arXiv:0901.4051v1 [quant-ph] 26 Jan 2009

Constructing Mutually Unbiased Bases in Dimension Six

Stephen Brierley and Stefan Weigert
Department of Mathematics, University of York
Heslington, UK-York YO10 5DD
sb572@york.ac.uk,slow500@york.ac.uk

January 2009

Abstract

The density matrix of a qudit may be reconstructed with *optimal* efficiency if the expectation values of a specific set of observables are known. In dimension six, the required observables only exist if it is possible to identify *six* mutually unbiased complex (6×6) Hadamard matrices. Prescribing a first Hadamard matrix, we construct all others mutually unbiased to it, using algebraic computations performed by a computer program. We repeat this calculation many times, sampling all known complex Hadamard matrices, and we never find more than *two* that are mutually unbiased. This result adds considerable support to the conjecture that no seven mutually unbiased bases exist in dimension six.

1 Introduction

Suppose you want to reconstruct the density matrix ρ of a qudit, a quantum system with d orthogonal states. To apply the *most efficient* reconstruction method you should measure a set of observables associated with d mutually unbiased complex Hadamard matrices of size $(d \times d)$. A *complex Hadamard matrix H* is a unitary matrix having entries of modulus $1/\sqrt{d}$ only; two such matrices are said to be *mutually unbiased* (MU) if their product is another Hadamard matrix,

$$H^\dagger H' = H'' \,, \tag{1}$$

where $H^\dagger$ denotes the adjoint of the matrix H. The columns of d MU complex Hadamard matrices and of the identity define a *complete* set of $(d+1)$ MU orthonormal bases in the space $\mathbb{C}^d$ suitable for optimal state reconstruction [1, 2]. Complete MU bases are often characterized directly by the scalar products between their elements,

$$\left|\langle \psi_j^b | \psi_{j'}^{b'} \rangle\right| = \begin{cases} \delta_{jj'} & \text{if } b = b' \,, \\ \frac{1}{\sqrt{d}} & \text{if } b \neq b' \,, \end{cases} \tag{2}$$

where $b, b' = 0, 1, \ldots, d$; they are also used in quantum cryptography [3] and play an important role in the solution of the Mean King's problem [4].

Here is the catch: as of today, complete sets of MU bases have been constructed only in spaces $\mathbb{C}^d$ of prime or prime power dimension. If the dimension is a *composite* number, $d = 6, 10, 12, \ldots$, the existence of a complete set of MU bases in $\mathbb{C}^d$ has neither been proved nor disproved (see [5] for a review). In other words, it is unknown even for a qubit-qutrit system whether there exists a set of observables which would realize optimal state reconstruction. Interestingly, constructing complete sets of MU bases is equivalent to finding an orthogonal decomposition of the Lie algebra $sl_d(\mathbb{C})$, which poses a long-standing open problem whenever d is not a prime power [6].

Let us summarize what is know about the (non-) existence of MU bases in composite dimensions. There are a few *analytic* results:

- it is possible to construct *three* MU bases in $\mathbb{C}^d$ without reference to the value of d [7]; hence, three MU bases do exist for any composite dimension d;
- there are at least $(p^k + 1)$ MU bases if p, the smallest factor of the prime decomposition of d, occurs $k \geq 1$ times [8];
- more than (p^k+1) MU bases are known exist for specific values of d; for example, if $d = 2^2 \times 13^2$, a total of 6 $(\equiv p^k + 2)$ MU bases have been identified [9].

Attempts to generalize number-theoretic formulæ used in the construction of complete MU bases from prime-power dimensions to composite dimensions fail [10]. Furthermore, searches for MU bases in dimension six by *numerical* means have been unsuccessful:

- no evidence for the existence of *four* MU bases in $\mathbb{C}^6$ has been found [11];
- strong numerical evidence against the existence of various MU *constellations* (corresponding to *subsets* of four MU bases) has been obtained, making the existence of a complete set highly unlikely [12].

Some rigorous results have been obtained by restricting the search to MU bases of a specific form:

- selecting a first Hadamard matrix and then searching for MU vectors with components given by suitable roots of unity leads to no more than two MU complex Hadamard matrices, or three MU bases in $\mathbb{C}^6$ [13];
- Grassl [7] has shown that only *finitely* many vectors exist which are MU with respect to the identity and a given complex Hadamard matrix related to the Heisenberg-Weyl group in $\mathbb{C}^6$. Again, no more than two MU Hadamard matrices emerge, giving rise to at most three MU bases; it is thus impossible to base the construction of a complete set on the Heisenberg-Weyl group.

The strategy of this paper will be to generalize Grassl's approach by removing the restriction that the second MU basis be related to the Heisenberg-Weyl group. Instead, we will consider many different choices for the second MU basis, thoroughly sampling the set of currently known complex Hadamard matrices. We will find that none of the matrices studied can be used to construct a complete set of MU bases. Taken together, these negative instances provide further strong support for the conjecture that no seven MU bases exist in dimension six.

Let us now present the outline of our argument. In Sec. 2, we briefly describe the set of known complex Hadamard matrices in dimension six. Then, we explain in Sec. 3 how to construct all vectors that are MU with respect to both the standard basis of $\mathbb{C}^6$ and a second basis, defined by an arbitrary fixed Hadamard matrix. We illustrate the algorithm for $d = 3$ only to rediscover the known complete set of four MU bases. Then, whilst rederiving Grassl's result for $d = 6$, we will explain the subtle interplay between algebraic and numerical calculations in this approach. Sec. 4 presents our findings which we obtain by applying the algorithm to nearly 6000 Hadamard matrices of dimension six. Conclusions are drawn in the final section.

2 Complex Hadamard matrices in dimension six

Traditionally, a Hadamard matrix H in dimension d is understood to have elements ± 1 only and to satisfy the condition $H^\dagger H = dI$, where I is the identity. In the context of MU bases, it is customary to call H a *Hadamard* matrix if it is unitary and its matrix elements are of the form

$$|H_{ij}| = \frac{1}{\sqrt{d}}\,, \qquad i, j = 0, 1, \ldots, d-1\,. \tag{3}$$

The d vectors formed by the columns of such a matrix provide an orthonormal basis of $\mathbb{C}^d$. Each of these vectors is mutually unbiased with respect to the standard basis, naturally associated with the identity matrix I. It is convenient to identify a Hadamard matrix with the MU basis formed by its columns.

Two Hadamard matrices are *equivalent* to each other, $H' \approx H$, if one can be obtained from the other by permutations of its columns and its rows, and by the multiplication of its columns and rows with individual phase factors. Explicitly, the equivalence relation reads

$$H' = M_1 H M_2\,, \tag{4}$$

where M_1 and M_2 are *monomial* matrices, i.e. they are unitary and have only one nonzero element in each row and column. Consequently, each Hadamard matrix is equivalent to a *dephased* Hadamard matrix, the first row and column of which have entries $1/\sqrt{d}$ only.

All (complex) Hadamard matrices are known for dimensions $d \leq 5$ but there is no exhaustive classification for $d = 6$. It is useful to briefly describe the Hadamard matrices known to exist in dimension six since we will 'parametrize' the search for MU bases in terms of Hadamard matrices. We use the notation introduced in [14] the authors of which maintain an online catalog of Hadamard matrices [15].

Each point in Fig. 1, an updated version of a figure presented in [13], corresponds to one Hadamard matrix of dimension six, except for the interior of the upper circle where a point represents two Hadamard matrices (cf. below). There is one *isolated point*, representing the spectral matrix S given in [16], also known as Tao's matrix [17]. Three sets of Hadamard matrices labeled by a *single parameter* are known: the Diţă family $D(x)$ introduced in [18], a family of symmetric matrices denoted by $M(t)$ [19] and the family of all Hermitean Hadamard matrices $B(\theta)$ [20]. Two *two-parameter* families of Hadamard matrices are known to arise from discrete Fourier-type transformations $F(x_1, x_2)$ in $\mathbb{C}^6$, and from their transpositions, $F^T(x_1, x_2)$ [21]. The Szöllősi family $X(a, b)$ is the only other known two-parameter set [22]. Interestingly, the matrix $X(0, 0)$ can be shown to be equivalent to $F(1/6, 0)$, and there is a second possibility to define a matrix at this point, giving rise to $X^T(0, 0) \approx F^T(1/6, 0)$ [23]. We have noticed that such a doubling actually occurs for *all* values of the parameters (a, b) leading to a set of Hadamard matrices $X^T(a, b)$ inequivalent to $X(a, b)$. Hence, the interior of the upper circle in Fig. 1 represents two layers of Hadamard matrices which are glued together at the boundary of the circle. Topologically, the Szöllősi family $X(a, b)$ and the set $X^T(a, b)$ thus combine to form the surface of a sphere. Appendix A lists the explicit forms of Hadamard matrices as well as the parameter ranges which have been reduced to their *fundamental regions* using the equivalence relation (4).

Fig. 1 also shows equivalences between Hadamard matrices simultaneously belonging to different families. The circulant Hadamard matrix C [24], for example, embeds into the Hermitean family which in turn is given by the boundary of the Szöllősi families. Lining up some of the points where different families overlap suggests that we arrange the Hadamard matrices in a symmetrical way. There are two reasons for this: for the Diţă, Hermitean and symmetric families, a reflection about the line passing through the points $F(0,0)$ and S maps $H(\mathbf{x})$ to $H(-\mathbf{x})$, while the same reflection sends $H(\mathbf{x})$ to $H^T(\mathbf{x})$ if the matrix $H(\mathbf{x})$ is a member of the Diţă, Hermitean or Fourier families; for the Szöllősi family, the reflection about the vertical axis must be supplemented by a change of layer in order to get from $X(a,b)$ to $X^T(a,b)$.

Let us finally mention that the known families of Hadamard matrices come in two different types, *affine* and *non-affine* ones. The set $H(\mathbf{x})$ is affine if it can be written in the form

$$H(\mathbf{x}) = H(0) \circ \text{Exp}[R(\mathbf{x})] \tag{5}$$

for some matrix R; the open circle denotes the Hadamard (elementwise) product of two matrices, $(A \circ B)_{ij} = A_{ij}B_{ij}$, and Exp$[R]$ represents the matrix R elementwise exponentiated: $(\text{Exp}[R])_{ij} = \exp R_{ij}$. Both Fourier-type families and the Diţă matrices are affine (cf. Appendix A) while the symmetric, Hermitean and Szöllősi families are not.

3 Constructing MU Vectors

In this section, we make explicit the conditions on a vector $\mathbb{C}^6$ to be MU with respect to the standard matrix and a fixed Hadamard matrix, i.e. tothe pair $\{I, H\}$. Then we outline an algorithm to construct *all* solutions of the resulting multivariate polynomial equations, allowing us to check how many additional MU Hadamard matrices do exist. We illustrate this approach by constructing a complete set of *four* MU bases in dimension $d = 3$, and we reproduce Grassl's result for $d = 6$ in order to explain that this approach produces rigorous results in spite of inevitable numerical approximations.

3.1 MU vectors and multivariate polynomial equations

A vector $|v\rangle \in \mathbb{C}^d$ is MU with respect to the standard basis (associated with the columns of the identity I) if each of its components has modulus $1/\sqrt{d}$. Furthermore, $|v\rangle$ is MU with respect to a fixed Hadamard matrix H if $|\langle h(k)|v\rangle|^2 = 1/d$, where $|h(k)\rangle$ is the state associated with the k^{th} column $h(k)$ of H, $k = 0, \ldots, d-1$.

Let us express these conditions on $|v\rangle$ in terms of its components v_j, written as

$$\sqrt{d} v_j = \begin{cases} 1 & j = 0\,, \\ x_j + iy_j & j = 1, \ldots, d-1\,, \end{cases} \tag{6}$$

where x_j, y_j are $2(d-1)$ real parameters. The overall phase of the state $|v\rangle$ is irrelevant which allows us to fix the phase of its first component. Then, the first set of constraints on the state $|v\rangle$ reads

$$x_j^2 + y_j^2 = 1\,, \quad j = 1, \ldots, d-1\,, \tag{7}$$

and the second set is given by

$$\left| \sum_{j=0}^{d-1} h_j^*(k) v_j \right|^2 \equiv \left| \sum_{j=0}^{d-1} H_{kj}^\dagger (x_j + iy_j) \right|^2 = \frac{1}{d}\,, \quad k = 0, \ldots, d-2\,, \tag{8}$$

where the state $|h(k)\rangle$ has components $h_j(k) \equiv H_{jk}$, $0 = 1, \ldots, d-1$. The completeness relation of the orthonormal basis $\{|h(k)\rangle, k = 0, \ldots, d-1\}$, implies that if a state $|v\rangle$ is

MU with respect to $(d-1)$ of its members, it is also MU with respect to the remaining one. Therefore, it is not necessary to include $k \equiv d-1$ in Eqs. (8).

For each given Hadamard matrix H, Eqs. (7) and (8) represent $2(d-1)$ simultaneous coupled quadratic equations for $2(d-1)$ real variables. Once we know *all* solutions of these equations, we know *all* vectors $|v\rangle$ MU with respect to the chosen pair of bases $\{I, H\}$. Analysing the set of solutions will reveal whether they form additional MU Hadamard matrices, or, equivalently, MU bases.

If Eqs. (7) and (8) were *linear*, one could apply Gaussian elimination to bring them into 'triangular' form. The resulting equations would have the same solutions as the original ones but the solutions could be obtained easily by successively solving for the unknowns.

The solutions of Eqs. (7) and (8) can be found using *Buchberger's algorithm* [25] which generalizes Gaussian elimination to *(nonlinear) multivariate polynomial* equations. In this approach, a set of polynomials $\mathcal{P} \equiv \{p_n(\mathbf{x}), n = 1, \ldots, N\}$ is transformed into a different set of polynomials $\mathcal{G} \equiv \{g_m(\mathbf{x}), m = 1, \ldots, M\}$ (usually with $M \neq N$) such that the equations $\mathcal{P} = 0$ and $\mathcal{G} = 0$ possess the *same* solutions; here $\mathcal{P} = 0$ is short for $p_n(\mathbf{x}) = 0, n = 1, \ldots, N$. Technically, one constructs a *Gröbner basis* $\mathcal{G}$ of the polynomials $\mathcal{P}$ which requires a choice of ordering the variables [25]. The transformed equations $\mathcal{G} = 0$ will be straightforward to solve due their 'triangular' form: one can find all possible values of a first unknown by solving for the zeros of a polynomial in a *single* variable; using each of these solutions will reduce one or more of the remaining equations to single-variable polynomials, allowing one to solve for a second unknown; etc. This process iteratively finds all solutions of $\mathcal{G} = 0$ and, therefore, all solutions of the original set of equations, $\mathcal{P} = 0$.

A Gröbner basis exists for any set of polynomial equations with a finite number of variables. However, the number of steps required to construct a Gröbner basis tends to be large even for polynomials of low degrees and a small number of unknowns. Thus, Buchberger's algorithm is most conveniently applied by means of algebraic software programs. We have used the implementation [27] of this algorithm suitable for the computational algebra system Maple [28] since we found it to be particularly fast for the system of equations under study.

Let us now illustrate how to construct all vectors MU with respect to a pair $\{I, H\}$ by solving the multivariate polynomial equations (7) and (8) using Buchberger's algorithm. We will consider two cases in dimensions $d = 3$ and $d = 6$, respectively, which have been solved before but they are suitable to illustrate the construction and to discuss some of its subleties.

3.2 Four MU bases in $\mathbb{C}^3$

In dimension $d = 3$, four MU bases are known to exist. We will now show how to construct two MU Hadamard matrices H_2 and H_3 given a pair $\{I, H\}$. The resulting three MU Hadamard matrices plus the identity are equivalent to a complete set of four MU bases in $\mathbb{C}^3$.

1. Choose a Hadamard In dimension three, all Hadamard matrices are known and there is only one choice for a dephased Hadamard matrix [21] given by the Fourier matrix,

$$F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} , \tag{9}$$

where $\omega = \exp(2\pi i/3)$ is a third root of unity.

2. List the constraints We want to find all states $|v\rangle \in \mathbb{C}^3$ which are MU with respect to the columns of the identity matrix I and the Fourier matrix F_3. Using the four real parameters x_1, x_2, y_1, and y_2 introduced in (6), the constraints (7) and (8) read explicitly

$$\begin{aligned}
1 - x_1^2 - y_1^2 &= 0\,,\\
1 - x_2^2 - y_2^2 &= 0\,,\\
x_1 + x_2 + x_1x_2 + y_1y_2 &= 0\,,\\
x_1 + x_2 - \sqrt{3}y_1 + \sqrt{3}y_2 + x_1x_2 - \sqrt{3}x_1y_2 + \sqrt{3}y_1x_2 + y_1y_2 &= 0\,. \qquad (10)
\end{aligned}$$

The solutions of these four coupled quadratic equations in four real variables, $\mathcal{P} = 0$, will tell us whether additional Hadamard matrices exist which are MU with respect to the Fourier matrix F_3.

3. Construct the solutions By running Buchberger's algorithm, we find the Gröbner basis $\mathcal{G}$ associated with the polynomials in Eqs. (10). Equating the resulting four polynomials $g_n(\mathbf{x}), n = 1, \ldots, 4$, to zero, gives rise to the equations

$$\begin{aligned}
3y_2 - 4y_2^3 &= 0\,,\\
1 - x_2 - 2y_2^2 &= 0\,,\\
1 + 2x_1 + 4y_1y_2 - 4y_2^2 &= 0\,,\\
3 - 4y_1^2 + 4y_1y_2 - 4y_2^2 &= 0\,. \qquad (11)
\end{aligned}$$

This set is 'triangular' in the sense that solutions can be found by iteratively determining the roots of polynomials for single variables only. The first equation has three solutions,

$$y_2 \in \{0\,, \pm\sqrt{3}/2\}\,; \qquad (12)$$

next, the second equation implies that

$$x_2 = \begin{cases} 0 & \text{if } y_2 = 0\,,\\ 2 & \text{if } y_2 = \pm\sqrt{3}/2\,; \end{cases} \qquad (13)$$

etc. Altogether, there are six solutions,

$$\begin{aligned}
\mathbf{s}_a &= \tfrac{1}{2}(-1, -1, \sqrt{3}, \sqrt{3})\,, & \mathbf{s}_b &= \tfrac{1}{2}(-1, 2, -\sqrt{3}, 0)\,,\\
\mathbf{s}_c &= \tfrac{1}{2}(2, -1, 0, -\sqrt{3})\,, & \mathbf{s}_d &= \tfrac{1}{2}(-1, -1, -\sqrt{3}, -\sqrt{3})\,,\\
\mathbf{s}_e &= \tfrac{1}{2}(2, -1, 0, \sqrt{3})\,, & \mathbf{s}_f &= \tfrac{1}{2}(-1, 2, \sqrt{3}, 0)\,,
\end{aligned}$$

defining $\mathbf{s} = (x_1, x_2, y_1, y_2)$.

Since the degrees of the polynomials $\mathcal{G}$ in Eqs. (11) does not exceed three, we are able to obtain analytic expressions for its solutions. This, however, is a fortunate coincidence due to the simplicity of the problem: in general, we will need to determine the roots of higher-order polynomials (cf. the example presented in Sec. 3.3) which requires numerical methods. The resulting complications will be discussed in Sec. 3.4.

4. List all MU vectors Upon substituting the solutions s_a to s_f into (6), one obtains six vectors

$$\begin{array}{c} v_a = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega \\ \omega \end{pmatrix}, \quad v_b = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega^2 \\ 1 \end{pmatrix}, \quad v_c = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ \omega^2 \end{pmatrix}, \\ v_d = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega^2 \\ \omega^2 \end{pmatrix}, \quad v_e = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ \omega \end{pmatrix}, \quad v_f = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega \\ 1 \end{pmatrix}, \end{array} \tag{14}$$

which are MU with respect to the columns of both the matrices I and F_3. No other vectors with this property exist, leaving us with $v_a, \dots, v_f$, as the only candidates for the columns of additional MU Hadamard matrices.

5. Analyse the vectors The six vectors in (14) allow us to define an additional Hadamard matrix only if any three of them are orthogonal; for a second Hadamard matrix the remaining three must be orthogonal among themselves *and* MU to the first three. Calculating the inner products between all pairs of the vectors v_a to v_f shows that they indeed fall into two groups with the required properties. Consequently, we have constructed a complete set of four MU bases in $\mathbb{C}^3$, corresponding to the set $\{I, F_3, H_2, H_3\}$ where the columns of the matrices H_2 and H_3 are given by $\{v_a, v_b, v_c\}$ and $\{v_d, v_e, v_f\}$, respectively.

We have also checked that the construction procedure works in dimensions $d = 2, 4, 5$ and $d = 7$ where it correctly produces complete sets of $d + 1$ MU bases. The matrices F_2, F_3 and F_5 are the *only* dephased Hadamard matrices in dimensions $d = 2, 3$ and $d = 5$, and there is only one way to construct complete MU bases from the vectors obtained. We have thus shown that the Heisenberg-Weyl construction of a complete set of MU bases is essentially *unique* in dimensions two, three and five.

3.3 Three MU bases in $\mathbb{C}^6$

In $d = 6$, the existence of seven MU bases is an open problem. We will search for all states $|v\rangle$ which are MU with respect to the identity I and the six-dimensional equivalent of F_3 given in (9), the dephased Fourier matrix

$$F_6 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 \\ 1 & \omega^2 & \omega^4 & 1 & \omega^2 & \omega^4 \\ 1 & \omega^3 & 1 & \omega^3 & 1 & \omega^3 \\ 1 & \omega^4 & \omega^2 & 1 & \omega^4 & \omega^2 \\ 1 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}, \tag{15}$$

with $\omega = \exp(\pi i/3)$ now being the sixth root of unity. This problem has been studied in the context of biunimodular sequences [24] and in relation to MU bases [7]. It is impossible to complement the pair $\{I, F_6\}$ by more than one Hadamard matrix MU with respect to F_6. Thus, the construction method of MU bases in prime-power dimensions, which is based on the Heisenberg-Weyl group, has no equivalent in the composite dimension $d = 6$. We will now reproduce this negative result.

Having chosen the first Hadamard matrix to be F_6, we can write down the conditions which the components of a state $|v\rangle$ must satisfy, $\mathcal{P} = 0$. After some algebraic operations detailed in Appendix B, one obtains the equations

$$\begin{aligned}
x_1 + x_5 + x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + y_1y_2 + y_2y_3 + y_3y_4 + y_4y_5 &= 0\,, \\
y_1 - y_5 + x_1y_2 - x_2y_1 + x_2y_3 - x_3y_2 + x_3y_4 - x_4y_3 + x_4y_5 - x_5y_4 &= 0\,, \\
x_3 + x_1x_4 + x_2x_5 + y_1y_4 + y_2y_5 &= 0\,, \\
x_2 + x_4 + x_1x_3 + x_1x_5 + x_2x_4 + x_3x_5 + y_1y_3 + y_1y_5 + y_2y_4 + y_3y_5 &= 0\,, \\
y_2 - y_4 + x_1y_3 - x_1y_5 + x_2y_4 - x_3y_1 + x_3y_5 - x_4y_2 + x_5y_1 - x_5y_3 &= 0\,, \qquad (16)
\end{aligned}$$

which must be supplemented by the five conditions (7) arising for $d = 6$.

We need to find all solutions of these ten coupled equations $\mathcal{P} = 0$ which are quadratic in ten real variables. The Gröbner basis $\mathcal{G}$ associated with the set $\mathcal{P}$ consists of 36 polynomials of considerably higher degrees. We reproduce only the first one of the new set of equations, $\mathcal{G} = 0$,

$$\begin{aligned}
&- 245025\, y_5 + 4318758\, {y_5}^3 - 28135161\, {y_5}^5 + 89685000\, {y_5}^7 - 158611892\, {y_5}^9 \\
&\quad +177275680\, {y_5}^{11} - 150745472\, {y_5}^{13} + 104333824\, {y_5}^{15} - 43667456\, {y_5}^{17} \qquad (17) \\
&\qquad +2351104\, {y_5}^{19} + 4882432\, {y_5}^{21} - 1703936\, {y_5}^{23} + 262144\, {y_5}^{25} \;=\; 0\,,
\end{aligned}$$

being of order 25 in the single variable y_5. This equation admits 15 real solutions,

$$y_5 \in \{0, \pm 1, \pm\frac{1}{2}, \pm\frac{\sqrt{3}}{2}, \pm\frac{1}{2}(1+\sqrt{3}), \pm\frac{1}{2}(1-\sqrt{3}), \pm 0.988940\ldots, \pm 0.622915\ldots\}\,, \qquad (18)$$

the last four of which we only find numerically. Due to the triangular structure resulting from Buchberger's algorithm, there will be equations (at least one) containing only y_5 and one other single variable. For each value of y_5 taken from (18), they reduce to single-variable polynomials the roots of which can be determined to desired numerical accuracy; etc. Keeping track of all possible branches we obtain 48 vectors that satisfy the Eqs. (16).

Having determined the candidates for columns of MU Hadamard matrices, we calculate the inner products among all pairs of the 48 vectors. It turns out that there are 16 different ways to group them into bases of $\mathbb{C}^6$. However, no two of these bases are MU with respect to each other. Consequently, it is possible to form at most 16 different *triples* of MU bases which include F_6, but it also follows that the Fourier matrix F_6 (or any other unitarily equivalent element of the Heisenberg-Weyl group [7]) *cannot* be part of three MU Hadamard matrices giving rise to four MU bases.

There are, however, many choices other than $H = F_6$ for a dephased Hadamard matrix in dimension six. In Sec. 4, we will repeat the calculations just presented for a large sample of currently known Hadamard matrices. Before doing so, we will discuss the fact that we are able to construct the desired vectors only approximately. In the following section we show that sufficiently high numerical accuracy allows us to draw *rigorous* conclusions about the properties of the exact vectors.

3.4 The Impact of Numerical Approximations

The previous section illustrated that the problem of finding MU vectors with respect to the identity I and a given Hadamard matrix H can be reduced to successively solving for the roots of polynomials of a single variable. These roots, however, can only be found approximately. Does the approximation prevent us from drawing rigorous conclusions about the properties of the MU vectors we construct? We will argue now that it remains possible to find upper bounds on the number of MU vectors with the desired properties.

Consider the system of polynomials $\mathcal{P} = \{p_n(\mathbf{x}), n = 1, \ldots, 10\}$ in the variables $\mathbf{x} \in\mathbb{R}^{10}$ resulting from some chosen Hadamard matrix H, and calculate a Gröbner basis, $\mathcal{G} = \{g_m(\mathbf{x}), m = 1, \ldots, M\}$. The roots of the equations $\mathcal{P} = 0$ and $\mathcal{G} = 0$ are identical by construction. Since $\mathcal{G} = 0$ corresponds to a 'triangular' set, its roots can be found iteratively but, in general, no closed form will exist. The implementation of Buchberger's algorithm which we have chosen finds these roots with user-specified accuracy, relying on the theory presented in [29].

Now suppose that $\mathcal{G} = 0$ has two roots $\mathbf{s}_a$ and $\mathbf{s}_b$, to which we have found approximations, $\mathbf{s}_A$ and $\mathbf{s}_B$. The associated states $|v_A\rangle$ and $|v_B\rangle$ will be close to the exact states, $|v_a\rangle$ and $|v_b\rangle$. It is convenient to think of the vectors $|v_A\rangle$ and $|v_B\rangle$ as lying inside a ball centered at the exact states, the radius of the ball being determined by the accuracy of the approximate roots. If the inner product of the exact states $|v_a\rangle$ and $|v_b\rangle$ has a non-zero modulus, $\delta > 0$, then they are *not* orthogonal. We can detect this by calculating the inner product of the *approximate* states $|v_A\rangle$ and $|v_B\rangle$. If we ensure that the error of the approximate inner product is *small* compared to the number δ, a non-zero lower bound for the exact scalar product can be obtained, and it signals non-orthogonality of the exact states. A similar argument allows us to exclude that two states are MU with respect to each other.

We determine the roots of $\mathcal{G} = 0$ to 20 significant digits which proves sufficient to put relevant limits on the properties of the vectors constructed in dimension six. The results presented in the next section thus provide strict limits on complementing pairs of bases $\{I, H\}$ by MU vectors.

4 Constructing MU Bases in Dimension Six

We are now in a position to present the main results of this paper. We will consider one Hadamard matrix H at a time constructing all additional Hadamard matrices MU with respect to the chosen one. Picking matrices both systematically and randomly, we will find that not a single one is compatible with the existence of four MU bases.

More specifically, we will calculate three quantities for each chosen Hadamard matrix H: the number N_v which equals the number of vectors MU with the pair $\{I, H\}$; the number N_t providing an upper bound of the number of different triples of MU bases $\{I, H, H'\}$; and the value of N_p, an upper bound of the number of constellations $\{5, 5, 1, 1\}$ (or $\{I, H, |v_a\rangle, |v_b\rangle\}$), i.e. we report how many *pairs* of MU vectors can be found among those already MU with respect to I and H.

4.1 Special Hadamard Matrices

To begin, we consider Hadamard matrices which are either isolated or special in the sense that they belong to different families simultaneously. All these matrices are to be found on the symmetry axis of Fig. (1): the Fourier matrix $F_6 \equiv F(0,0)$ being invariant under transposition, the Diţă matrix $D_0 \equiv D(0)$ which is both symmetric and Hermitean, the circulant matrix C, and the Spectral matrix S.

The first row of Table 1 completes the findings of Sec. 3.3 obtained for the *Fourier* matrix F_6: there are $N_v = 48$ vectors MU with respect to both I and F_6, forming $N_p = 144$ MU pairs. The 48 vectors can be arranged in $N_t = 16$ different ways to form a second Hadamard matrix H' which is MU with respect to F_6. However, no two of these 16 Hadamard matrices are MU between themselves, limiting the number of MU bases containing F_6 to three.

A similar analysis for the *Diţă* matrix D_0 reveals that there are 120 vectors MU to its columns and those of the identity, 60 of which form ten bases but none of these are MU with respect to each other. Whilst ten triples of MU bases exist, sets of four MU bases which include D_0 do *not* exist since $N_p = 0$.

Interestingly, the components of the 120 vectors have phases ϕ which take values in a small set only,

$$\phi_D \equiv \{0, \pi, \pm\pi/12, \ldots, \pm 11\pi/12, \pm\alpha\}\,, \tag{19}$$

where $\tan\alpha = 2$. This result[1] agrees with the one obtained by Bengtsson et al. [13] (note, however, that the descriptions given in the last two entries of the list in their Sec. 7 must be swapped). What is more, our approach *proves* that these authors have been able to identify *all* vectors MU with the pair $\{I, D_0\}$ by means of their ansatz for the form of MU vectors. In fact, the values of N_t and N_p in Table 1 given for D_0 are *exact*, not upper bounds, since the phases of the MU states $|v\rangle$ are known in closed form.

The *circulant* matrix C permits only 38 MU vectors, none of which are MU with respect to each other, $N_p = 0$, and none of their subsets forms a MU basis as $N_t = 0$.

The *spectral* matrix S is the only known *isolated* Hadamard matrix. We find 90 MU vectors but not a single sextuple of orthonormal ones among them while there are 1,115 pairs of MU vectors. Thus, the pair $\{I, S\}$ cannot even be extended to a triple of MU bases.

4.2 Affine Families

Table 2 collects the properties of vectors MU with respect to the pair $\{I, H\}$ where H is an affine Hadamard matrix, i.e. taken either from the one-parameter set discovered by Diţă or from the two-parameter Fourier or Szöllősi families. Again, we have sampled the relevant parameter spaces both systematically and randomly.

The set of *Diţă* matrices $D(x)$ depends on a single continuous parameter x, with $|x| \leq 1/8$. We have sampled the interval in steps of size $1/144$ making sure that the resulting grid of points include the 24th roots of unity which play an important role for D_0, so

$$\Gamma_D = \{a/144 : a = \pm 1, \pm 2 \ldots, \pm 18\}\,; \tag{20}$$

note that the matrix D_0 has been left out. The number of vectors MU with the pair $\{I, D(x)\}$ depends on the *value* of the parameter x: the Diţă matrices $D(x)$ on the grid Γ_D allow for either 72 or 120 MU vectors which can be grouped into into four additional Hadamard matrices. Since they are not MU between themselves, there are at most three MU bases containing any of these Diţă matrices. No MU pairs exist, $N_p = 0$—except for two small intervals near $x = \pm 1/8$ where either 24 or 48 pairs can be found.

The results obtained from *randomly* picking points in the fundamental interval are in line with the observations made for grid points. Fig. 2 shows N_v, the number of vectors MU with respect to the pair $\{I, D(x)\}$ for all 536 values of the parameter x which we have considered. The function $N_v(x)$ appears to be symmetric about $x = 0$ and piecewise constant, dropping from 120 for small values of x to 72 at $x \simeq \pm 0.0177$, and to 48 at the end points of the interval, $x = \pm 1/8$. We are not able to explain why $N_v(x) = N_v(-x)$ should hold although we do know how to derive a similar property

[1] Such a restricted set of phases also occurs for other members of the Diţă family. For example, all 48 vectors MU with the pair $\{I, D(1/8)\}$ have phases limited to the set $\phi_D \cup \{\pm\beta\}$ where $\tan\beta = 3$.

for the families of symmetric and Hermitean Hadamard matrices (cf. Sec. 4.3). The values for N_p and N_v can be found in Table 2.

The results for members of *Fourier* family $F(\mathbf{x})$ are qualitatively similar. Picking values of $\mathbf{x} \equiv (x_1, x_2)$ either randomly in the fundamental area or from the two-dimensional grid

$$\Gamma_F = \{(a,b)/144 : a = 1, 2, \ldots, 24,\ b = 0, 1, \ldots, 12,\ a \geq 2b\}\,, \tag{21}$$

invariably leads to 48 vectors being MU to the columns of the pair $\{I, F(\mathbf{x})\}$. There are eight different ways to form additional Hadamard matrices for each point considered except for the matrix $F(1/6, 0)$ with an upper bound of 70 triples. The number of pairs varies, $N_p \in \{0, 6, 12, 24\}$, without any recognizable systematic behaviour. It is important to realize that Grassl's result—the construction of complete sets of MU bases cannot be based on the Heisenberg-Weyl group in dimension $d = 6$—also holds for the 2,168 other Fourier matrices we have considered.

The situation is similar when turning to the family of *transposed Fourier* matrices, $F^T(\mathbf{x})$. The number N_v equals 48 throughout and a second Hadamard matrix can be formed in eight different ways, and only matrix $F^T(1/6, 0)$ allows for 70 different triples, eight being the norm. The number N_p runs through the same values as in the Fourier family.

4.3 Non-Affine Families

The equations $\mathcal{P} = 0$ encoding MU vectors for the symmetric $M(t)$, Hermitian $B(\theta)$ and Szöllősi $X(a, b)$ families turn out to be more challenging from a computational perspective: the program has, in general, not been able to construct the associated Gröbner bases $\mathcal{G}$. The problem is not a fundamental one—the desired Gröbner bases do exist but it appears that their construction requires more memory than the 16GB available to us.

We suspect that the difficulties are due to the fact that, for non-affine matrices, the coefficients of the polynomials $\mathcal{P} = 0$ are no longer equal to fractions or simple roots of integers. When approximating the coefficients in question by fractions we obtain different sets of polynomials, $\tilde{\mathcal{P}}$, and, interestingly, the program indeed succeeds in constructing the corresponding Gröbner bases, $\tilde{\mathcal{G}}$, outputting (approximate) MU vectors $|\tilde{v}\rangle$. Being continuous functions of the coefficients, the approximate vectors will resemble the exact ones, $|\tilde{v}\rangle \simeq |v\rangle$. However, the *number* of MU vectors may change discontinuously if $\tilde{\mathcal{P}} = 0$ is considered instead of $\mathcal{P} = 0$, similar to the discontinuous change in the number N_v for the family $D(x)$ near $x \simeq 0.0177$, shown in Fig. 2. In other words, it could happen that we 'lose' some solutions due to a geometric instability as a consequence of modifying the defining polynomials.

To determine the impact of such an approximation, we have studied how the number N_v of MU vectors changes in a case for which we know rigorous bounds. We retain only five significant digits of the coefficients in the equations $\mathcal{P} = 0$ associated with the family $D(t)$ and solve for the approximate MU vectors. The inset of Fig. 2 shows that the plateaus of 120 and 72 MU vectors continue to be well-defined away from the discontinuity at $x \simeq 0.0177$ while the values of N_v fluctuate close to it. Assuming that a qualitatively similar behaviour will also occur for symmetric and Hermitean matrices, we now simplify the equations $\mathcal{P} = 0$ associated with them. Retaining only five significant digits of the coefficients in these equations, we determine the number of MU vectors $|\tilde{v}\rangle$ and their inner products.

Fig. 3 shows that the family of *symmetric* Hadamard matrices $M(t)$ comes with 48 MU vectors $|\tilde{v}\rangle$ close to the point $t = 0$, while there are 120 near $t = 1/4$. These numbers are consistent with the rigorous bounds obtained in Sec. 4.2 if we recall that $M(0) = M(1/2) \approx F(0,0)$ and $M(1/4) \approx D(0)$ holds (cf. Fig. 1). Across the entire parameter range, the number of MU vectors is a piecewise constant function symmetric about $x = 1/4$, with distinct plateaus of $48, 52, 120$ and possibly 96 MU vectors. We suspect that the other values of N_v near the discontinuities are spurious. An analysis of the scalar products among the approximate MU vectors shows that they cannot be arranged into a single additional basis. Table 3 lists the results obtained for both a regular grid

$$\Gamma_M = \{a/144 : a = 1, 2, \ldots, 71; a \neq 36\}\,; \tag{22}$$

and 300 randomly selected points in the fundamental interval; the reason for leaving out $a = 36$ is the equivalence $M(1/4) \approx D_0$ just mentioned. We are confident that a more rigorous approach will confirm the absence of triples of MU bases containing a single symmetric Hadamard matrix $M(t)$.

Further support for the reliability of the approximation follows from the overall symmetry of N_v in the fundamental interval. To show that N_v must be an even function of the parameter t, let us make explicit the transformation of a symmetric matrix $M(t)$ under complex conjugation,

$$M(-t) = PM^*(t)P\,, \tag{23}$$

where P is a permutation matrix. Now consider a vector $|v\rangle$ which is MU to the columns $m(t)$ of the matrix $M(t)$; then

$$|\langle m(t)|v\rangle|^2 = |\langle m(t)|v\rangle^*|^2 = |\langle m^*(t)|v^*\rangle|^2 = |\langle m(-t)P|v^*\rangle|^2\ , \tag{24}$$

and, therefore, $P|v^*\rangle$ is MU with respect to each column of $M(-t)$.

Thus, the vectors MU to $M(-t)$ are the complex conjugates of those MU to $M(t)$ with entries permuted by P. Hence the number of vectors, N_v, is an *even* function of t and the vectors MU to $M(t)$ have the same properties as those MU to $M(-t)$. Although we did not pay any attention to the existence of this exact symmetries when introducing the approximations, the results obtained do respect it.

The results obtained for *Hermitean* Hadamard matrices $B(\theta)$, shown in Fig. 3, are similar to those of the symmetric family. The observed plateaus blend in with the rigorous bounds found for $N_v = 120$ and $N_v = 38$ due to the equivalences $B(1/2) \approx D(0)$ and $B(\theta_0) \approx C$ (cf. Table 1). We consider the plateaus at 56, 58, 60, 72, 84 and 108 to be genuine while spurious values for N_v proliferate near their ends, where N_v is likely to vary discontinuously. Once more, Table 3 reveals that neither regularly spaced points on the grid

$$\Gamma_B = \{a/144 : a = 55, 56, \ldots, 89; a \neq 72\}\,; \tag{25}$$

nor randomly chosen values of θ define Hadamard matrices $B(\theta)$ which would allow the construction of more than three MU bases. As for the symmetric family, we are able to explain the symmetry of N_v: members of the Hermitean family satisfy the relation $B(1-\theta) = B^*(\theta)$ which implies that the number N_v of MU vectors (and their properties) will not change upon a reflection about the point $\theta = 1/2$.

Finally, let us consider the *Szöllősi* family, the non-affine two-parameter set of Hadamard matrices $X(a,b)$. Fig. 4 shows the values of N_v for randomly chosen parameters on two cuts through parameter space, namely along the line

$$\Lambda = \{(a,b) : \arg(a + ib) = \pi/6\} \tag{26}$$

which connects $X(0,0) \approx F(1/6,0)$ to the circulant matrix C, and the randomly chosen line

$$\Lambda' = \{(a,b) : \arg(a+ib) = 0.3510\} \tag{27}$$

connecting $X(0,0)$ to $B(\theta')$, a Hermitean Hadamard matrix on the boundary. The values of N_v at the end points of the lines are, in both cases, consistent with results obtained above for $F(1/6,0)$, C, and $B(\theta')$; broadly speaking, the number of solutions again represents a step function. However, the plateaus at $48, 52, 54, 56, 58$ and 60 in Fig. 4 (b) show considerable overlap: the effect of approximating the coefficients in the relevant polynomials is even more pronounced for the Szöllősi family than for the other non-affine families. The results for the 300 randomly chosen parameter values sampling the two-dimensional parameter space resemble those of the symmetric and Hermitean families: we find $48 \leq N_v \leq 120$ throughout, and none of the selected Hadamard matrices allow for a triple of MU bases. Preliminary calculations show that the properties of the new family of transposed Szöllősi matrices $X^T(a,b)$ are similar to those of the set $X(a,b)$.

While not being exact, the results for the symmetric, Hermitean and Szöllősi families provide bounds on the number of MU bases which can be constructed from their members. Except in some special cases with higher symmetry, it is not possible to even find a third MU basis. We consider it unlikely that the approximation made would systematically suppress other MU vectors with properties invalidating this conclusion.

5 Summary and Conclusions

We have searched for MU bases related to pairs $\{I, H\}$ where I is the unit matrix and H runs through a discrete subset of known (6 × 6) complex Hadamard matrices. Using Buchberger's algorithm, we have obtained upper bounds on the number of MU bases; the bounds are *rigorous* in many cases and *approximate* in others. Each of the 5,980 calculations required between 4 and 16 GB of memory and, altogether, would have lasted approximately 29,000 hours on a single 2.2 GHz processor.

Each point in Fig. 5 represents one of the Hadamard matrices H we have been investigating. We find that for any set of *three* MU bases, $\{I, H, H'\}$, at least one of the MU Hadamard matrices H and H' must either be a member of the Diţă or Fourier families. None of the remaining Hadamard matrices shown in Fig. 5 can be a member of a triple of MU bases. Further, any set of four (seven) MU bases in dimension six would require three (six) MU Hadamard matrices different from the ones shown in Fig. 5. This clearly conforms with the numerically obtained evidence that no four MU basis do exist [12].

There is one caveat that we must make regarding the results of the non-affine families. In general, the program was unable to construct the associated Gröbner bases for the symmetric, Hermitian and Szöllősi families. For these Hadamard matrices, we are unable to guarantee that we have found *all* MU vectors, however, we consider it unlikely that the approximation made would systematically suppress the missing vectors.

It has been suggested that the set of Hadamard matrices in $\mathbb{C}^6$ depend on four parameters [13], a conjecture which recently gained some numerical support [30]. It remains difficult to draw general conclusions about the number of MU bases in dimension $d = 6$. However, we would like to point out that the approach presented here is *future-proof*: it will work for any Hadamard matrix—including currently unknown ones.

In summary, we have shown that the construction of more than three MU bases in $\mathbb{C}^6$ is not possible in a considerable number of instances. The results add significant weight to the conjecture that a complete set of seven MU bases does not exist in dimension six. It becomes ever more likely that only prime-power dimensions allow for optimal state reconstruction.

Acknowledgments

The calculations have been performed on the White Rose Grid provided by the Universities of Leeds, Sheffield and York; we thank A. Turner and M. Hewitt, who run its node at York, for their help in using the grid.

References

[1] I. D. Ivanović, J. Phys. A **14**, 3241 (1981)

[2] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989)

[3] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin: Phys. Rev. Lett. **88**, 127902 (2002)

[4] Y. Aharonov and B. G. Englert, Z. Naturforsch. A: Phys. Sci. **56a**, 16 (2001)

[5] M. Planat, H. Rosu, and S. Perrine, Found. Phys. **36**, 1662 (2006)

[6] P.O. Boykin, M. Sitharam, P.H Tiep and P. Wocjan, Quantum Inf. Comp. **7**, 371 (2007)

[7] M. Grassl, *On SIC-POVMs and MUBs in Dimension 6*, in: *Proc. ERATO Conference on Quantum Information Science (EQUIS 2004)*, J. Gruska (ed.)

[8] A. Klappenecker and M. Roetteler, *Lecture Notes in Computer Science*, Vol. 2948, 262-266 (2004)

[9] P. Wocjan and T. Beth, Quantum Inf. Comput. **5**, 93-101 (2005)

[10] C. Archer, J. Math. Phys. **46**, 022106 (2005)

[11] P. Butterley and W. Hall, Phys. Lett. A **369**, 5 (2007)

[12] S. Brierley and S. Weigert, Phys. Rev. A **78**, 042312 (2008)

[13] I. Bengtsson, W. Bruzda, Å. Ericsson, J-Å. Larsson, W. Tadej and K. Życzkowski, J. Math. Phys. **48**, 052106 (2007)

[14] W. Tadej and K. Życzkowski, Open Sys. Info. Dynamics **13**, 133 (2006)

[15] *On-line catalgue of known Hadamard matrices* maintained by W. Tadej and K. Życzkowski at `http://chaos.if.uj.edu.pl/~karol/hadamard/`

[16] G. E. Moorhouse, *The 2-Transitive Complex Hadamard Matrices*, `http://www.uwyo.edu/moorhouse/pub` (2001)

[17] T. Tao, Math. Res. Lett. **11**, 251 (2004)

[18] P. Diţă, J. Phys. A **37**, 5355 (2004)

[19] M. Matolcsi and F Szöllősi, *Towards a Classification of* 6×6 *Complex Hadamard Matrices*, arXiv:math/0702043 (2006)

[20] K. Beauchamp, R. Nicoara, *Orthogonal maximal abelian *-subalgebras of the 6x6 matrices*, arXiv:math/0609076 (2006)

[21] U. Haagerup, *Orthogonal abelian *-subalgebras of the* $n \times n$ *matrices and cyclic* n*-roots*, in: *Proc. Operator Algebras and Quantum Field Theory (Rome 1996)*, S. Doplicher (ed.)

[22] F. Szöllősi, *A Two-Parameter Family of Hadamard Matrices of Order 6 Induced by Hypocycloids*, arXiv:0811.3930v1 (2008)

[23] I. Bengtsson, private communication

[24] G. Björck and B. Saffari, C. R. Acad Sci. Paris Sér. I **320**, 319 (1995)

[25] B. Buchberger, *An Algorithm for Finding the Basis Elements of the Residue Class Ring of a Zero Dimensional Polynomial Ideal.* Ph.D. Dissertation, University of Innsbruck (1965) (English translation by M. Abramson in J. Symb. Comp. **41**, 471 (2006))

[26] B. Buchberger, *Gröbner Bases and Applications* in *LMS Lecture note series, 251* (1998), B. Buchberger and F. Winkler (eds.)

[27] SALSA: SOLVERS FOR ALGEBRAIC SYSTEMS AND APPLICATIONS; software available from http://fgbrs.lip6.fr/salsa/

[28] Maple 11, Waterloo Maple Inc. Waterloo, Ontario, Canada

[29] F. Rouillier, Applic. Alg. in Eng. Comm. Comp. **9**, 433 (1999)

[30] A. J. Skinner, V. A. Newell, R. Sanchez. *Unbiased bases (Hadamards) for 6-level systems: Four ways from Fourier*, arXiv:0810.1761 (2008)

Figures

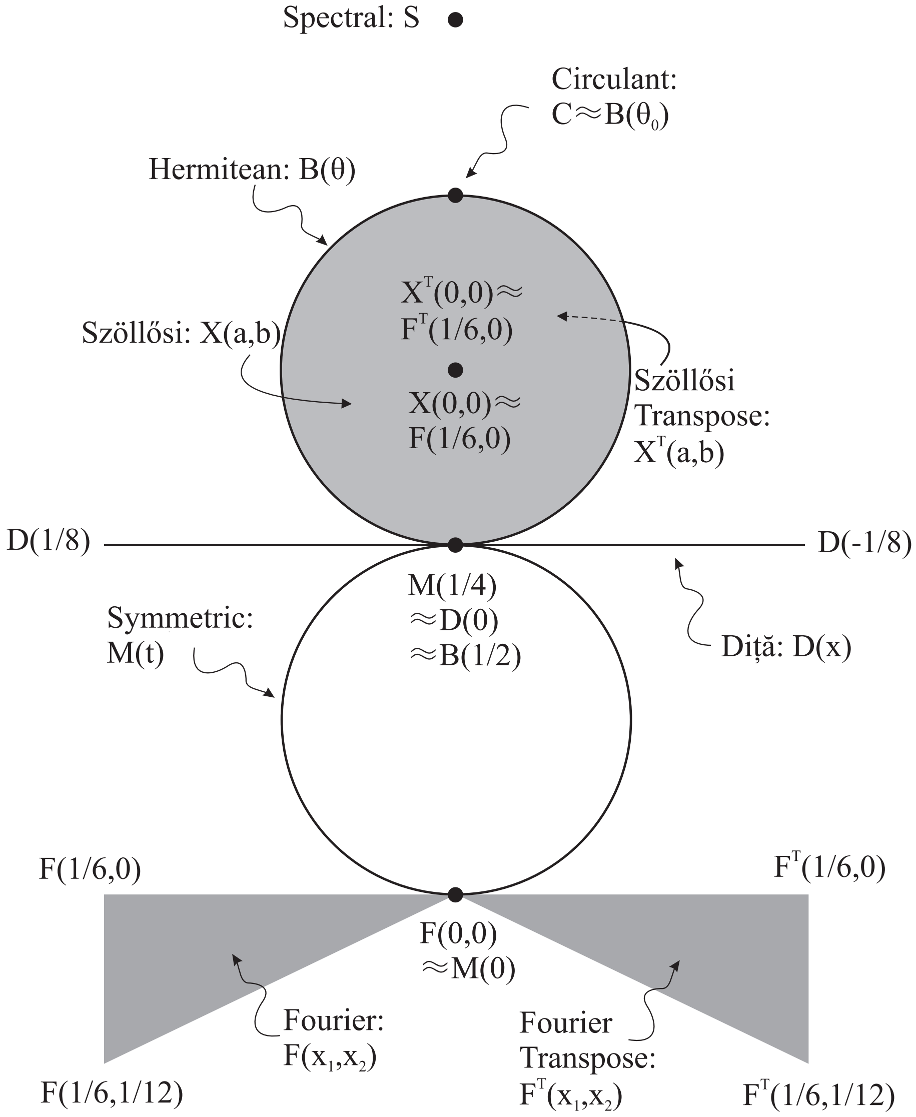

Figure 1: The set of known Hadamard matrices in dimension six consists of *special* Hadamard matrices $F(0,0) \equiv F_6$, $D(0) \equiv D_0$, C, and S, located on the vertical symmetry axis; of the *affine* families $D(x)$, $F(\mathbf{x})$, and $F^T(\mathbf{x})$; and of the *non-affine* families $M(t)$, $B(\theta)$, $X(a,b)$, and $X^T(a,b)$ (see Appendix A for definitions). Note that the sets $X(a,b)$ and $X^T(a,b)$ cover the interior of the upper circle twice.

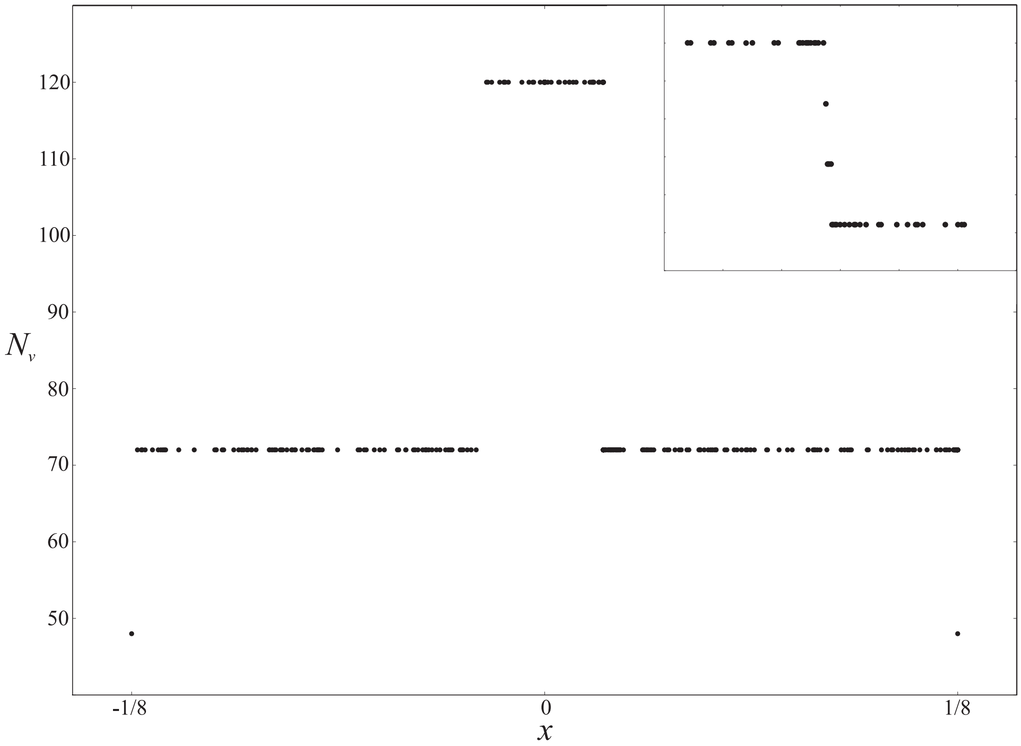

Figure 2: The number N_v of vectors $|v\rangle$ which are MU with respect to the columns of the identity I and Diţă matrices $D(x)$; the parameter x assumes 72 parameter values $x \in \Gamma_D$, and 500 randomly chosen ones in the fundamental interval $[-1/8, 1/8]$ of the parameter x. The inset illustrates the impact on N_v near the discontinuity $x \simeq 0.0177$ if an *approximate* set of equations is used (cf. Sec. 4.3).

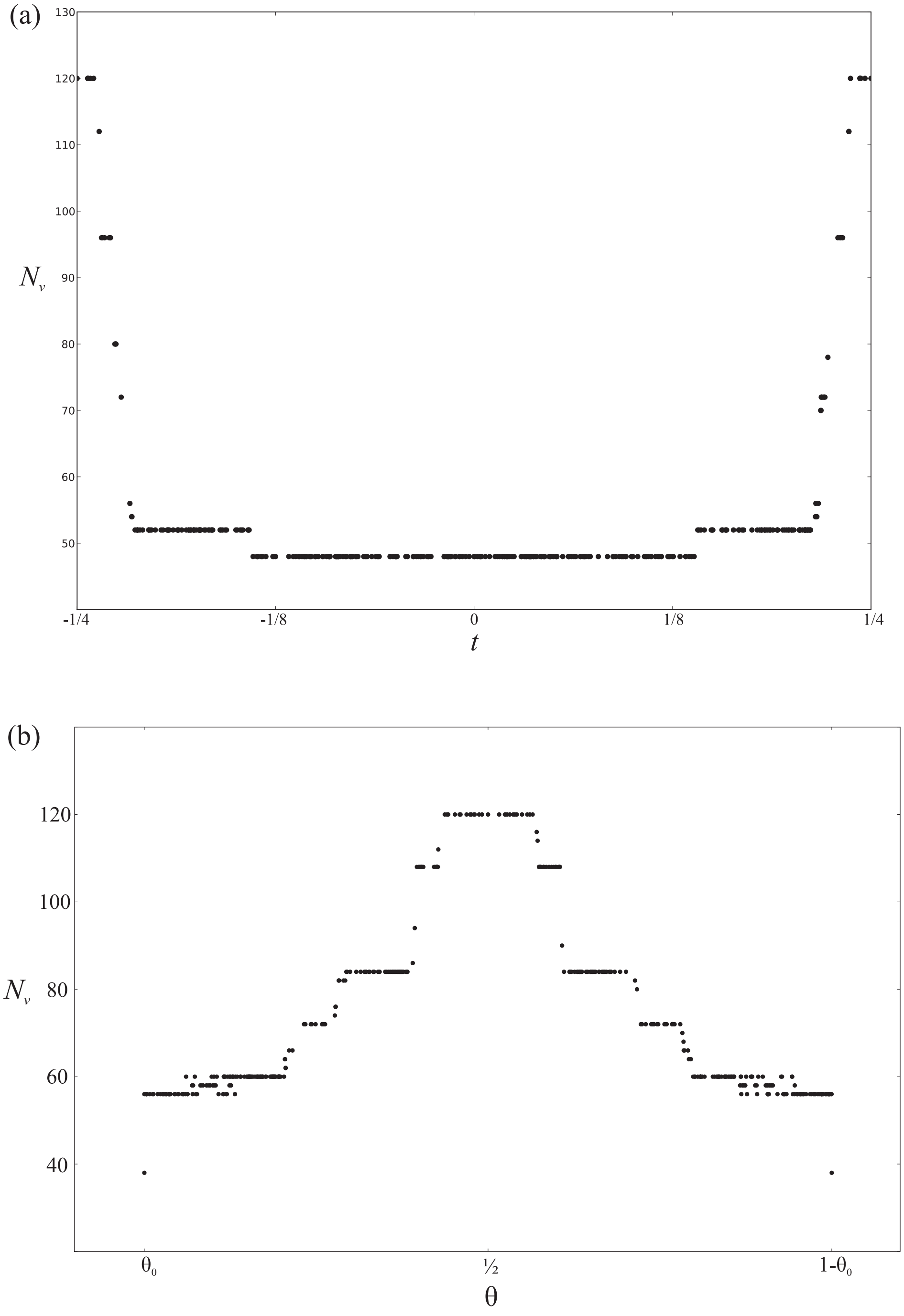

Figure 3: The number N_v of vectors $|v\rangle$ which are MU with respect to the columns of the identity I and (a) symmetric Hadamard matrices $M(t)$; the parameter t assumes 60 parameter values $t \in \Gamma_M$, and 300 randomly chosen ones in the fundamental interval $[0, 1/2]$, and of (b) Hermitean matrices $B(\theta)$; the parameter θ assumes 34 parameter values $\theta \in \Gamma_B$, and 300 randomly chosen ones in the fundamental interval $[\theta_0, 1-\theta_0]$. The phase θ_0 has been defined in equation (35).

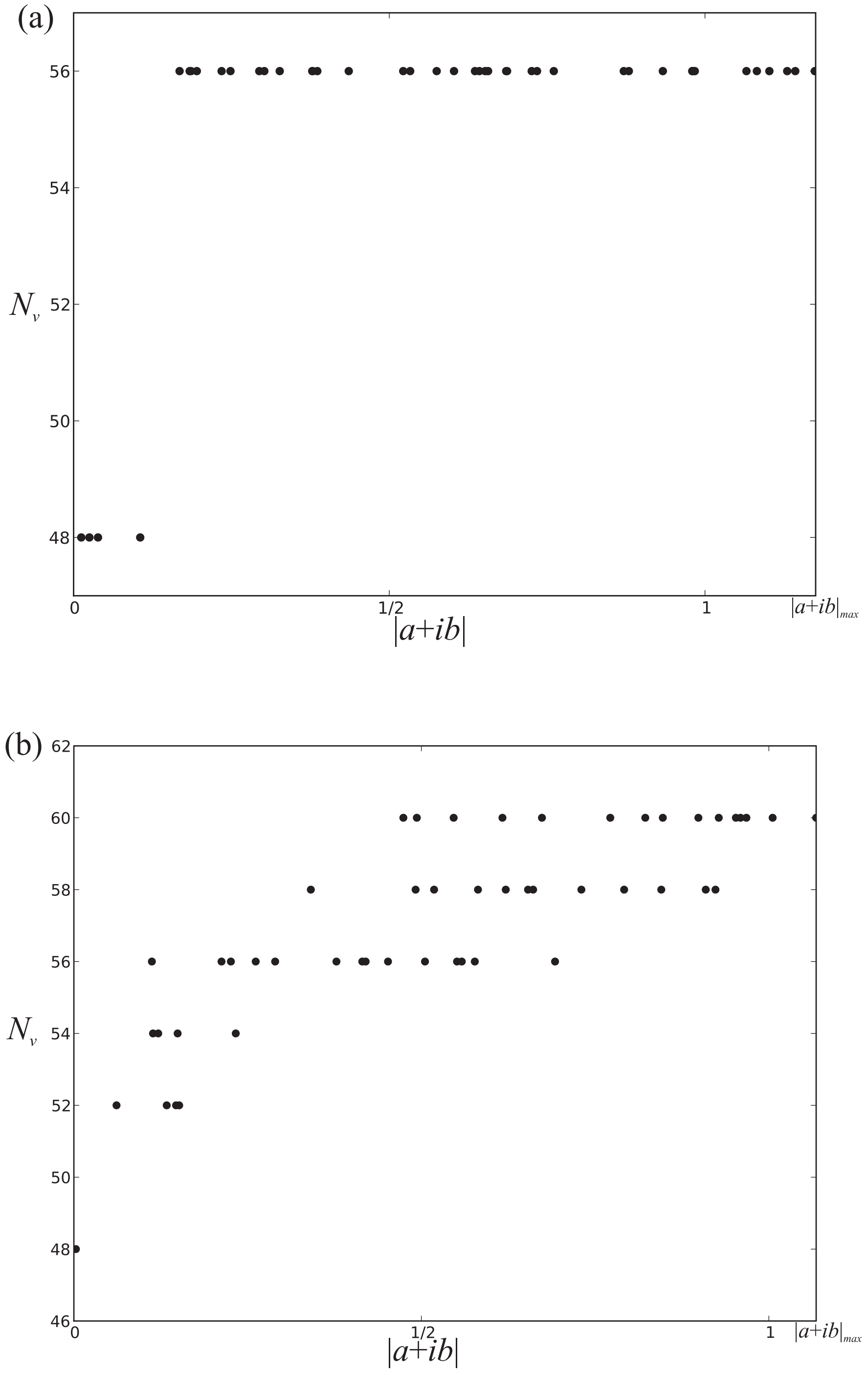

Figure 4: The number N_v of vectors $|v\rangle$ which are MU with respect to the columns of the identity I and Szöllősi Hadamard matrices $X(a,b)$ for 50 randomly chosen parameter values (a) on the line Λ connecting $F(1/6,0)$ to C, and (b) on the line Λ' connecting $F(1/6,0)$ to $B(\theta')$; in both figures, the maximum modulus $|a+ib|$ is defined by Eq. (41).

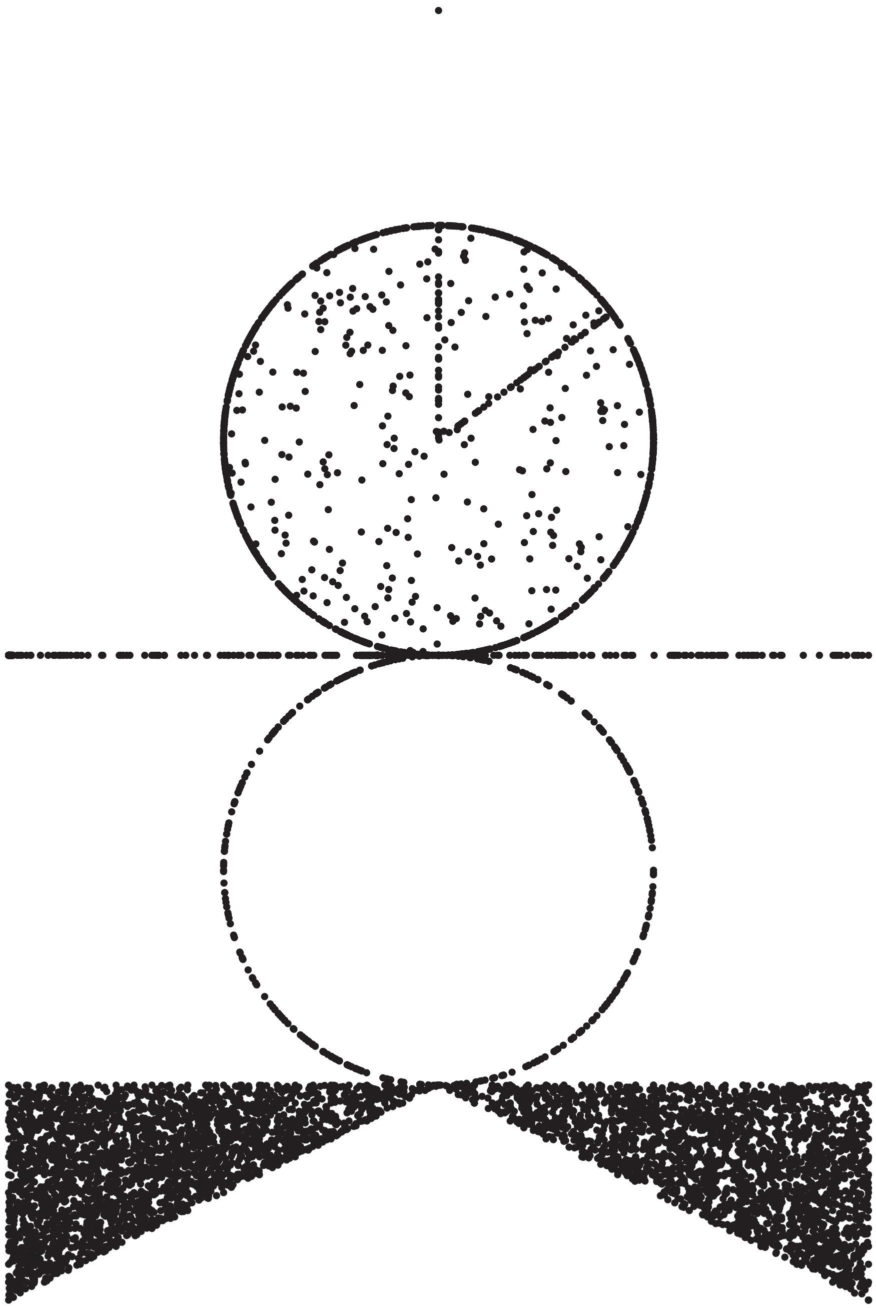

Figure 5: The set of all Hadamard matrices H which have been considered (cf. Fig. 1 and Tables 1-3): given $\{I, H\}$, only the Fourier matrices $F(\mathbf{x})$, the (transposed) Fourier matrices $F^T(\mathbf{x})$, and the Diţă matrices $D(x)$ allow for the construction of a second MU Hadamard matrix and, thus, a third MU basis; in all other cases not even three MU bases exist.

Tables

H	N_v	N_t	N_p
F_6	48	16	144
D_0	120	10	0
C	38	0	0
S	90	0	1115

Table 1: The number of MU vectors and their properties for *special* Hadamard matrices: there are N_v vectors being MU with respect to the pair of matrices $\{I, H\}$; these vectors form N_t additional Hadamard matrices (i.e. there are N_t different *triples* of MU bases) and N_p is the number of *pairs* of vectors MU to themselves and to $\{I, H\}$.

H	$\mathbf{x}$	#($\mathbf{x}$)	N_v	N_t	N_p
$D(x)$	Γ_D	36	72/120	4	0/24/48
	random	500	72/120	4	0/24/48
$F(\mathbf{x})$	Γ_F	168	48	8/70	0/6/12/24
	random	2,000	48	8	0/6/12/24
$F^T(\mathbf{x})$	Γ_F	168	48	8/70	0/6/12/24
	random	2,000	48	8	0/6/12/24

Table 2: The number of MU vectors and their properties for *affine* Hadamard matrices: the second column indicates which values have been chosen for the parameters $\mathbf{x}$; the grids of points Γ_M and Γ_F are defined in Eqs. (20) and (21), respectively; the third column displays the number of Hadamard matrices considered in a sample; N_v, N_t and N_p are defined as in Table 1 and vary as a function of the parameter values (cf. Sec. 4.2).

H	$\mathbf{x}$	#($\mathbf{x}$)	N_v	N_t	N_p
$M(t)$	Γ_M	70	48-120	0	0-18
	random	300	48-120	0	0-18
$B(\theta)$	Γ_B	34	56-120	0	0-14
	random	300	56-120	0	0-14
$X(a, b)$	Λ	50	48/56	0	0-10
	Λ'	50	48-60	0	0-10
	random	300	48-120	0	0-10

Table 3: The number of MU vectors and their properties for *non-affine* Hadamard matrices: the grids Γ_M and Γ_B are defined in Eqs. (22) and (25), respectively; see Eqs. (26) and (27) for the definition of the lines Λ and Λ'; other notation as in Table 2; preliminary results for the family $X^T(a, b)$ resemble those obtained for $X(a, b)$.

A Known complex Hadamards matrices in dimension six

This Appendix lists the currently known complex Hadamard matrices for easy reference and to establish notation. For more details the reader is referred to [13] and to the online catalogue [15].

A.1 Special Hadamard matrices

The *Fourier matrix* F_6 has been introduced in Eq. (15); it is contained in both the Fourier family $F(\mathbf{x})$ and the transposed Fourier family $F^T(\mathbf{x})$ for $\mathbf{x} = 0$, where $F_6 \equiv F(0,0) \approx F^T(0,0)$ holds (cf. Sec. A.2).

The *Diţă matrix* D_0 is an example of a complex symmetric Hadamard matrix,

$$D_0 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i & -i & i \\ 1 & i & -1 & i & -i & -i \\ 1 & -i & i & -1 & i & -i \\ 1 & -i & -i & i & -1 & i \\ 1 & i & -i & -i & i & -1 \end{pmatrix}, \tag{28}$$

embedded in a continuous one-parameter set of Hadamard matrices, the Diţă family (cf. A.2).

Björck's *circulant matrix* [24] is defined by

$$C = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & iz & -z & -i & -z^* & iz^* \\ iz^* & 1 & iz & -z & -i & -z^* \\ -z^* & iz^* & 1 & iz & -z & -i \\ -i & -z^* & iz^* & 1 & iz & -z \\ -z & -i & -z^* & iz^* & 1 & iz \\ iz & -z & -i & -z^* & iz^* & 1 \end{pmatrix}, \tag{29}$$

where

$$z = \frac{1-\sqrt{3}}{2} + i\sqrt{\frac{\sqrt{3}}{2}}. \tag{30}$$

It was originally thought to be isolated but it is now known to be part of the family of Hermitian Hadamard matrices, $C \approx B(\theta_0)$ (cf. A.3).

The only known isolated Hadamard matrix is the *spectral matrix*,

$$S = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega & \omega^2 & \omega^2 \\ 1 & \omega & 1 & \omega^2 & \omega^2 & \omega \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^2 & \omega & 1 & \omega \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 \end{pmatrix}, \tag{31}$$

where ω is a third root of unity, $\omega = e^{2\pi i/3}$. It has been discovered by Moorhouse [16] and, independently, by Tao [17].

A.2 Affine Families

There are three affine families of Hadamard matrices, characterized by the property (5) that they can be written as a non-trivial Hadamard product. The *Diţă family* [18] is given by $D(x) = D_0 \circ \text{Exp}[2\pi i R(x)]$, $|x| \leq 1/8$, with D_0 from Eq. (28) and

$$R(x) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x & x & 0 \\ 0 & 0 & -x & 0 & 0 & -x \\ 0 & 0 & -x & 0 & 0 & -x \\ 0 & 0 & 0 & x & x & 0 \end{pmatrix} ; \tag{32}$$

the componentwise exponential $\text{Exp}[\cdot]$ of a matrix has been defined after Eq. (5).

The Fourier matrix F_6 has been embedded in a similar way into a *two*-parameter set, namely the Fourier family $F(\mathbf{x}) = F_6 \circ \text{Exp}[2\pi i R(\mathbf{x})]$, where

$$R(\mathbf{x}) \equiv R(x_1, x_2) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_1 & x_2 & 0 & x_1 & x_2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_1 & x_2 & 0 & x_1 & x_2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_1 & x_2 & 0 & x_1 & x_2 \end{pmatrix} ; \tag{33}$$

the parameters (x_1, x_2) take values in a fundamental region given by a triangle with vertices $(0,0)$, $(1/6, 0)$ and $(1/6, 1/12)$.

Upon transposing the matrices $F(\mathbf{x})$ one obtains a different two-parameter set of Hadamard matrices, called the *transposed Fourier family* $F^T(\mathbf{x})$. It has the same fundamental region as the Fourier family.

A.3 Non-Affine Families

Non-affine Hadamard matrices cannot be written in the form (5). The *Hermitean family* [20] provides a one-parameter example of such a set,

$$B(\theta) = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & x^* & -y & y & x^* \\ 1 & -x & 1 & y & z^* & t^* \\ 1 & y^* & y^* & 1 & t^* & t^* \\ 1 & y^* & z & -t & 1 & x^* \\ 1 & x & -t & t & -x & 1 \end{pmatrix} , \tag{34}$$

where $y = e^{2\pi i \theta}$ and $t = xyz$, with

$$\begin{aligned} z &= \frac{1 + 2y - y^2}{y(-1 + 2y + y^2)} , \\ x &= \frac{1 + 2y + y^2 \pm \sqrt{2(1 + 2y + 2y^3 + y^4)}}{1 + 2y - y^2} ; \end{aligned}$$

the free parameter θ is restricted to vary within the fundamental interval $[\theta_0, 1 - \theta_0]$, and the number θ_0 is defined by the condition

$$2\pi\theta_0 = \cos^{-1}\left(1 - \sqrt{3}\right) . \tag{35}$$

Note that this is a smaller fundamental region than was previously known; the reduction is due to equivalences that have become apparent since the discovery of the Szöllősi family (cf. below).

Another non-affine one-parameter set of Hadamard matrices is given by the *symmetric family* [19],

$$M(t) = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & x & x & -x & -x \\ 1 & x & d & a & b & c \\ 1 & x & a & d & c & b \\ 1 & -x & b & c & p & q \\ 1 & -x & c & b & q & p \end{pmatrix} , \tag{36}$$

where $x = e^{2\pi i t}$, and the complex numbers a, b, c, d, p, q are the unique solutions of the equations

$$\begin{aligned} 1 + x + d + a + b + c &= 0 \, , \\ x^2 - 2x - 2a - 2d - 1 &= 0 \, , \\ 1 - x + b + c + p + q &= 0 \, , \\ x^2 + 2b + 2c + 1 &= 0 \, . \end{aligned} \tag{37}$$

In addition, one needs the fact that given a row $(r_1, \ldots, r_6)$ of a Hadamard matrix, the last two elements are determined by $\Sigma = (r_1 + r_2 + r_3 + r_4)/2$, since

$$r_{5,6} = -\Sigma \pm i \frac{\Sigma}{|\Sigma|} \sqrt{1 - |\Sigma|^2} \tag{38}$$

if $\Sigma \neq 0$. The fundamental region is given by $t \in [0, 1/2]$.

Finally, there is the non-affine *Szöllősi family* [22]

$$X(a,b) \equiv H(x,y,u,v) = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x^2 y & x y^2 & \frac{xy}{uv} & uxy & vxy \\ 1 & \frac{x}{y} & x^2 y & \frac{x}{u} & \frac{x}{v} & uvx \\ 1 & uvx & uxy & -1 & -uxy & -uvx \\ 1 & \frac{x}{u} & vxy & -\frac{x}{u} & -1 & -vxy \\ 1 & \frac{x}{v} & \frac{xy}{uv} & -\frac{xy}{uv} & -\frac{x}{v} & -1 \end{pmatrix} . \tag{39}$$

The entries x, y and u, v are solutions to the equations $f_\alpha = 0$ and $f_{-\alpha} = 0$, respectively, where

$$f_\alpha(z) \equiv z^3 - \alpha z^2 + \alpha^* z - 1 \, , \tag{40}$$

and $\alpha \equiv a + ib$ is restricted to the region $\mathbb{D}$ defined by $D(\alpha) \leq 0$ and $D(-\alpha) \leq 0$, with

$$D(\alpha) \equiv |\alpha|^4 + 18|\alpha|^2 - 8\mathrm{Re}[\alpha^3] - 27 \, . \tag{41}$$

It is possible to reduce $\mathbb{D}$ to a smaller fundamental region [23] since, firstly, the transformation $\alpha \to -\alpha$ maps Hadamard matrices to equivalent ones and, second, Eq. (40) is invariant under the substitutions $\alpha \to \omega\alpha$ and $y \to \omega y$ with $\omega = \exp(2\pi i/3)$. As the second transformation leaves the dephased Hadamard matrix invariant, this establishes an equivalence between the Hadamard matrices associated with points in $\mathbb{D}$ and in $\mathbb{D}'$ (which one obtains from $\mathbb{D}$ through a rotation by $2\pi/3$). As a result, the region $\mathbb{D}$ is found to consist of six equivalent sectors, and one may restrict α by

$$0 \leq \arg(\alpha) \leq \frac{\pi}{3} \, . \tag{42}$$

The *transposed Szöllősi family*, $X^T(a,b)$ is obtained by transposing $X(a,b)$ or by using the equivalence $H(x,y,u,v)^T \approx H(x,y,v,u)$. Fig. 1 illustrates that the points on the boundary of the reduced fundamental region for both $X(a,b)$ and $X^T(a,b)$ correspond to the members of the Hermitean family.

B Simplification of the Fourier equations in dimension 6

The conditions for a state $|v\rangle \in \mathbb{C}^6$ to be MU with respect to F_6 are given by $\mathcal{P} = 0$ where $\mathcal{P} = \{p_\pm, q_\pm, r_\pm\}$ with

$$\begin{aligned}
p_\pm &= -5 \pm 2\,x_5 + 2\,x_4 \pm 2\,x_3 + 2\,x_2 \pm 2\,x_1 + {x_5}^2 \pm 2\,x_4x_5 + {x_4}^2 + 2\,x_3x_5 \pm 2\,x_3x_4 \\
&\quad + {x_3}^2 \pm 2\,x_2x_5 + 2\,x_2x_4 \pm 2\,x_2x_3 + {x_2}^2 + 2\,x_1x_5 \pm 2\,x_1x_4 + 2\,x_1x_3 \pm 2\,x_1x_2 \\
&\quad + {x_1}^2 + {y_5}^2 \pm 2\,y_4y_5 + {y_4}^2 + 2\,y_3y_5 \pm 2\,y_3y_4 + {y_3}^2 \pm 2\,y_2y_5 + 2\,y_2y_4 \pm 2\,y_2y_3 \\
&\quad + {y_2}^2 + 2\,y_1y_5 \pm 2\,y_1y_4 + 2\,y_1y_3 \pm 2\,y_1y_2 + {y_1}^2\,, \\
q_\pm &= -5 + x_5 - x_4 - 2\,x_3 - x_2 + x_1 \mp \sqrt{3}y_5 \mp \sqrt{3}y_4 \pm \sqrt{3}y_2 \pm \sqrt{3}y_1 + {x_5}^2 + x_4x_5 \\
&\quad + {x_4}^2 - x_3x_5 + x_3x_4 + {x_3}^2 - 2\,x_2x_5 - x_2x_4 + x_2x_3 + {x_2}^2 - x_1x_5 - 2\,x_1x_4 \\
&\quad - x_1x_3 + x_1x_2 + {x_1}^2 \pm \sqrt{3}y_5x_4 \pm \sqrt{3}y_5x_3 \mp \sqrt{3}y_5x_1 + {y_5}^2 \mp \sqrt{3}y_4x_5 \pm \sqrt{3}y_4x_3 \\
&\quad \pm \sqrt{3}y_4x_2 + y_4y_5 + {y_4}^2 \mp \sqrt{3}y_3x_5 \mp \sqrt{3}y_3x_4 \pm \sqrt{3}y_3x_2 \pm \sqrt{3}y_3x_1 - y_3y_5 \\
&\quad + y_3y_4 + {y_3}^2 \mp \sqrt{3}y_2x_4 \mp \sqrt{3}y_2x_3 \pm \sqrt{3}y_2x_1 - 2\,y_2y_5 - y_2y_4 + y_2y_3 + {y_2}^2 \\
&\quad \pm \sqrt{3}y_1x_5 \mp \sqrt{3}y_1x_3 \mp \sqrt{3}y_1x_2 - y_1y_5 - 2\,y_1y_4 - y_1y_3 + y_1y_2 + {y_1}^2\,, \\
r_\pm &= -5 - x_5 - x_4 + 2\,x_3 - x_2 - x_1 \mp \sqrt{3}y_5 \mp \sqrt{3}y_4 \pm \sqrt{3}y_2 \mp \sqrt{3}y_1 + {x_5}^2 - x_4x_5 \\
&\quad + {x_4}^2 - x_3x_5 - x_3x_4 + {x_3}^2 + 2\,x_2x_5 - x_2x_4 - x_2x_3 + {x_2}^2 - x_1x_5 + 2\,x_1x_4 \\
&\quad - x_1x_3 - x_1x_2 + {x_1}^2 \pm \sqrt{3}y_5x_4 \mp \sqrt{3}y_5x_3 \pm \sqrt{3}y_5x_1 + {y_5}^2 \mp \sqrt{3}y_4x_5 \pm \sqrt{3}y_4x_3 \\
&\quad \mp \sqrt{3}y_4x_2 - y_4y_5 + {y_4}^2 \pm \sqrt{3}y_3x_5 \mp \sqrt{3}y_3x_4 \pm \sqrt{3}y_3x_2 \mp \sqrt{3}y_3x_1 - y_3y_5 \\
&\quad - y_3y_4 + {y_3}^2 \pm \sqrt{3}y_2x_4 \mp \sqrt{3}y_2x_3 \pm \sqrt{3}y_2x_1 + 2\,y_2y_5 - y_2y_4 - y_2y_3 + {y_2}^2 \\
&\quad \mp \sqrt{3}y_1x_5 \pm \sqrt{3}y_1x_3 \mp \sqrt{3}y_1x_2 - y_1y_5 + 2\,y_1y_4 - y_1y_3 - y_1y_2 + {y_1}^2\,.
\end{aligned} \tag{43}$$

Upon substituting the normalization condition $\langle v|v\rangle = 1$, or

$${x_1}^2 + {y_1}^2 + {x_2}^2 + {y_2}^2 + {x_3}^2 + {y_3}^2 + {x_4}^2 + {y_4}^2 + {x_5}^2 + {y_5}^2 = 5\,, \tag{44}$$

one finds

$$\begin{aligned}
p_+ + p_- &= 0\,, \\
p_+ - p_- - q_+ + q_- + r_+ - r_- &= 0\,, \\
2p_+ - 2\,p_- + q_+ - q_- - r_+ + r_- &= 0\,, \\
p_+ \pm p_- \mp r_+ - r_- &= 0\,,
\end{aligned} \tag{45}$$

giving Eqs. (16).