. We then repeat this operation, obtaining grandchildren who have to satisfy the bound (28) for all $\tilde{\mathbf{f}}_j$, $(0 \leqslant j \leqslant 5)$, with even smaller intervals. Again, if none of the grandchildren satisfies this bound, then the grandmother is discarded. We repeat this operation for seven generations, i.e., a vector $\tilde{\mathbf{u}}$ of the form (22) survives this test if and only if it has a surviving descendant down to seven generations. Our computer search then shows that for a fixed pair of values $(\tilde{a}, \tilde{b})$ we typically obtain 110–140 such vectors $\tilde{\mathbf{u}} \in \mathrm{FUB}^{\tilde{a},\tilde{b}}_{N,N'}$. (This is quite satisfying considering that a, b are allowed to range over small intervals, and we conjecture that the *precise* number of unbiased vectors for any *exact* pair a, b is 48.) These vectors are the candidates for the columns of $\tilde{C}, \tilde{D}$.

Next, we attempt to compile the basis $\tilde{C}$. If there exists a quartet $(Id, F(a,b), C, D)$ of mutually unbiased bases, then all the columns of $\tilde{C}$ must come from the set $\mathrm{FUB}^{\tilde{a},\tilde{b}}_{N,N'}$ and, furthermore, they must be 'almost-orthogonal' to each other. To be more precise, let $\mathbf{u} = \frac{1}{\sqrt{6}}(1, \mathrm{e}^{2\mathrm{i}\pi\phi_1}, \ldots, \mathrm{e}^{2\mathrm{i}\pi\phi_5})$ and $\mathbf{v} = \frac{1}{\sqrt{6}}(1, \mathrm{e}^{2\mathrm{i}\pi\psi_1}, \ldots, \mathrm{e}^{2\mathrm{i}\pi\psi_5})$ be any two vectors from C and let

$$\tilde{\mathbf{u}} = \frac{1}{\sqrt{6}}\left(1, \mathrm{e}^{2\mathrm{i}\pi r_{j_1}^{(N')}}, \ldots, \mathrm{e}^{2\mathrm{i}\pi r_{j_5}^{(N')}}\right) \tag{32}$$

and

$$\tilde{\mathbf{v}} = \frac{1}{\sqrt{6}}(1, \mathrm{e}^{2\mathrm{i}\pi r_{m_1}^{(N')}}, \ldots, \mathrm{e}^{2\mathrm{i}\pi r_{m_5}^{(N')}}) \tag{33}$$

[8] We actually only take those $\tilde{a}, \tilde{b}$ which approximate a, b in the triangle $(0,0)(1/6,0)$, $(1/6, 1/12)$, i.e., in the fundamental domain.

be their approximation in $\mathrm{FUB}^{\tilde{a},\tilde{b}}_{N,N'}$. Recall that we only have at hand the vectors $\tilde{\mathbf{u}}, \tilde{\mathbf{v}}$ and keep in mind that the actual phases of $\mathbf{u}, \mathbf{v}$ can lie anywhere in the *intervals* $I^{N'}_{j_1}, \ldots, I^{N'}_{j_5}$ and $I^{N'}_{m_1}, \ldots, I^{N'}_{m_5}$, respectively. The fact that $\langle \mathbf{u}, \mathbf{v}\rangle = 0$ implies the following condition on $\tilde{\mathbf{u}}, \tilde{\mathbf{v}}$:

Definition 3.1. *We will say that the vectors* $\tilde{\mathbf{u}}$ *and* $\tilde{\mathbf{v}}$ *of the form (32), (33) are* N'*-orthogonal if there exist numbers* ϕ_k *and* ψ_k *in the intervals* $I^{(N')}_{j_k}$ *and* $I^{(N')}_{m_k}$*, such that* $\frac{1}{6}\big(1 + \sum_{k=1}^{5} \mathrm{e}^{2\mathrm{i}\pi(\phi_k-\psi_k)}\big) = 0$.

Similarly, we will say that $\tilde{\mathbf{u}}$ *and* $\tilde{\mathbf{v}}$ *are* N'*-unbiased if there exist* $\phi_k \in I^{(N')}_{j_k}$ *and* $\psi_k \in I^{(N')}_{m_k}$*, such that* $\big|\frac{1}{6}\big(1 + \sum_{k=1}^{5} \mathrm{e}^{2\mathrm{i}\pi(\phi_k-\psi_k)}\big)\big| = \frac{1}{\sqrt{6}}$.

These properties are clearly rotation invariant in the sense that they only depend on the values $\mathrm{e}^{2\mathrm{i}\pi(r^{(N')}_{j_1}-r^{(N')}_{m_1})}, \ldots, \mathrm{e}^{2\mathrm{i}\pi(r^{(N')}_{j_5}-r^{(N')}_{m_5})}$, i.e., the values of $r^{(N')}_{j_1}-r^{(N')}_{m_1}, \ldots, r^{(N')}_{j_5}-r^{(N')}_{m_5}$ modulo 1. We can therefore take $m_1 = \cdots = m_5 = 0$ and correspondingly $\tilde{\mathbf{v}}_0 = \frac{1}{\sqrt{6}}(1, \mathrm{e}^{\mathrm{i}\pi/N'}, \ldots, \mathrm{e}^{\mathrm{i}\pi/N'})$ (where the exponents of the last five coordinates represent intervals, of course) and define the set $\mathrm{ORT}_{\mathrm{eps},N'}$ as the set of vectors which are N'-orthogonal to $\tilde{\mathbf{v}}_0$. With this notation the rotation invariance means that $\tilde{\mathbf{u}}$ and $\tilde{\mathbf{v}}$ as in (32) and (33) are N'-orthogonal if and only if the vector $\frac{1}{\sqrt{6}}\big(1, \mathrm{e}^{2\mathrm{i}\pi(r^{(N')}_{j_1}-r^{(N')}_{m_1})}, \ldots, \mathrm{e}^{2\mathrm{i}\pi(r^{(N')}_{j_5}-r^{(N')}_{m_5})}\big)$ is in $\mathrm{ORT}_{\mathrm{eps},N'}$.

Note that the set $\mathrm{ORT}_{\mathrm{eps},N'}$ is independent of $\tilde{a}, \tilde{b}$, so it can be computed once and for all at the beginning of the computer search. In order to find the set $\mathrm{ORT}_{\mathrm{eps},N'}$ we first introduce the simpler set $\mathrm{ORT}_{N'}$ as the set of vectors $\tilde{\mathbf{u}}$ (as in (32)) for which there exist $\phi_k \in I_{j_k}$ such that $\frac{1}{6}(1 + \sum_{k=1}^{5} \mathrm{e}^{2\mathrm{i}\pi\phi_k}) = 0$. We will check each possible vector $\tilde{\mathbf{u}}$ whether it is in $\mathrm{ORT}_{N'}$ (recall that there are N'^5 possibilities for $\tilde{\mathbf{u}}$). In order to do so, we apply lemma 3.2 to $\tilde{\mathbf{u}}$ and the *exact* vector $\mathbf{v}_0 = (1, 1, \ldots, 1)$ (so that in the notations of the lemma the intervals J_k are degenerate). We then use our multiscale strategy again, i.e., we test the descendants of $\tilde{\mathbf{u}}$ against $\mathbf{v}_0$ with lemma 3.2 down to seven generations. We keep only those vectors $\tilde{\mathbf{u}}$ which have at least one surviving descendant in each generation. Having constructed the set $\mathrm{ORT}_{N'}$ it is now easy to obtain $\mathrm{ORT}_{eps,N'}$. Indeed, by definition a vector $\tilde{\mathbf{u}} = \frac{1}{\sqrt{6}}\big(1, \mathrm{e}^{2\mathrm{i}\pi r^{(N')}_{j_1}}, \ldots, \mathrm{e}^{2\mathrm{i}\pi r^{(N')}_{j_5}}\big)$ can only be N'-orthogonal to $\tilde{\mathbf{v}}_0$ if there exist numbers ϕ_k in the intervals I_{j_k} and ψ_k in $[0, \frac{1}{N'})$, such that $\frac{1}{6}\big(1 + \sum_{k=1}^{5} \mathrm{e}^{2\mathrm{i}\pi(\phi_k-\psi_k)}\big) = 0$. But then the numbers $\phi_k - \psi_k$ must fall in the intervals $I_{j_k-\epsilon_k}$ where ϵ_k is either 0 or 1, and hence the vector $\tilde{\mathbf{u}}_\epsilon = \frac{1}{\sqrt{6}}\big(1, \mathrm{e}^{2\mathrm{i}\pi r^{(N')}_{j_1-\epsilon_1}}, \ldots, \mathrm{e}^{2\mathrm{i}\pi r^{(N')}_{j_5-\epsilon_5}}\big)$ is in $\mathrm{ORT}_{N'}$. Therefore, to construct $\mathrm{ORT}_{\mathrm{eps},N'}$ we take all vectors of the form $\tilde{\mathbf{u}}^\epsilon = \frac{1}{\sqrt{6}}\big(1, \mathrm{e}^{2\mathrm{i}\pi r^{(N')}_{j_1+\epsilon_1}}, \ldots, \mathrm{e}^{2\mathrm{i}\pi r^{(N')}_{j_5+\epsilon_5}}\big)$, where ϵ_k is 0 or 1, and the vector $\frac{1}{\sqrt{6}}\big(1, \mathrm{e}^{2\mathrm{i}\pi r^{(N')}_{j_1}}, \ldots, \mathrm{e}^{2\mathrm{i}\pi r^{(N')}_{j_5}}\big)$ is in $\mathrm{ORT}_{N'}$. In the specific case $N' = 19$, we found that the set $\mathrm{ORT}_{\mathrm{eps},N'}$ contains 322040 vectors. This means that the 'probability' of two random vectors being N'-orthogonal is $322040/19^5 \approx 0.13$.

Having constructed the set $\mathrm{ORT}_{\mathrm{eps},N'}$ we search for the columns of the matrix $\tilde{C}$ in such a way that for any two columns $\tilde{\mathbf{u}}$ and $\tilde{\mathbf{v}}$ (as in (32) and (33)) we require that $\tilde{\mathbf{u}}, \tilde{\mathbf{v}} \in \mathrm{FUB}^{\tilde{a},\tilde{b}}_{N,N'}$ and that the vector $\frac{1}{\sqrt{6}}\big(1, \mathrm{e}^{2\mathrm{i}\pi(r^{(N')}_{j_1}-r^{(N')}_{m_1})}, \ldots, \mathrm{e}^{2\mathrm{i}\pi(r^{(N')}_{j_5}-r^{(N')}_{m_5})}\big)$ be in $\mathrm{ORT}_{\mathrm{eps},N'}$.

Let us make a last simplifying remark. It is clear that we can permute the columns of all appearing matrices, and hence we are free to choose the *order* of the columns of $\tilde{C}$. Therefore we assume in our search that the columns of $\tilde{C}$ are lexicographically ordered, meaning that for any two columns $\tilde{\mathbf{u}}$ and $\tilde{\mathbf{v}}$ (as in (32) and (33)) we have that $\tilde{\mathbf{u}}$ precedes $\tilde{\mathbf{v}}$ if and only if $(j_1, \ldots, j_5)$ precedes $(m_1, \ldots, m_5)$ in lexicographic order.

Our computer search has shown that for a fixed pair of values $(\tilde{a}, \tilde{b})$ there are typically 1000–5000 such N'-orthonormal bases $\tilde{C}$. (At some special values of $(\tilde{a}, \tilde{b})$, however, there are millions. This nicely complies with the finding of [10] that for $(a, b) = (1/6, 0)$ there exist 70 bases C, whereas for generic values of (a, b) there exist only 8.)

Finally, for any fixed pair $(\tilde{a}, \tilde{b})$ and any corresponding matrix $\tilde{C}$ we attempt to compile the basis $\tilde{D}$. The columns of $\tilde{D}$ must also come from the set $\mathrm{FUB}^{\tilde{a},\tilde{b}}_{N,N'}$, they must be N'-orthogonal to each other and they must be N'-unbiased to the columns of $\tilde{C}$. Therefore, to find the candidates for the columns of $\tilde{D}$ we will check any vector $\tilde{\mathbf{u}} \in \mathrm{FUB}^{\tilde{a},\tilde{b}}_{N,N'}$ whether it is N'-unbiased simultaneously to all the columns $\tilde{\mathbf{c}}_k$ of $\tilde{C}$. This is done by applying the trivial bound, lemma 3.1, to the vector $\tilde{\mathbf{u}}$ (and its descendants for seven generations) and the vectors $\tilde{\mathbf{c}}_k$ for $k = 0, \ldots, 5$. The reason why we use the trivial bound instead of the improved bound is that it speeds up calculations and very few vectors $\tilde{\mathbf{u}}$ survive this test anyway. Let $\mathrm{COL}_{\tilde{D}}$ denote the set of surviving vectors, the candidates for the columns of $\tilde{D}$. If there are less than six vectors in $\mathrm{COL}_{\tilde{D}}$ then we conclude that $\tilde{D}$ cannot exist (as it would need six columns). If there are at least six vectors in $\mathrm{COL}_{\tilde{D}}$ then we check whether any 6 of them can be pairwise N'-orthogonal to each other (this is done by using the set $\mathrm{ORT}_{\mathrm{eps},N'}$ again).

Our computer search shows that there are no values of $(\tilde{a}, \tilde{b})$ and corresponding $\tilde{C}$ for which all these conditions on $\tilde{D}$ can be met. This concludes the proof of the theorem.

Remark 3.3. In *principle*, this discretization scheme could successfully be applied to settle problem 1.1. Of course, in the general case we cannot assume that B is of the form $B = F(a, b)$. However, we know that B is *some* complex Hadamard matrix. If a complete classification of complex Hadamard matrices of order 6 were available in some parametric form then a similar search could be carried out as above. Without such classification at hand we can still use a *finite* set of N representatives in *each coordinate* of B to approximate it with a quasi-Hadamard matrix $\tilde{B}$. The rest of the algorithm concerning the selection of quasi-unbiased vectors and the checking of the possibly arising matrices $\tilde{C}$ and $\tilde{D}$ remains the same. Note that B has 25 free entries (as the first row and column can be assumed to be 1). At first glance, an exhaustive search for B should go through N^{25} cases, way out of the realm of possibilities, if $N \approx 100$. However, one can reduce the number of cases with intelligent tricks, so that the search can actually be carried out. The problem is that while in the case of $B = F(a, b)$ and $N = 180$ we had only 270 candidates for $\tilde{B}$, in the general case we have about 10^{12} such candidates already at $N \approx 100$. And for each candidate $\tilde{B}$ we need to run the final part of the algorithm concerning the selection of unbiased vectors and compiling the bases $\tilde{C}, \tilde{D}$. While it is not absolutely out of the question to carry out a computer search at such magnitudes, it definitely needs meticulous programming and probably some further mathematical ideas to reduce the number of cases.

Let us also recall that the non-existence of projective planes of order 10 was also shown by an exhaustive computer search [24]—and no 'theoretical' proofs are known.

4. Smooth families of mutually unbiased bases

Throughout this section, we will assume that

$$\mathcal{F}(t) = (\mathbf{f}_1(t), \ldots, \mathbf{f}_d(t)) \tag{34}$$

is a 'time-dependent' family of orthonormal bases. More precisely, we assume that the maps $I \ni t \mapsto \mathbf{f}_k(t) \in \mathbb{C}^d$ (for $k = 1, \ldots, d$) are smooth (where $I \subset \mathbb{R}$ is a certain fixed open interval) and that $\mathcal{F}(t)$ is an orthonormal basis (ONB) for each $t \in I$. We shall then say that

$t \mapsto (\mathcal{E}, \mathcal{F}(t))$ is a *smooth family of pairs of MUB* if $\mathcal{E} = (\mathbf{e}_1, \dots, \mathbf{e}_d)$ is a fixed ONB such that $\mathcal{E}$ and $\mathcal{F}(t)$ are mutually unbiased for all $t \in I$.

4.1. Smooth families of MUB and common unbiased vectors

Let us consider now the following question. Assume we are given a vector $\mathbf{b}_0$ of unit length which is unbiased to both $\mathcal{E}$ and $\mathcal{F}(0)$. Can we 'continue' $\mathbf{b}_0$ so as to find a common unbiased vector $\mathbf{b}(t)$ for $\mathcal{E}$ and $\mathcal{F}(t)$ for t in a neighborhood of 0?

In order to answer this question, we shall need some further notions and notations. First, if $\mathbf{u}$ is any vector in $\mathbb{C}^d$ with $\|\mathbf{u}\| = 1$, let $\mathcal{P}_\mathbf{u}$ be the ortho-projection on the span of $\mathbf{u}$; i.e., $\mathcal{P}_\mathbf{u}\mathbf{x} = \langle \mathbf{x}, \mathbf{u}\rangle \mathbf{u}$. Next, consider the $d \times d$ complex matrix $M = [M_{k,l}]_{1\leqslant k,l\leqslant d}$ defined by the formula

$$M_{k,l} := \mathrm{Tr}(P_k Q_l R), \tag{35}$$

where $P_k = \mathcal{P}_{\mathbf{e}_k}$, $Q_l = \mathcal{P}_{\mathbf{f}_l(0)}$ and $R = \mathcal{P}_{\mathbf{b}_0}$. A simple computation shows that

$$M_{k,l} = \langle \mathbf{b}_0, \mathbf{e}_k\rangle \langle \mathbf{e}_k, \mathbf{f}_l(0)\rangle \langle \mathbf{f}_l(0), \mathbf{b}_0\rangle.$$

Note that $M_{k,l}$ is unchanged if any of the vectors $\mathbf{b}_0, \mathbf{e}_k, \mathbf{f}_l(0)$ is multiplied by a complex number of modulus 1. Moreover, $M = D_1 H D_2$ where D_1 is the non-singular diagonal matrix with entries $\langle \mathbf{b}_0, \mathbf{e}_k\rangle$, D_2 is the non-singular diagonal matrix with entries $\langle \mathbf{f}_l(0), \mathbf{b}_0\rangle$ and $H = [\langle \mathbf{e}_k, \mathbf{f}_l(0)\rangle]_{1\leqslant k,l\leqslant d}$ is a multiple of a Hadamard matrix. Thus M is of rank d. However, the *real* matrix N whose entries are obtained by taking the imaginary part of the entries of M,

$$N_{k,l} := \mathrm{Im}(M_{k,l}) = \frac{1}{2\mathrm{i}} \mathrm{Tr}([P_k, Q_l]R) \tag{36}$$

cannot be of maximal rank. Indeed, for all $l = 1, \dots, d$,

$$\sum_k N_{k,l} = \sum_k \frac{1}{2\mathrm{i}} \mathrm{Tr}([P_k, Q_l]R) = \frac{1}{2\mathrm{i}} \mathrm{Tr}([\mathbf{1}, Q_l]R) = 0$$

since $\sum_k P_k = \mathbf{1}$.

Definition 4.1. *We say that a unit vector* $\mathbf{b}$ *that is unbiased to both members of a MUB pair* $(\mathcal{E}, \mathcal{F})$ *is non-degenerate if the associated real matrix* $N(\mathbf{b}) = [\mathrm{Im}(\langle \mathbf{b}, \mathbf{e}_k\rangle\langle \mathbf{e}_k, \mathbf{f}_l\rangle\langle \mathbf{f}_l, \mathbf{b}\rangle)]_{1\leqslant k,l\leqslant d}$ *has rank* $d - 1$.

Theorem 4.1. *Let* $(\mathcal{E}, \mathcal{F}(t))$ *be a smooth family of pairs of MUB. Let* $\mathbf{b}_0$ *be a non-degenerate common normalized unbiased vector for the MUB pair* $(\mathcal{E}, \mathcal{F}(0))$. *Then there exists an* $\epsilon > 0$ *and a smooth map* $(-\epsilon, \epsilon) \ni t \mapsto \mathbf{b}(t)$ *such that* $\mathbf{b}(0) = \mathbf{b}_0$ *and* $\mathbf{b}(t)$ *is a common normalized unbiased vector to* $(\mathcal{E}, \mathcal{F}(t))$ *for all* $t \in (-\epsilon, \epsilon)$.

Proof. We may modify the order of columns and rows of $N := N(\mathbf{b}_0)$ by reordering the vectors in $\mathcal{E}$ and $\mathcal{F}$. But, from the rank condition, N has a $(d-1) \times (d-1)$ invertible submatrix so, without loss of generality, we may assume that the $(d-1) \times (d-1)$ submatrix in the upper-left corner of N is invertible.

A vector $\mathbf{v}$ is unbiased to a given pair of MUB if and only if $\lambda\mathbf{v}$ is so, where $\lambda \in \mathbb{C}$, $|\lambda| = 1$. Thus, without loss of generality, we may assume that $\langle \mathbf{e}_d, \mathbf{b}_0\rangle = d^{-1/2}$ and in fact we may further require $t \mapsto \mathbf{b}(t)$ to satisfy $\langle \mathbf{e}_d, \mathbf{b}(t)\rangle = d^{-1/2}$ for all $t \in (-\epsilon, \epsilon)$. (Indeed, if $t \mapsto \mathbf{b}(t)$ satisfies the original requirements of our theorem, then $t \mapsto \tilde{\mathbf{b}}(t) := \alpha(t)\mathbf{b}(t)$ where $\alpha(t) = d^{-1/2}\langle \mathbf{e}_d, \mathbf{b}(t)\rangle$ satisfies the just introduced extra condition, too.) Then the condition

$|\langle \mathbf{e}_j, \mathbf{b}(t)\rangle| = d^{-1/2}$ (for $j = 1, \ldots, d-1$), together with the condition of smoothness, is equivalent to saying that $\mathbf{b}(t) = \mathbf{v}(x(t))$ where

$$\mathbf{v}(x) = d^{-1/2}\left(\sum_{j=1}^{d-1} \mathrm{e}^{\mathrm{i}x_j}\mathbf{e}_j + \mathbf{e}_d\right) \tag{37}$$

and $t \mapsto x(t) \in \mathbb{R}^{d-1}$ is a real smooth curve. In this rephrasing of the problem, the initial condition $\mathbf{b}(0) = \mathbf{b}_0$ reads as $x(0) = x^{(0)}$ where $x^{(0)} = \left(x_1^{(0)}, \ldots, x_{d-1}^{(0)}\right) \in \mathbb{R}^{d-1}$ is such that $\langle \mathbf{b}_0, \mathbf{e}_j\rangle = d^{-1/2}\,\mathrm{e}^{\mathrm{i}x_j^{(0)}}$. Note also that $\|\mathbf{v}(x)\| = 1$ is automatically satisfied.

Let us now introduce the function $u : I \times \mathbb{R}^{d-1} \to \mathbb{R}^{d-1}$ defined by the formula

$$u_k(t, x) = |\langle \mathbf{f}_k(t), \mathbf{v}(x)\rangle| - \frac{1}{\sqrt{d}}(k = 1, \ldots, d-1), \tag{38}$$

and note that $\mathbf{v}(x)$ is unbiased to $\mathcal{F}(t)$ if and only if $u(t, x) = 0$; that is, if $u_k(t, x) = 0$ for all $k = 1, \ldots, d-1$.

By assumption, $u(0, x^{(0)}) = 0$ since $\mathbf{v}(x^{(0)}) = \mathbf{b}_0$ is an unbiased vector for $\mathcal{F}(0)$. Further, as $|\langle \mathbf{f}_k, \mathbf{b}_0\rangle| = d^{-1/2} \neq 0$ for all $k = 1, \ldots, d-1$, the function u is smooth in a neighborhood of $(0, x^{(0)})$.[9] A simple computation then shows $\partial_{x_k}\mathbf{v}(x) = \mathrm{i}\langle \mathbf{v}(x), \mathbf{e}_k, \rangle \mathbf{e}_k$ form which we deduce

$$\begin{aligned}
\partial_{x_k} u_j(t, x) &= \frac{1}{\left|\langle \mathbf{f}_j(t), \mathbf{v}(x)\rangle\right|}\,\mathrm{Re}\big(\big\langle \partial_{x_k}\mathbf{v}(x), \mathbf{f}_j(t)\big\rangle \langle \mathbf{f}_j(t), \mathbf{v}(x)\rangle\big) \\
&= \frac{1}{|\langle \mathbf{f}_j(t), \mathbf{v}(x)\rangle|}\,\mathrm{Re}(\mathrm{i}\langle \mathbf{v}(x), \mathbf{e}_k\rangle\langle \mathbf{e}_k, \mathbf{f}_j(t)\rangle\langle \mathbf{f}_j(t), \mathbf{v}(x)\rangle).
\end{aligned}$$

Therefore

$$\begin{aligned}
\partial_{x_k} u_j(t, x)|_{(t,x)=(0,x^{(0)})} &= \sqrt{d}\,\mathrm{Re}(\mathrm{i}\langle \mathbf{b}_0, \mathbf{e}_k\rangle\langle \mathbf{e}_k, \mathbf{f}_j\rangle\langle \mathbf{f}_j, \mathbf{b}_0\rangle) \\
&= -\sqrt{d}\,\mathrm{Im}(\langle \mathbf{b}_0, \mathbf{e}_k\rangle\langle \mathbf{e}_k, \mathbf{f}_j\rangle\langle \mathbf{f}_j, \mathbf{b}_0\rangle) \\
&= -\sqrt{d}N_{k,j}.
\end{aligned}$$

Thus, the Jacobian of $u(0, \cdot)$ at $x = x^{(0)}$ is a nonzero multiple of the $(d-1) \times (d-1)$ submatrix in the upper-left corner of N, and the theorem follows by a use of the implicit function theorem. □

Note that the implicit function theorem, used in the above proof, actually tells us more than just existence. The invertibility of the Jacobian of the function $u(0, \cdot) : \mathbb{R}^{d-1} \to \mathbb{R}^{d-1}$ at $x = x^{(0)}$ guarantees the existence of a neighborhood of $(0, x^{(0)})$ in which the only solution of $u(t, x) = 0$ is $(t, x) = (t, x(t))$. In particular, for $|t|$ small enough, in a neighborhood of $\mathbf{b}(t)$, the only vectors that are unbiased for the MUB pair $(\mathcal{E}, \mathcal{F}(t))$ are the multiples of $\mathbf{b}(t)$.

Corollary 4.2. *Let* $\mathbf{b}$ *be a common non-degenerate unbiased vector for the MUB pair* $(\mathcal{E}, \mathcal{F})$*. Then there is a neighborhood of* $\mathbf{b}$ *in which all common unbiased vectors to* $(\mathcal{E}, \mathcal{F})$ *are multiples of* $\mathbf{b}$*.*

Actually, our theorem also allows us to prove that the number of vectors (counted up to multiples) that are unbiased to the family $(\mathcal{E}, \mathcal{F}(t))$ is (under some non-degeneracy conditions) independent of t (for $|t|$ small enough).

Corollary 4.3. *Let* $(\mathcal{E}, \mathcal{F}(t))$ *be a smooth family of pairs of MUB and assume that every common normalized unbiased vector to* $(\mathcal{E}, \mathcal{F}(0))$ *is non-degenerate. Then there exists an*

[9] Actually, if $s \mapsto z(s) \in \mathbb{C}$ is smooth and $z(s) \neq 0$ then $\frac{\mathrm{d}}{\mathrm{d}s}|z(s)| = \frac{1}{|z(s)|}\mathrm{Re}(\overline{z'(s)}z(s))$.

$\epsilon > 0$ *such that for* $|t| < \epsilon$*, the number of common normalized unbiased vectors to* $(\mathcal{E}, \mathcal{F}(t))$*, when counted up to multiples, is finite and independent of t. Moreover each of these vectors is given by theorem 4.1.*

Proof. At $t = 0$, corollary 4.2 implies that each normalized vector that is unbiased to both $\mathcal{E}$ and $\mathcal{F}(0)$ is isolated in the explained sense. Since the unit sphere of $\mathbb{C}^d$ is compact, it follows that up to multiples, there can be only finitely many such vectors; say $\mathbf{b}^{(1)}, \ldots, \mathbf{b}_0^{(m)}$. According to theorem 4.1, for each of these vectors, there is a smooth curve $t \mapsto \mathbf{b}^{(k)}(t)$ such that $\mathbf{b}^{(k)}(0) = \mathbf{b}_0^{(k)}$ and $\mathbf{b}^{(k)}(t)$ is unbiased to $(\mathcal{E}, \mathcal{F}(t))$. By the comment before corollary 4.2 and by the fact that the just introduced m is a finite number, there exist some $\tilde{\epsilon}, r > 0$ such that if $|t| < \tilde{\epsilon}$ then none of the vectors $\mathbf{b}^{(1)}(t), \ldots, \mathbf{b}^{(m)}(t)$ are multiples of each other and if $\mathbf{b}$ is a common unbiased vector to $(\mathcal{E}, \mathcal{F}(t))$, then for every $k = 1, \ldots, m$, either

$$\|\mathbf{b} - \mathbf{b}^{(k)}(t)\| > r$$

or $\mathbf{b}$ is a multiple of $\mathbf{b}^{(k)}(t)$. In particular, the number of common normalized unbiased vectors to $(\mathcal{E}, \mathcal{F}(t))$, counted up to multiples, is at least m (since we have the vectors $\mathbf{b}^{(1)}(t), \ldots, \mathbf{b}^{(m)}(t)$).

To prove the remaining part of our statement, we shall argue by contradiction. Assume there is no such $\epsilon > 0$ whose existence is stated in our theorem. Then there should exist a real sequence $t_n (n \in \mathbb{N})$ converging to 0 and a sequence of unit vectors $\mathbf{b}_n (n \in \mathbb{N})$ such that for every $n \in \mathbb{N}$

- $\mathbf{b}_n$ is a common unbiased vector to $(\mathcal{E}, \mathcal{F}(t_n))$,
- $\mathbf{b}_n$ is not a multiple of any of the vectors $\mathbf{b}^{(1)}(t_n), \ldots, \mathbf{b}^{(m)}(t_n)$.

Since the unit sphere of $\mathbb{C}^d$ is compact, it follows that there is a subsequence of $\mathbf{b}_n (n \in \mathbb{N})$ which is convergent. In fact, without loss of generality we may assume that our original sequence was such. Let $\mathbf{b} := \lim_n(\mathbf{b}_n)$; it is then clear that $\|\mathbf{b}\| = 1$ and since $|\langle \mathbf{b}_n, \mathbf{e}_k \rangle| = |\langle \mathbf{b}_n, \mathbf{f}_j(t_n) \rangle| = d^{-1/2}$, by continuity of the scalar product, absolute value and the map $t \mapsto \mathbf{f}_j(t)$, we have that $\mathbf{b}$ is a common unbiased vector to $(\mathcal{E}, \mathcal{F}(0))$. Hence by assumption there must exist a k such that $\mathbf{b}$ is a multiple of $\mathbf{b}_0^{(k)}$. Actually it is clear that we even may assume that $\mathbf{b}$ is not only a *multiple* of $\mathbf{b}_0^{(k)}$, but equal to it. We can then conclude our proof since as $n \to \infty$, we have

$$r < \|\mathbf{b}_n - \mathbf{b}^{(k)(t_n)}\| \to \left\|\mathbf{b}_0^{(k)} - \mathbf{b}_0^{(k)}\right\| = 0$$

which is clearly a contradiction. □

4.2. *Unitary symmetries of mutually unbiased bases*

Recall that if $\mathcal{E} = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ and $\mathcal{F} = (\mathbf{f}_1, \ldots, \mathbf{f}_n)$ are two mutually unbiased ONBs, then upon multiplying each vector by a complex number of modulus 1 and changing the orders of the vectors in the individual bases, they still remain two mutually unbiased ONBs. In order not to distinguish between such pairs, we will associate with an ONB $\mathcal{E} = (\mathbf{e}_1, \ldots, \mathbf{e}_d)$ a maximal Abelian star algebra

$$\mathcal{A}_{\mathcal{E}} := \mathrm{Span}\{\mathcal{P}_{\mathbf{e}_k} | k = 1, \ldots, d\},$$

where $\mathcal{P}_{\mathbf{e}_k}$ is the ortho-projection onto $\mathbb{C}\mathbf{e}_k$, $(k = 1, \ldots, d)$. Indeed, $\mathcal{A}_{\mathcal{E}}$ is invariant under reordering and changing phases of the vectors in $\mathcal{E}$. Moreover, as is well known and easy to show, $\mathcal{E} = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ and $\mathcal{F} = (\mathbf{f}_1, \ldots, \mathbf{f}_n)$ are two mutually unbiased ONBs if and only if $\mathcal{A}_{\mathcal{E}}$ and $\mathcal{A}_{\mathcal{F}}$ are *quasi-orthogonal*. Recall that this means that the subspaces of $M_d(\mathbb{C})$ given by

$\mathbf{1}^\perp \cap \mathcal{A}_\mathcal{E}$ and $\mathbf{1}^\perp \cap \mathcal{A}_\mathcal{F}$ are orthogonal with respect to the usual Hilbert–Schmidt scalar product $\langle A, B\rangle_{M_d(\mathbb{C})} = \mathrm{Tr}(A^*B)$ on $M_d(\mathbb{C})$.

Further, to a unitary operator U on $\mathbb{C}^d$, we associate the authomorphism α_U defined by the formula $\alpha_U(X) = UXU^*$. We will say that U *implements a symmetry* of $(\mathcal{E}, \mathcal{F})$ if $\alpha(\mathcal{A}_\mathcal{E}) = \mathcal{A}_\mathcal{E}$ and $\alpha(\mathcal{A}_\mathcal{F}) = \mathcal{A}_\mathcal{F}$. Accordingly, we shall talk about the *unitary symmetry group* of $(\mathcal{E}, \mathcal{F})$.

There is a natural homomorphism from the group of symmetries of $(\mathcal{E}, \mathcal{F})$ to $S_d \times S_d$ where S_d is the group of permutations of d elements. Indeed, a symmetry takes a minimal projection of $\mathcal{A}_\mathcal{E}$ and $\mathcal{A}_\mathcal{F}$ into a minimal projection of $\mathcal{A}_\mathcal{E}$ and $\mathcal{A}_\mathcal{F}$, respectively. Thus if α is a symmetry, then there exist two permutations $\sigma = \sigma_\alpha$, $\mu = \mu_\alpha \in S_d$ such that

$$\alpha(P_{\mathbf{e}_k}) = P_{\mathbf{e}_{\sigma(k)}} \qquad \text{and} \qquad \alpha(P_{\mathbf{f}_k}) = P_{\mathbf{f}_{\mu(k)}}$$

for all $k = 1, \ldots, d$. Moreover, it is straightforward to show that the map that associates the pair (σ, μ) with α defines a group homomorphism.

Theorem 4.4. *The homomorphism from the group of unitary symmetries to $S_n \times S_n$ defined above is injective. In particular, the group of unitary symmetries can have at most $(d!)^2$ elements.*

Proof. For the injectivity all we need to show is that if U is a unitary operator such that $UP_{\mathbf{e}_k}U^* = P_{\mathbf{e}_k}$ and $UP_{\mathbf{f}_k}U^* = P_{\mathbf{f}_k}$ for all $k = 1, \ldots, n$ then U is a multiple of $\mathbf{1}$.

However, the assumed invariance means that both the vectors of $\mathcal{E}$ and the vectors of $\mathcal{F}$ are eigenvectors for U. Thus U commutes with all elements of $\mathcal{A}_\mathcal{E}$ and $\mathcal{A}_\mathcal{F}$. As both of these are maximal Abelian, it follows that $U \in \mathcal{A}_\mathcal{E} \cap \mathcal{A}_\mathcal{F}$. However, by the quasi-orthogonality this intersection contains only multiples of the identity. □

Suppose $(\mathcal{E}, \mathcal{F})$ is a MUB pair and that the unitary operator U implements a symmetry of $(\mathcal{E}, \mathcal{F})$. Since U may only reorder and multiply by unit complex numbers the vectors of both $\mathcal{E}$ and $\mathcal{F}$, it is clear that if $\mathbf{b}$ is a common unbiased vector to $(\mathcal{E}, \mathcal{F})$, then so is $U\mathbf{b}$. Thus such unitary operators allow us to construct (possibly new) common unbiased vectors, once we have at least one such vector.

Before giving a general result, let us show how this may be used to construct an ONB that is unbiased to both the standard basis $\mathcal{E}$ and the Fourier basis of $\mathbb{C}^d$. Let U, V be the linear operators defined by the formulae

$$U\mathbf{e}_k = \mathrm{e}^{\mathrm{i}\frac{2\pi}{d}(k-1)}\mathbf{e}_k, \qquad \text{and} \qquad V\mathbf{e}_k = \mathbf{e}_{k-1}, \tag{39}$$

where the index '$k-1$' is meant by modulo d. Then U, V are unitary, $U^d = V^d = \mathbf{1}$ and $VU = \mathrm{e}^{\mathrm{i}\frac{2\pi}{d}}UV$. However, by the definition of the Fourier basis, a simple check shows that

$$V\mathbf{f}_k = \mathrm{e}^{\mathrm{i}\frac{2\pi}{d}(k-1)}\mathbf{f}_k, \qquad \text{and} \qquad U\mathbf{f}_k = \mathbf{f}_{k+1} \tag{40}$$

for all $k = 1, \ldots, d$ (where the index '$k+1$' is again meant by modulo d). Thus U and V only change the 'phases' and reorder the vectors of both $\mathcal{E}$ and $\mathcal{F}$, thus they implement unitary symmetries of $(\mathcal{E}, \mathcal{F})$. In particular, if $\mathbf{b}$ is a common UB vector for both the standard and the Fourier basis, then so is $U^kV^l\mathbf{b}$ for all $k, l = 1, \ldots, d$.

As is well known in the case of the Fourier basis, if $\mathbf{b}$ is a common normalized UB vector for $(\mathcal{E}, \mathcal{F})$ then the vectors

$$\mathbf{b}, V\mathbf{b}, V^2\mathbf{b}, \ldots, V^{d-1}\mathbf{b}$$

form an ONB. The same stays true if one replaces V by U.

We would like now to extend this to more general pairs of unbiased bases. To do so, note first that in the above case, the natural injection from unitary symmetries into $S_d \times S_d$ sends

U and V to (id, σ) and (σ, id), respectively, where $\sigma \in S_d$ is a cyclic permutation of d, which is a particular example of a permutation without fixed points.

Theorem 4.5. *Let* $(\mathcal{E}, \mathcal{F})$ *be a MUB pair and let* $\mathbf{b}$ *be a normalized vector that is unbiased to both of them. Let* $U_0 = \mathbf{1}, U_1, \ldots, U_k$ *be unitary operators implementing symmetries* $\alpha_0 := \alpha_{U_0} = \mathrm{id}, \alpha_1 := \alpha_{U_1}, \ldots, \alpha_k := \alpha_{U_k}$ *of* $(\mathcal{E}, \mathcal{F})$*. Assume further that for every* $j \neq l$ *the image of* $\alpha_j^{-1} \circ \alpha_l$ *under the natural injection into* $S_n \times S_n$ *is of the form* (σ, id) *or* (id, σ) *where* $\sigma \in S_n$ *is a permutation with no fixed points. Then*

$$(U_0\mathbf{b} = \mathbf{b}, U_1\mathbf{b}, \ldots, U_k\mathbf{b})$$

is an orthonormal family of vectors that are unbiased to both $\mathcal{E}$ *and* $\mathcal{F}$*.*

Proof. Suppose that the image of $\alpha_j^{-1} \circ \alpha_l$ under the natural injection into $S_d \times S_d$ is of the form (σ, id). Then each vector of $\mathcal{F}$ must be an eigenvector for $U_j^* U_l$: there exist some $\lambda_1, \ldots, \lambda_d \in \mathbb{C}$ such that $U_l^* U_j \mathbf{f}_k = \lambda_k \mathbf{f}_k$. Thus

$$\begin{aligned}\langle U_l\mathbf{b}, U_j\mathbf{b}\rangle = \langle \mathbf{b}, U_l^* U_j \mathbf{b}\rangle &= \sum_k \langle \mathbf{b}, \mathbf{f}_k\rangle\langle \mathbf{f}_k, U_l^* U_j \mathbf{b}\rangle \\ &= \sum_k \langle \mathbf{b}, \mathbf{f}_k\rangle\langle U_j^* U_l f_k, \mathbf{b}\rangle = \sum_k \lambda_k |\langle \mathbf{b}, \mathbf{f}_k\rangle|^2 \\ &= \frac{1}{d}\,\mathrm{Tr}(U_j^* U_l).\end{aligned}$$

For this last identity, we have used the fact that $\mathbf{b}$ is unbiased to $\mathcal{F}$, thus $|\langle \mathbf{b}, \mathbf{f}_k\rangle|^2 = 1/d$, and the fact that the sum of the eigenvalues of a diagonalizable operator is its trace. However, by assumption $U_j^* U_l$ takes the vector $\mathbf{e}_k$ into a multiple of $\mathbf{e}_{\sigma(k)}$; say to $\mu_k\, \mathbf{e}_{\sigma(k)}$. Therefore

$$\mathrm{Tr}(U_j^* U_l) = \sum_k \langle U_j^* U_l \mathbf{e}_k, \mathbf{e}_k\rangle = \sum_k \langle \mu_k e_{\sigma(k)}, e_k\rangle = 0$$

as $\mathbf{e}_k$ is always orthogonal to $\mathbf{e}_{\sigma(k)}$ (since σ has no fixed points). □

4.3. Application to the case of $\mathcal{F}_{(a,b)}$

We shall now apply the general statements made so far to the case $(\mathcal{E}, \mathcal{F}(a, b))$ where $\mathcal{E}$ is the standard basis of $\mathbb{C}^6$. As was explained, we have numerical evidence that up to multiple, the number of common normalized unbiased vectors is always 48. At $(a, b) = (0, 0)$, this is a known fact.

Theorem 4.6. *There exists a neighborhood* K *of* $(0, 0)$ *such that when counted up to multiples,* $(\mathcal{E}, \mathcal{F}_{(a,b)})$ *has exactly 48 common normalized unbiased vectors for all* $(a, b) \in K$*.*

Proof. For simplicity, theorem 4.1 and corollary 4.3 were stated for a one-parameter smooth pair of MUB. However, the proofs only rely on the implicit function theorem, so they easily extend to any number of parameters.

But for $(\mathcal{E}, \mathcal{F}(0, 0))$, i.e., for the standard and the (usual) Fourier basis, all 48 vectors (counted up to multiples) that are unbiased to them are explicitly known [7]. It is then easy (but cumbersome) to check that the conditions of corollary 4.3 hold for each of them. □

We have seen that there is a theoretical reason (at least in a neighborhood of the origin) behind the numerical facts that indicate that the number of common unbiased vectors (counted up to multiples) to $(\mathcal{E}, \mathcal{F}(a, b))$ is always 48. Unfortunately, we have so far been unable to find a theoretical ground for the fact that these vectors can always be grouped into eight orthonormal bases. However, we may now give a partial result by applying what we have established about symmetries. To do so, first we shall need to investigate in particular the symmetries of the pair $(\mathcal{E}, \mathcal{F}_{(a,b)})$.

Consider the unitaries U and V defined by equation (39). For a generic value of the parameters a, b they do not implement symmetries. However, U^2 and V^3 implement symmetries of $(\mathcal{E}, \mathcal{F}_{(a,b)})$ for all $(a, b) \in \mathbb{R}^2$. Indeed, it is easy to check that regardless of the value of a and b we still have the relations

$$\begin{array}{lcl} U^2\mathbf{e}_k = \mathrm{e}^{\mathrm{i}\frac{2\pi}{6}2(k-1)}\mathbf{e}_k, & \text{and} & U^2\mathbf{f}_k = \mathbf{f}_{k+2}, \\ V^3\mathbf{e}_k = \mathbf{e}_{k-3} & \text{and} & V^3\mathbf{f}_k = \mathrm{e}^{\mathrm{i}\frac{2\pi}{6}3(k-1)}\mathbf{f}_k, \end{array}$$

where now $\mathbf{f}_1, \ldots, \mathbf{f}_6$ are the vectors of $\mathcal{F}_{(a,b)}$. Thus, by applying theorem 4.5 we can draw the following conclusion.

Corollary 4.7. *Let a, b be two fixed real numbers. Suppose* $\mathbf{b}$ *is a common unbiased vector to the standard basis $\mathcal{E}$ and to the basis $\mathcal{F}_{(a,b)}$. Consider the unitaries U and V defined by equation (39). Then all of the vectors in the table below*

$\mathbf{b}$	$U^2\mathbf{b}$	$U^4\mathbf{b}$
$V^3\mathbf{b}$	$U^2V^3\mathbf{b}$	$U^4V^3\mathbf{b}$

are unbiased to both bases. Moreover, each row and each column consists of pairwise orthogonal vectors.

Unfortunately, this does not show that every common normalized unbiased vector can be extended to an ONB consisting of common unbiased vectors, only. However, in particular, it shows that every common normalized unbiased vector can be extended to an orthonormal *triplet* of unbiased vectors.

Acknowledgments

M Matolcsi was supported by OTKA grants PF-64061 and K-77748, the Junior Fellowship of ESI (Wien, February 2008), and a Visiting Professorship of the University of Orleans, October 2007. J Philippe was partially supported by the French ANR project AHPI (Analyse Harmonique pour les Problems Inverses).

Appendix A. The calculations leading to theorem 2.4

In this section, we provide the detailed calculations leading to theorem 2.4.

Recall the form of the Fourier matrices $F(0, b)$ from equation (3), with $x = 1$, $y = \mathrm{e}^{2\mathrm{i}\pi b}$. We will first look for vectors $\mathbf{u} = \frac{1}{\sqrt{6}}(1, \overline{c}_1, \overline{c}_2, \overline{c}_3, \overline{c}_4, \overline{c}_5)$ that obey the following further constraints[10]: $c_1 = c_3c_4$ or equivalently $c_1\overline{c_4} = c_3$.

We will also write $c_5 = \eta\zeta$ and $c_2 = \overline{\eta}\zeta$ with $|\eta| = |\zeta| = 1$. Then lemma 2.2 implies that

$$\mathrm{Re}(2c_3 + \eta^2) = 0$$

$$(1 + \mathrm{Re}\, c_3)\overline{c_4} + c_4(1 + c_3)\overline{\zeta}\,\mathrm{Re}\,\eta + \overline{(1 + c_3)}\zeta\,\mathrm{Re}\,\eta = 0 \tag{A.1}$$

$$(1 - \mathrm{Re}\, c_3)\overline{c_4} + \mathrm{i}\overline{y}c_4(1 - c_3)\overline{\zeta}\,\mathrm{Im}\,\eta - \mathrm{i}y\overline{(1 - c_3)}\zeta\,\mathrm{Im}\,\eta = 0. \tag{A.2}$$

[10] This particular form was suggested by numerical evidence.

We will write $c_4 = c_6^2$ and multiply (A.1) and (A.2) by $\overline{c_6}$ to obtain

$$(1 + \operatorname{Re} c_3)\overline{c_6}^3 + 2\operatorname{Re}(\overline{(1 + c_3)c_6}\zeta)\operatorname{Re}\eta = 0 \tag{A.3}$$

$$(1 - \operatorname{Re} c_3)\overline{c_6}^3 + 2\operatorname{Im}(\overline{(1 - c_3)c_6}\zeta y)\operatorname{Im}\eta = 0. \tag{A.4}$$

Note that either (A.3) or (A.4) imply that c_6^3 is real, i.e., $c_6^3 = \pm 1$. We will restrict our attention to $c_6^3 = 1$, that is, $c_6 = 1, \omega, \omega^2$, thus $c_4 = c_6^2 = \overline{c_6} = 1, \omega^2$ or ω.

Further, writing $\nu = \overline{c_6}\zeta$, $z = -\mathrm{i}y$ and using elementary computations, we obtain

$$2\operatorname{Re} c_3 + \operatorname{Re}\eta^2 = 0 \tag{A.5}$$

$$(1 + \operatorname{Re} c_3)(1 + 2\operatorname{Re}\nu\operatorname{Re}\eta) + 2\operatorname{Im} c_3\operatorname{Im}\nu\operatorname{Re}\eta = 0 \tag{A.6}$$

$$(1 - \operatorname{Re} c_3)(1 + 2\operatorname{Im}(\nu y)\operatorname{Im}\eta) + 2\operatorname{Im} c_3\operatorname{Re}(\nu y)\operatorname{Im}\eta = 0. \tag{A.7}$$

Assume now we have a solution (c_3, ν, η) of the system (A.5)–(A.6)–(A.7). Then $(1, c_3c_4, \nu\overline{\eta c_4}, c_3, c_4, \nu\eta\overline{c_4})$ with $c_4 = 1, \omega$ or ω^2 are solutions of (12)–(14)–(15) (with $x = 1$). In other words, the conjugates (!) of the following vectors

$$w_1 = (1, c_3, \nu\bar{\eta}, c_3, 1, \nu\eta), \qquad w_2 = (1, c_3\omega, \nu\bar{\eta}\omega^2, c_3, \omega, \nu\eta\omega^2)$$

and

$$w_3 = (1, c_3\omega^2, \nu\bar{\eta}\omega, c_3, \omega^2, \nu\eta\omega)$$

are unbiased to both the standard and the $F(0, b)$ basis. It is also easy to see that these three vectors are orthogonal to each other.

However, we need three more vectors. This is achieved via a *miracle* that was indicated by numerical evidence. More precisely, assume that (c_3, η, ν) is a solution of the system and that $(\tilde{c}_3, \tilde{\eta}, \tilde{\nu}) = (-c_3, \mathrm{i}\eta, \tilde{\nu})$ is another solution of the system. We then have six vectors that are unbiased to both the standard and the $F(0, b)$ basis. Moreover, the three vectors $\overline{w_1}, \overline{w_2}, \overline{w_3}$ stemming from the first solution are orthogonal and so are those stemming from the second solution, $\overline{w_4}, \overline{w_5}, \overline{w_6}$, namely

$$w_4 = (1, -c_3, -\mathrm{i}\tilde{\nu}\bar{\eta}, -c_3, 1, \mathrm{i}\tilde{\nu}\eta), \qquad w_5 = (1, -c_3\omega, -\mathrm{i}\tilde{\nu}\bar{\eta}\omega^2, -c_3, \omega, \mathrm{i}\tilde{\nu}\eta\omega^2)$$

and

$$w_6 = (1, -c_3\omega^2, -\mathrm{i}\tilde{\nu}\bar{\eta}\omega, -c_3, \omega^2, \mathrm{i}\tilde{\nu}\eta\omega).$$

Finally, it is easy to check that each of

$$\overline{w_1}, \overline{w_2}, \overline{w_3}$$

is orthogonal to each of

$$\overline{w_4}, \overline{w_5}, \overline{w_6}$$

so that $(\overline{w_1}, \ldots, \overline{w_6})$ is an orthogonal basis unbiased to both the standard and the $F(0, b)$ basis.

It thus remains to exhibit two such families of solutions. To be more precise, we will write $\eta = \mathrm{e}^{\mathrm{i}t}$ and show that, for a certain range of t, we may chose $y = \mathrm{e}^{\mathrm{i}\beta(t)}$ in such a way that the system (A.5)–(A.6)–(A.7) has a solution $\big(c_3(t), \mathrm{e}^{\mathrm{i}t}, \nu(t)\big)$, and such that there is a second solution $\big(-c_3(t), \mathrm{i}\,\mathrm{e}^{\mathrm{i}t}, \tilde{\nu}(t)\big)$.

Now, if $\eta = \mathrm{e}^{\mathrm{i}t}$, then $\operatorname{Re} c_3(t) = -\frac{\cos 2t}{2}$ and, as $|c_3| = 1$, there are only two possibilities, $c_3(t) = -\frac{\cos 2t}{2} \pm \mathrm{i}\big(1 - \frac{\cos^2 2t}{4}\big)^{1/2}$. For the sake of simplicity, we will take the + sign:

$$c_3(t) = -\frac{\cos 2t}{2} + \mathrm{i}\left(1 - \frac{\cos^2 2t}{4}\right)^{1/2}. \tag{A.8}$$

Let us first determine $\nu = \mathrm{e}^{\mathrm{i}\varphi(t)}$. To reduce the length and complexity of formulae, we will drop the dependence on t in them and simply write c_3, β, φ.

But ν satisfies (A.6)–(A.7) which now read

$$-(2-\cos 2t)\cos t\cos\varphi - \sqrt{4-\cos^2 2t}\cos t\sin\varphi = 1-\frac{\cos 2t}{2}$$

$$\begin{aligned}&((2+\cos 2t)\sin\beta + \sqrt{4-\cos^2 2t}\cos\beta)\sin t\cos\varphi\\ &\qquad + ((2+\cos 2t)\cos\beta - \sqrt{4-\cos^2 2t}\sin\beta)\sin t\sin\varphi = -1-\frac{\cos 2t}{2}.\end{aligned}$$

Let us write these equations in a simpler form by introducing the following parameter:

$$\psi = \arccos\frac{\sqrt{2+\cos 2t}}{2} \tag{A.9}$$

so that $\cos\psi = \frac{\sqrt{2+\cos 2t}}{2}$ and $\sin\psi = \frac{\sqrt{2-\cos 2t}}{2}$. A simple computation then shows that we want to solve

$$-\sin\psi\cos t\cos\varphi - \cos\psi\cos t\sin\varphi = \frac{\sin\psi}{2} \tag{A.10}$$

$$\sin(\beta+\psi)\sin t\cos\varphi + \cos(\beta+\psi)\sin t\sin\varphi = -\frac{\cos\psi}{2}. \tag{A.11}$$

Remark A.1. This system may not have solutions. For instance, it is easy to see that $\cos\psi$ and $\sin\psi$ do not vanish, but the left-hand side of (A.10)—resp. (A.11)—vanishes when $t = \pi/2$ — resp. $t = 0$. So for t near 0 or t near $\pi/2$, we do not expect to find a solution this way.

The solution is now easy to obtain:

$$\cos\varphi = \frac{-\cos^2\psi\cos t + \cos(\beta+\psi)\sin\psi\sin t}{\sin\beta\sin 2t} \tag{A.12}$$

and

$$\sin\varphi = \frac{\sin\psi\cos\psi\cos t - \sin(\beta+\psi)\sin\psi\sin t}{\sin\beta\sin 2t}. \tag{A.13}$$

It has still to be shown that this is a legitimate solution, that is, to check whether (A.12)–(A.13) define the cosine and sine of an angle φ. For this, it is sufficient to check that $\cos\varphi, \sin\varphi$ defined by these formulae satisfy $\cos^2\varphi + \sin^2\varphi = 1$. This easily reduces to

$$\cos^2\psi\cos^2 t + \sin^2\psi\sin^2 t - 2\cos t\sin t\cos\psi\sin\psi\cos\beta = \sin^2\beta\sin^2 2t. \tag{A.14}$$

Note that $\cos\psi\sin\psi = \frac{\sqrt{4-\cos^2 2t}}{4}$ and

$$\begin{aligned}\cos^2\psi\cos^2 t + \sin^2\psi\sin^2 t - \sin^2 2t &= \frac{2+\cos 2t}{4}\cos^2 t + \frac{2-\cos 2t}{4}\sin^2 t - \sin^2 2t\\ &= -\frac{1}{2} + \frac{5}{4}\cos^2 2t.\end{aligned}$$

We thus have to check that

$$-\frac{1}{2} + \frac{5}{4}\cos^2 2t - \frac{\sqrt{4-\cos^2 2t}}{4}u + u^2 = 0,$$

where $u = \cos\beta \sin 2t$. One solution of this equation is

$$\cos\beta = \frac{\sqrt{4-\cos^2 2t} + 3\sqrt{4-9\cos^2 2t}}{8\sin 2t} = \frac{\sqrt{3+\sin^2 2t} + 3\sqrt{9\sin^2 2t - 5}}{8\sin 2t}, \tag{A.15}$$

and we omit the possible other root here. It is clear that, whenever $\frac{\sqrt{5}}{3} \leqslant |\sin 2t| \leqslant 1$ holds, we obtain a legitimate real number for β.

It remains to find $\tilde{\nu} = \mathrm{e}^{\mathrm{i}\tilde{\varphi}}$ such that

$$(\tilde{c}_3(t), \tilde{\eta}(t), \tilde{\nu}(t)) = (-c_3(t), \mathrm{i}\,\mathrm{e}^{\mathrm{i}t}, \tilde{\nu}(t))$$

is also a solution of (A.5), (A.6), (A.7). Recall that the value of $y = \mathbf{e}^{\mathbf{i}\beta}$ has just been determined.

Note that

$$2\,\mathrm{Re}\,\tilde{c}_3 + \mathrm{Re}\,\tilde{\eta}^2 = -(2\,\mathrm{Re}\,c_3 + \mathrm{Re}\,\eta^2) = 0$$

so that (A.5) is satisfied. The other two equations read

$$-(2+\cos 2t)\sin t\cos\tilde{\varphi} + \sqrt{4-\cos^2 2t}\,\sin t\sin\tilde{\varphi} = -\frac{2+\cos 2t}{2}$$

and

$$((2-\cos 2t)\sin\beta - \sqrt{4-\cos^2 2t}\,\cos\beta)\cos t\cos\tilde{\varphi} + ((2-\cos 2t)\cos\beta + \sqrt{4-\cos^2 2t}\,\sin\beta)\cos t\sin\tilde{\varphi} = -\frac{2-\cos 2t}{2},$$

where the dependence on t in β and $\tilde{\varphi}$ has been dropped. From this, we deduce that

$$\cos\tilde{\varphi} = \frac{-\sin t\sin^2\psi + \cos\psi\cos t\sin(\beta+\psi)}{\sin\beta\sin 2t} \tag{A.16}$$

$$\sin\tilde{\varphi} = \frac{\cos\psi\cos(\beta+\psi)\cos t - \cos\psi\sin t\sin\psi}{\sin\beta\sin 2t}. \tag{A.17}$$

It is left to see that $\tilde{\varphi}$ is a legitimate real number, that is, summing the squares of the two numbers defined in (A.16)–(A.17) yields 1. It is easy to check that this holds if and only if (A.14) holds, hence there are no further restrictions on t.

In summary, we have proved theorem 2.4.

Remark A.2. As pointed out by one of the Referees, lemma 2.2 may be reformulated in the following way: consider the shift matrix S and the diagonal matrix D given by

$$S = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad\text{and}\quad D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & y \end{pmatrix}.$$

Let

$$\mathbf{w} = \begin{pmatrix} 1+c_3 \\ c_1+c_4 \\ c_2+c_5 \end{pmatrix}, \qquad \mathbf{v} = \begin{pmatrix} 1-c_3 \\ c_4-c_1 \\ c_2-c_5 \end{pmatrix}$$

and

$$\mathbf{u} = \frac{1}{\sqrt{6}}(1, \bar{c}_1, \bar{c}_2, \bar{c}_3, \bar{c}_4, \bar{c}_5).$$

Note that the pair $(\mathbf{w}, \mathbf{v})$ and the vector $\mathbf{u}$ determine each other uniquely. Also, equations (11)–(14) (and therefore lemma 2.2) are equivalent to

$$\langle \mathbf{w}, S\mathbf{w}\rangle = \langle D\mathbf{v}, SD\mathbf{v}\rangle = 0, \qquad |\mathbf{w}|^2 = |D\mathbf{v}|^2 = 6.$$

The solutions found above are of the particular form

$$\mathbf{w} = (1 \pm c_3)\begin{pmatrix} 1 \\ \omega^k \\ z \end{pmatrix} \qquad \text{and} \qquad \mathbf{v} = (1 \mp c_3)\begin{pmatrix} 1 \\ \omega^k \\ z' \end{pmatrix},$$

for $k = 0, 1, 2$ and for suitable z, z'. For an arbitrary choice of parameters (x, y), it would be desirable to describe all 48 pairs $(\mathbf{w}, \mathbf{v})$ corresponding to the 48 vectors $\mathbf{u}$ unbiased to the standard basis and $F(x, y)$. We have unfortunately been unable to exploit this observation any further. Possibly an automated calculation using Gröbner bases could lead to a general analytic solution in the future (e.g., a generalization of the method in [10]).

Appendix B. A construction by G Zauner that leads to another one-parameter family

This section is inspired by Zauner's PhD thesis [32]. As this thesis is only available in German, we take this occasion to present his construction to a wider audience and to compare his construction to our family given in theorem 2.4. We emphasize that the all credit for the results of this section goes to Zauner.

Let us recall that a *circulant* matrix A is a matrix of the form

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & \cdots & a_{m-1} \\ a_{m-1} & a_0 & a_1 & \cdots & \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & a_0 & a_1 \\ a_1 & \cdots & \cdots & a_{m-1} & a_0 \end{pmatrix}.$$

It is easy to check that, for each $k = 0, \ldots, m-1$, the vector

$$\mathbf{f}_k = (1, \omega^k, \omega^{2k}, \ldots, \omega^{(m-1)k}), \qquad \omega = \mathrm{e}^{2\mathrm{i}\pi/m}$$

is an eigenvector of A. We may thus write $A = \mathcal{F}_m^* \bar{A} \mathcal{F}_m$ where $\mathcal{F}_m = [m^{-1/2}\omega^{jk}]_{0\leqslant j,k\leqslant m-1}$ is the $m \times m$ Fourier matrix and $\bar{A}$ is a diagonal matrix.

Now, let $A_{0,0}, A_{0,1}, A_{1,0}, A_{1,1}$ be four $m \times m$ circulant matrices and write $A_{i,j} = \mathcal{F}_m^* \bar{A}_{i,j} \mathcal{F}_m$ where

$$\bar{A}_{i,j} = \mathrm{diag}(\alpha_{i,j}(0), \ldots, \alpha_{i,j}(m-1)) := \begin{pmatrix} \alpha_{i,j}(0) & & 0 \\ & \ddots & \\ 0 & & \alpha_{i,j}(m-1) \end{pmatrix}$$

is diagonal. Let T be the $2m \times 2m$ matrix given by $T = \begin{pmatrix} A_{0,0} & A_{0,1} \\ A_{1,0} & A_{1,1} \end{pmatrix}$. Then

$$T = \begin{pmatrix} \mathcal{F}_m^* & 0 \\ 0 & \mathcal{F}_m^* \end{pmatrix} \begin{pmatrix} \bar{A}_{0,0} & \bar{A}_{0,1} \\ \bar{A}_{1,0} & \bar{A}_{1,1} \end{pmatrix} \begin{pmatrix} \mathcal{F}_m & 0 \\ 0 & \mathcal{F}_m \end{pmatrix}$$

so that T is unitary if and only if $\begin{pmatrix} \bar{A}_{0,0} & \bar{A}_{0,1} \\ \bar{A}_{1,0} & \bar{A}_{1,1} \end{pmatrix}$ is unitary. But, this matrix is unitary if and only if the m matrices $S_k = \begin{pmatrix} \alpha_{0,0}(k) & \alpha_{0,1}(k) \\ \alpha_{1,0}(k) & \alpha_{1,1}(k) \end{pmatrix}$ are unitary $(k = 0, \ldots, m-1)$. Finally, one may easily check that a 2×2 matrix is unitary if and only if it can be written in the form

$$S(\beta_0, \beta_1, \beta_2, \beta_3) = \frac{1}{2}\begin{pmatrix} \mathrm{e}^{\mathrm{i}\beta_0} + \mathrm{e}^{\mathrm{i}\beta_1} & \mathrm{e}^{\mathrm{i}\beta_3}(\mathrm{e}^{\mathrm{i}\beta_0} - \mathrm{e}^{\mathrm{i}\beta_1}) \\ \mathrm{e}^{\mathrm{i}\beta_2}(\mathrm{e}^{\mathrm{i}\beta_0} - \mathrm{e}^{\mathrm{i}\beta_1}) & \mathrm{e}^{\mathrm{i}\beta_2}\,\mathrm{e}^{\mathrm{i}\beta_3}(\mathrm{e}^{\mathrm{i}\beta_0} + \mathrm{e}^{\mathrm{i}\beta_1}) \end{pmatrix}.$$

For all $0 \leqslant k \leqslant m-1$, we may thus write $S_k = S(\beta_0(k), \beta_1(k), \beta_2(k), \beta_3(k))$ and define $U_\ell = \operatorname{diag}(\mathrm{e}^{\mathrm{i}\beta_\ell(0)}, \ldots, \mathrm{e}^{\mathrm{i}\beta_\ell(m-1)})$ for $\ell = 0, 1, 2$ and 3. Then define

$$E_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathcal{F}_m & U_2^* \mathcal{F}_m \\ \mathcal{F}_m & -U_2^* \mathcal{F}_m \end{pmatrix} \tag{B.1}$$

and

$$E_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} U_0 \mathcal{F}_m & U_0 U_3 \mathcal{F}_m \\ U_1 \mathcal{F}_m & -U_1 U_3 \mathcal{F}_m \end{pmatrix}, \tag{B.2}$$

and a straightforward computation gives $T = E_1^* E_2$. Finally, note that E_1 and E_2 are Hadamard matrices so that if T itself is a Hadamard matrix, then the standard matrix, the columns of E_1 and the columns of E_2 are three mutually unbiased bases in $\mathbb{C}^{2m}$.

As an example for $m = 3$, Zauner [32] considers the following matrix:

$$T(x) = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & -\mathrm{e}^{-\mathrm{i}x} & \mathrm{e}^{\mathrm{i}x} & -1 & \mathrm{i}\,\mathrm{e}^{-\mathrm{i}x} & \mathrm{i}\,\mathrm{e}^{\mathrm{i}x} \\ \mathrm{e}^{\mathrm{i}x} & 1 & -\mathrm{e}^{-\mathrm{i}x} & \mathrm{i}\,\mathrm{e}^{\mathrm{i}x} & -1 & \mathrm{i}\,\mathrm{e}^{-\mathrm{i}x} \\ -\mathrm{e}^{-\mathrm{i}x} & \mathrm{e}^{\mathrm{i}x} & 1 & \mathrm{i}\,\mathrm{e}^{-\mathrm{i}x} & \mathrm{i}\,\mathrm{e}^{\mathrm{i}x} & -1 \\ 1 & \mathrm{i}\,\mathrm{e}^{-\mathrm{i}x} & \mathrm{i}\,\mathrm{e}^{\mathrm{i}x} & 1 & \mathrm{e}^{-\mathrm{i}x} & -\mathrm{e}^{\mathrm{i}x} \\ \mathrm{i}\,\mathrm{e}^{\mathrm{i}x} & 1 & \mathrm{i}\,\mathrm{e}^{-\mathrm{i}x} & -\mathrm{e}^{\mathrm{i}x} & 1 & \mathrm{e}^{-\mathrm{i}x} \\ \mathrm{i}\,\mathrm{e}^{-\mathrm{i}x} & \mathrm{i}\,\mathrm{e}^{\mathrm{i}x} & 1 & \mathrm{e}^{-\mathrm{i}x} & -\mathrm{e}^{\mathrm{i}x} & 1 \end{pmatrix}.$$

Then $T(x)$ is a one-parameter family of complex Hadamard matrices of the form $T(x) = \left(\begin{smallmatrix} A_{0,0}(x) & A_{0,1}(x) \\ A_{1,0}(x) & A_{1,1}(x) \end{smallmatrix}\right)$. Therefore, the construction above yields a one-parameter family of MUB-triplets $(Id, E_1(x), E_2(x))$.

Finally we note that Zauner's family $(Id, E_1(x), E_2(x))$ is not equivalent to our family presented in theorem 2.4. This can be seen in the following way. After dephasing the rows and columns, the transition matrix $T(x) = E_1^*(x) E_2(x)$ is easily seen to be a member of the Dita-family $D_6(x)$ (cf [29] for the Dita-family of complex Hadamard matrices of order 6). However, in our construction in theorem 2.4, generically none of the appearing matrices $F(0, b(t))$, $C(t)$ and $F(0, b(t))^* C(t)$ are members of the Dita-family. This is true, because $F(0, b(t))$, $C(t)$ are members of the generalized Fourier family $F(a, b)$, while the transition matrix $F(0, b(t))^* C(t)$ generically has a much larger Haagerup-invariant set than the Dita-matrices $D_6(x)$, therefore they cannot be equivalent.

References

[1] Aharonov Y and Englert B-G 2001 The mean king's problem: spin 1 *Z. Naturforsch.* **56a** 16

[2] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 A new proof for the existence of mutually unbiased bases *Algorithmica* **34** 512–28

[3] Beauchamp K and Nicoara R 2008 Orthogonal maximal Abelian ∗-subalgebras of the 6 × 6 matrices *Linear Algebra Appl.* **428** 1833–53

[4] Bechmann-Pasquinucci H and Tittel W 2000 Quantum cryptography using larger alphabets *Phys. Rev.* A **61** 062308

[5] Bengtsson I, Bruzda W, Ericsson Å, Larsson J-A, Tadej W and Życzkowski K 2007 Mutually unbiased bases and Hadamard matrices of order six *J. Math. Phys.* **48** 052106

[6] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing, IEEE* pp 175–79

[7] 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 1* **320** 319–24

[8] Bonami A and Poly J-B The discrete Pauli problem (in preparation)

[9] Brierley S and Weigert S 2008 Maximal sets of mutually unbiased quantum states in dimension six arXiv:0808.1614 [quant-ph]

[10] Brierley S and Weigert S 2009 Constructing mutually unbiased bases in dimension six arXiv:0901.4051

[11] 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

[12] Combescure M 2007 The mutually unbiased bases revisited *Adventures in Mathematical Physics (Contemp. Math.* vol 447*)* (Providence, RI: American Mathematical Society) pp 29–43

[13] Combescure M 2007 Circulant matrices, Gauss sums and mutually unbiased bases: I. The prime number case arXiv:0710.5642v1

[14] Combescure M 2007 Circulant matrices, Gauss sums and mutually unbiased bases: II. The prime power case arXiv:0710.5643v1

[15] Corbett J V 2006 The Pauli problem, state reconstruction and quantum-real numbers *Rep. Math. Phys.* **57** 53–68

[16] Delsarte P, Goethals J M and Seidel J J 1977 Spherical codes and designs *Geom. Dedic.* **6** (3) 363–88

[17] Grassl M 2004 On SIC-POVMs and MUBs in dimension 6 *Proc. ERATO Conf. on Quantum Information Science (EQUIS 2004)* ed J Gruska

[18] Haagerup U 1996 Ortogonal maximal Abelian ∗-subalgebras of $n \times n$ matrices and cyclic n-roots *Operator Algebras and Quantum Field Theory (Rome)* (Cambridge: International) pp 296–322

[19] Hoggar S G 1982 T-designs in projective spaces *Eur. J. Comb.* **3** 233–54

[20] Ivanovic I D 1981 Geometrical description of quantal state determination *J. Phys. A: Math. Gen.* **14** 3241

[21] Jaming Ph 1999 Phase retrieval techniques for radar ambiguity problems *J. Fourier Anal. Appl.* **5** 309–29

[22] Kabatiansky G A and Levenshtein V I 1978 Bounds for packings on a sphere and in space *Probl. Inf. Transm.* **14** 1–17

[23] Klappenecker A and Rötteler M 2004 Constructions of mutually unbiased bases *Finite Fields and Applications (Lecture Notes in Computer Science* vol 2948*)* (Berlin: Springer) pp 137–44

[24] Lam C W H, Thiel L H and Swiercz S 1989 The non-existence of finite projective planes of order 10 *Can. J. Math.* **XLI** 1117–23

[25] Matolcsi M and Szöllősi F 2008 Towards a classification of 6 × 6 complex Hadamard matrices *Open Syst. Inf. Dyn.* **15** 93–108

[26] Renes J M 2005 Equiangular spherical codes in quantum cryptography *Quantum Inf. Comput.* **5** 81–92

[27] Schwinger J 1960 Unitary operator bases *Proc. Natl Acad. Sci. USA* **46** 560

[28] Skinner A J, Newell V A and Sanchez R 2008 Unbiased bases (Hadamards) for 6-level systems: four ways from Fourier arXiv:0810.1761

[29] Tadej W and Życzkowski K 2006 A concise guide to complex Hadamard matrices *Open Syst. Inf. Dyn.* **13** 133–77

[30] Werner R F 2001 All teleportation and dense coding schemes. Quantum information and computation *J. Phys. A: Math. Gen.* **34** 7081–94

[31] Wootters W K and Fields B D 1989 Optimal state-determination by mutually unbiased measurements *Ann. Phys.* **191** 363–81

[32] Zauner G 1999 Quantendesigns Grundzüge einer nichtkommutativen Designtheorie *PhD Thesis,* Universität Wien (available at http://www.mat.univie.ac.at/∼neum/ms/zauner.pdf)

[33] Documentation of results: http://www.math.bme.hu/∼matolcsi/angpubl.html