Constructing mutually unbiased bases in dimension six

Stephen Brierley* and Stefan Weigert†

Department of Mathematics, University of York Heslington, York YO10 5DD, United Kingdom

(Received 27 January 2009; published 14 May 2009)

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.

I. 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,

$$H^\dagger H' = H'', \qquad (1)$$

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]. Such bases are often characterized directly by the scalar products between their elements,

$$|\langle \psi_j^b | \psi_{j'}^{b'} \rangle| = \begin{cases} \delta_{jj'} & \text{if } b = b', \\ \dfrac{1}{\sqrt{d}} & \text{if } b \neq b', \end{cases} \qquad (2)$$

where $b, b' = 0, 1, \ldots, d$. MU bases are also useful for 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 proven 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 a complete set of MU bases in $\mathbb{C}^d$ is equivalent to finding an orthogonal decomposition of the Lie algebra $sl_d(\mathbb{C})$. This 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:

(1) 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;

(2) there are at least (p^k+1) MU bases where the p^k is the smallest factor in the prime decomposition of d [8];

(3) more than (p^k+1) MU bases are known to 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 has 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:

(i) no evidence for the existence of *four* MU bases in $\mathbb{C}^6$ has been found [11];

(ii) 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:

(a) selecting a first Hadamard matrix and then searching for MU vectors with components given by suitable roots of unity lead to no more than two MU complex Hadamard matrices or three MU bases in $\mathbb{C}^6$ [13];

(b) Grassl [7] showed 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 the approach of Grassl [7] by removing the restriction that the second MU basis should 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 in $\mathbb{C}^6$. 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.

*sb572@york.ac.uk
†slow500@york.ac.uk

Let us now present the outline of our argument. In Sec. II, we briefly describe the set of known complex Hadamard matrices in dimension six. Then, we explain in Sec. III 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, while rederiving the result of Grassl [7] for $d=6$, we will explain the subtle interplay between algebraic and numerical calculations in this approach. Sec. IV 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.

II. 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

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

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 as

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

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 has 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
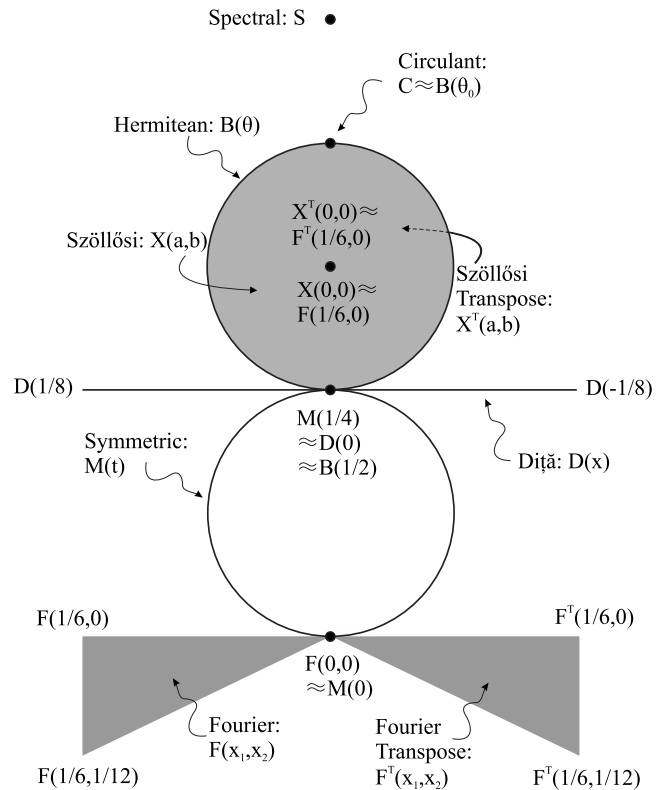

FIG. 1. The set of known Hadamard matrices in dimension six consists of *special* Hadamard matrices $F(0,0) \equiv F_6$, $D(0) \equiv D_0$, C, and S, located on the vertical symmetry axis; of the *affine* families $D(x)$, $F(\mathbf{x})$, and $F^T(\mathbf{x})$; and of the *nonaffine* families $M(t)$, $B(\theta)$, $X(a,b)$, 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.

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 its boundary. 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 equivalence relation (4).

Figure 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; interestingly, the Diţă matrices are also contained therein [22]. Lining up some of the points where different families overlap suggests that we arrange the

Hadamard matrices in a symmetrical way. Then, a reflection about the line passing through the points $F(0,0)$ and S maps $H(\mathbf{x})$ to $H(-\mathbf{x})$ if $H(\mathbf{x})$ is a member of the Diţă, Hermitean or symmetric families; furthermore, the same reflection sends $H(\mathbf{x})$ to $H^T(\mathbf{x})$ if the matrix $H(\mathbf{x})$ is taken from Diţă, Hermitean, or Fourier families. For the Szöllősi family, the reflection about the vertical axis must be supplemented by a change in layer in order to get from $X(a,b)$ to $X^T(a,b)$. We will see that the findings presented in Sec. IV echo this symmetry which we will explain in the conclusion.

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

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

for some matrix R; the open circle denotes the Hadamard (elementwise) product of two matrices, $(A \circ B)_{ij} = A_{ij}B_{ij}$, and $\text{Exp}[R]$ 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.

III. CONSTRUCTING MU VECTORS

In this section, we make explicit the conditions on a vector in $\mathbb{C}^6$ to be MU with respect to the standard matrix and a fixed Hadamard matrix, i.e., to the 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 the result of Grassl [7] for $d=6$ in order to explain that this approach produces rigorous results in spite of inevitable numerical approximations.

A. 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 kth 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

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

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

$$x_j^2 + y_j^2 = 1, \quad j=1,\ldots,d-1, \qquad (7)$$

and the second set is given by

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

where the state $|h(k)\rangle$, $k=0,\ldots,d-2$, has components $h_j(k) \equiv H_{jk}$ and $j=0,\ldots,d-1$. 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 Eq. (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 $|v\rangle$ which are MU to the chosen pair of bases $\{I,H\}$. Analyzing 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 variable ordering [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 generates all solutions of $\mathcal{G}=0$ and, therefore, all solutions of the original set of equations, $\mathcal{P}=0$ [26].

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 make explicit how to construct all vectors MU with respect to a pair $\{I,H\}$ by solving for the roots of the multivariate polynomials given in Eqs. (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 method and to discuss some of its subtleties.

B. 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 provide a complete set of four MU bases in $\mathbb{C}^3$.

1. Choose a Hadamard Matrix

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,

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

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 Eq. (6), constraints (7) and (8) read explicitly as

$$1 - x_1^2 - y_1^2 = 0,$$

$$1 - x_2^2 - y_2^2 = 0,$$

$$x_1 + x_2 + x_1 x_2 + y_1 y_2 = 0,$$

$$x_1 + x_2 - \sqrt{3}y_1 + \sqrt{3}y_2 + x_1 x_2 - \sqrt{3}x_1 y_2 + \sqrt{3}y_1 x_2 + y_1 y_2 = 0. \qquad (10)$$

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 Eq. (10). Equating the resulting four polynomials $g_n(\mathbf{x})$, $n = 1, \ldots, 4$, to zero gives rise to the equations

$$3y_2 - 4y_2^3 = 0,$$

$$1 - x_2 - 2y_2^2 = 0,$$

$$1 + 2x_1 + 4y_1 y_2 - 4y_2^2 = 0,$$

$$3 - 4y_1^2 + 4y_1 y_2 - 4y_2^2 = 0. \qquad (11)$$

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,

$$\mathbf{s}_a = \frac{1}{2}(-1, -1, \sqrt{3}, \sqrt{3}), \quad \mathbf{s}_b = \frac{1}{2}(-1, 2, -\sqrt{3}, 0),$$

$$\mathbf{s}_c = \frac{1}{2}(2, -1, 0, -\sqrt{3}), \quad \mathbf{s}_d = \frac{1}{2}(-1, -1, -\sqrt{3}, -\sqrt{3}),$$

$$\mathbf{s}_e = \frac{1}{2}(2, -1, 0, \sqrt{3}), \quad \mathbf{s}_f = \frac{1}{2}(-1, 2, \sqrt{3}, 0),$$

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

Since the degrees of the polynomials $\mathcal{G}$ in Eq. (11) do not exceed 3, 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. III C) which requires numerical methods. The resulting complications will be discussed in Sec. III D.

4. List all MU vectors

Upon substituting the solutions $\mathbf{s}_a$ to $\mathbf{s}_f$ into Eq. (6), one obtains six vectors

$$v_a = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega \\ \omega \end{pmatrix}, \quad v_b = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega^2 \\ 1 \end{pmatrix}, \quad v_c = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ \omega^2 \end{pmatrix},$$

$$v_d = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega^2 \\ \omega^2 \end{pmatrix}, \quad v_e = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ \omega \end{pmatrix}, \quad v_f = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega \\ 1 \end{pmatrix}, \qquad (14)$$

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 $v_a, \ldots, v_f$ as the only candidates for the columns of additional MU Hadamard matrices.

5. Analyze the vectors

The six vectors in Eq. (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 $d = 2, 5$ and $d = 7$ where it correctly generates 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, correctly reproducing known results [6,29].

C. 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 Eq. (9), the dephased Fourier matrix

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

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

$$x_1 + x_5 + x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_5 + y_1 y_2 + y_2 y_3$$
$$+ y_3 y_4 + y_4 y_5 = 0,$$

$$y_1 - y_5 + x_1 y_2 - x_2 y_1 + x_2 y_3 - x_3 y_2 + x_3 y_4$$
$$- x_4 y_3 + x_4 y_5 - x_5 y_4 = 0,$$

$$x_3 + x_1 x_4 + x_2 x_5 + y_1 y_4 + y_2 y_5 = 0,$$

$$x_2 + x_4 + x_1 x_3 + x_1 x_5 + x_2 x_4 + x_3 x_5 + y_1 y_3 + y_1 y_5$$
$$+ y_2 y_4 + y_3 y_5 = 0,$$

$$y_2 - y_4 + x_1 y_3 - x_1 y_5 + x_2 y_4 - x_3 y_1 + x_3 y_5 - x_4 y_2$$
$$+ x_5 y_1 - x_5 y_3 = 0, \qquad (16)$$

which must be supplemented by the five conditions spelt out in Eq. (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, $\mathcal{G}=0$,

$$-245\,025 y_5 + 4\,318\,758 y_5^3 - 28\,135\,161 y_5^5 + 89\,685\,000 y_5^7$$
$$- 158\,611\,892 y_5^9 + 177\,275\,680 y_5^{11} - 150\,745\,472 y_5^{13}$$
$$+ 104\,333\,824 y_5^{15} - 43\,667\,456 y_5^{17} + 2\,351\,104 y_5^{19}$$
$$+ 4\,882\,432 y_5^{21} - 1\,703\,936 y_5^{23} + 262\,144 y_5^{25} = 0, \quad (17)$$

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

$$y_5 \in \left\{ 0, \pm 1, \pm \frac{1}{2}, \pm \frac{\sqrt{3}}{2}, \pm \frac{1}{2}(1+\sqrt{3}), \right.$$
$$\left. \pm \frac{1}{2}(1-\sqrt{3}), \pm 0.988\,940\ldots, \pm 0.622\,915\ldots \right\}, \qquad (18)$$

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 Eq. (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 Eq. (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. It also follows that the Fourier matrix F_6 (or any other unitarily equivalent element of the Heisenberg-Weyl group [7]) *cannot* be supplemented by two MU Hadamard matrices—no four MU bases can exist.

There are, however, many choices other than $H=F_6$ for a dephased Hadamard matrix in dimension six. In Sec. IV, 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.

D. 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 [30].

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 exact states, $|v_a\rangle$ and $|v_b\rangle$, differ from the approximate states, $|v_A\rangle$

and $|v_B\rangle$, by error terms $|\delta v_a\rangle = |v_A\rangle - |v_a\rangle$ and similarly for the second solution. The components of the vectors $|\delta v_a\rangle$ all have moduli smaller than the user-defined accuracy of 10^{-r}, say. If the inner product of the exact states $|v_a\rangle$ and $|v_b\rangle$ has a nonzero modulus, $\Delta > 0$, then they are *not* orthogonal. We can detect this by calculating the inner product of the *approximate* states,

$$|\langle v_A|v_B\rangle| = |\langle v_a|v_b\rangle + \langle v_a|\delta v_b\rangle + \langle \delta v_a|v_b\rangle + \langle \delta v_a|\delta v_b\rangle|$$
$$\leq |\langle v_a|v_b\rangle| + |\langle v_a|\delta v_b\rangle| + |\langle \delta v_a|v_b\rangle| + O(10^{-2r})$$
$$\leq |\langle v_a|v_b\rangle| + 10\sqrt{2} \times 10^{-r} + O(10^{-2r}), \quad (19)$$

using $\||\delta v_a\rangle\| \leq 5\sqrt{2} \times 10^{-r}$ and $\||v_a\rangle\| = 1$. Thus, a nonzero lower bound for the exact scalar product follows if the approximate inner product is *larger* than $\sqrt{2} \times 10^{-r+1}$. In other words, we may conclude that the exact states are nonorthogonal if we ensure that the error in the approximate scalar product is negligible, i.e., $\Delta \geq |\langle v_A|v_B\rangle| - \sqrt{2} \times 10^{-r+1} > 0$. A similar argument allows us to exclude that two approximate states are MU with respect to each other.

We determine the roots of $\mathcal{G} = 0$ to $r = 20$ significant digits which proves sufficient to put relevant limits on the properties of the vectors constructed in dimension six. The results presented in the Secs. IV A and IV B thus represent rigorous limits on the number of vectors MU with respect to specific Hadamard matrices and hence on the number of MU bases.

IV. 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 determine two quantities for each chosen Hadamard matrix H. The number N_v equals the number of vectors MU with the pair $\{I, H\}$, and the number N_t provides an upper bound on how many different triples of MU bases $\{I, H, H'\}$ exist.

A. Special Hadamard matrices

To begin, we consider the Hadamard matrices 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. These matrices are special in the sense that they are either isolated or belong to different Hadamard families simultaneously.

The first row of Table I completes the findings of Sec. III C obtained for the *Fourier* matrix F_6: there are $N_v = 48$ vectors MU with respect to both I and F_6 that can be arranged in $N_t = 16$ different ways to form a second Hadamard matrix H' being 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,

TABLE I. The number of MU vectors and their properties for *special* Hadamard matrices: there are N_v vectors MU with respect to the pair of matrices $\{I, H\}$ that form N_t additional Hadamard matrices; i.e., there are N_t different *triples* of MU bases.

H	N_v	N_t
F_6	48	16
D_0	120	10
C	56	4
S	90	0

60 of which form ten bases but none of these are MU with respect to each other. While ten triples of MU bases exist, sets of four MU bases which include D_0 do *not* exist.

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

$$\phi_D \equiv \{0, \pi, \pm \pi/12, \ldots, \pm 11\pi/12, \pm \alpha\}, \quad (20)$$

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. VII must be swapped). What is more, our approach *proves* that these authors had 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 value of N_t in Table I given for D_0 is *exact*; rather than an upper bound since the phases of the MU states $|v\rangle$ are known in closed form.

The *circulant* matrix C permits 56 MU vectors, which can be arranged into four different bases, $N_t = 4$. 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. Thus, the pair $\{I, S\}$ cannot even be extended to a triple of MU bases.

B. Affine families

Table II 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 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 includes the 24th roots of unity which play an important role for D_0, so

$$\Gamma_D = \{a/144 : a = \pm 1, \pm 2 \ldots, \pm 18\}; \quad (21)$$

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

---

[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 $\tan \beta = 3$.

TABLE II. The number of MU vectors and their properties for *affine* Hadamard matrices: the second column indicates which values have been chosen for the parameters **x**; the grids of points Γ_D and Γ_F are defined in Eqs. (21) and (22), respectively; the third column displays the number of Hadamard matrices considered in a sample; and N_v and N_t are defined as in Table I and vary as a function of the parameter values (cf. Sec. IV B).

H	$\mathbf{x}$	#($\mathbf{x}$)	N_v	N_t
$D(x)$	Γ_D	36	48/72/120	4
	random	500	72/120	4
$F(\mathbf{x})$	Γ_F	168	48	8/70
	random	2000	48	8
$F^T(\mathbf{x})$	Γ_F	168	48	8/70
	random	2000	48	8

for 48, 72, or 120 MU vectors which can be grouped 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.

The results obtained from *randomly* picking points in the fundamental interval are in line with the observations made for grid points. Figure 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, $x = \pm 1/8$.

The results for members of the *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,
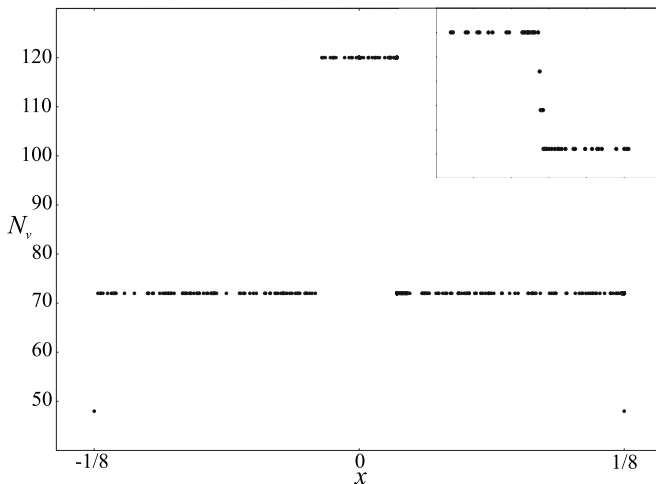

FIG. 2. The number N_v of vectors $|v\rangle$ which are MU with respect to the columns of the identity I and Diţă matrices $D(x)$; the parameter x assumes 72 parameter values $x \in \Gamma_D$ defined in Eq. (21) and 500 randomly chosen ones in the fundamental interval [$-1/8, 1/8$] of the parameter x. 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. IV C).

$$\Gamma_F = \{(a,b)/144 : a = 1, 2, \ldots, 24, \ b = 0, 1, \ldots, 12, \ a \geq 2b\},$$
$$(22)$$

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. It is important to realize that the result of Grassl [7]—the construction of complete sets of MU bases cannot be based on the Heisenberg-Weyl group in dimension $d = 6$—also holds for the 2168 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, 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.

C. Nonaffine families

The equations $\mathcal{P} = 0$ encoding MU vectors for the symmetric $M(t)$, Hermitean $B(\theta)$ 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 nonaffine 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, $\widetilde{\mathcal{P}}$, and the program indeed succeeds in constructing the corresponding Gröbner bases, $\widetilde{\mathcal{G}}$, 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 $\widetilde{\mathcal{P}} = 0$ 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 behavior 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.

Figure 3 shows that the family of *symmetric* Hadamard matrices $M(t)$ comes with 48 MU vectors $|\tilde{v}\rangle$ close to the
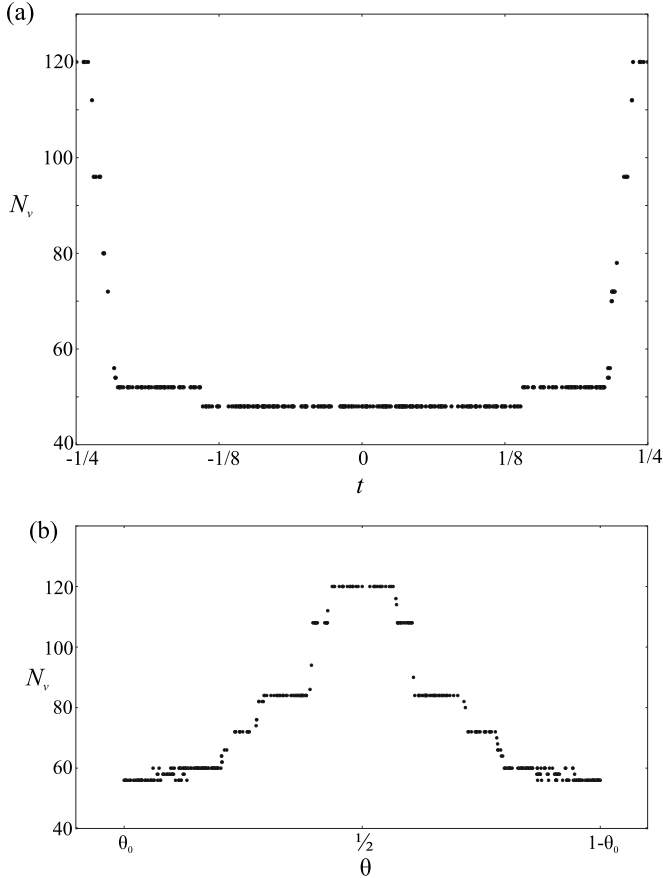
FIG. 3. The number N_v of vectors $|v\rangle$ which are MU with respect to the columns of the identity I and (a) symmetric Hadamard matrices $M(t)$; the parameter t assumes 60 parameter values $t \in \Gamma_M$ defined in Eq. (23) and 300 randomly chosen ones in the fundamental interval $[0,1/2]$ and of (b) Hermitean matrices $B(\theta)$; the parameter θ assumes 34 parameter values $\theta \in \Gamma_B$ defined in Eq. (26) and 300 randomly chosen ones in the fundamental interval $[\theta_0, 1-\theta_0]$. The phase θ_0 has been defined in Eq. (A8).

TABLE III. The number of MU vectors and their properties for *nonaffine* Hadamard matrices: the grids Γ_M and Γ_B are defined in Eqs. (23) and (24), respectively; see Eqs. (25) and (26) for the definition of the lines Λ and Λ'; other notation as in Table II.

H	$\mathbf{x}$	#$(\mathbf{x})$	N_v	N_t
$M(t)$	Γ_M	70	48–120	1–16
	random	300	48–120	1–16
$B(\theta)$	Γ_B	34	56–120	1/4/8/16
	random	300	56–120	1/4/8/16
$X(a,b)$	Λ	50	48/56	4/16/70
	Λ'	50	48–60	4/8/16/70
	random	300	48–120	1–70

rigorous approach will confirm the absence of a set of four MU bases containing a single symmetric Hadamard matrix $M(t)$.

The results obtained for *Hermitean* Hadamard matrices $B(\theta)$, shown in Fig. 3, are similar to those of the symmetric family. The observed plateaus conform with the rigorous bounds found for $N_v=120$ and $N_v=56$ due to the equivalences $B(1/2) \approx D(0)$ and $B(\theta_0) \approx C$ (cf. Table I). 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 III reveals that both regularly spaced points on the grid

$$\Gamma_B = \{a/144 : a = 55, 56, \ldots, 89; \ a \neq 72\} \qquad (24)$$

and randomly chosen values of the parameter θ define Hadamard matrices $B(\theta)$ which allow the construction of three MU bases but not four.

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

$$\Lambda = \{(a,b) : \arg(a+ib) = \pi/6\} \qquad (25)$$

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

$$\Lambda' = \{(a,b) : \arg(a+ib) = 0.3510\} \qquad (26)$$

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 nonaffine 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 which allow for triples of MU bases but never for a quadruple. Preliminary calculations show that the properties of the new family of transposed
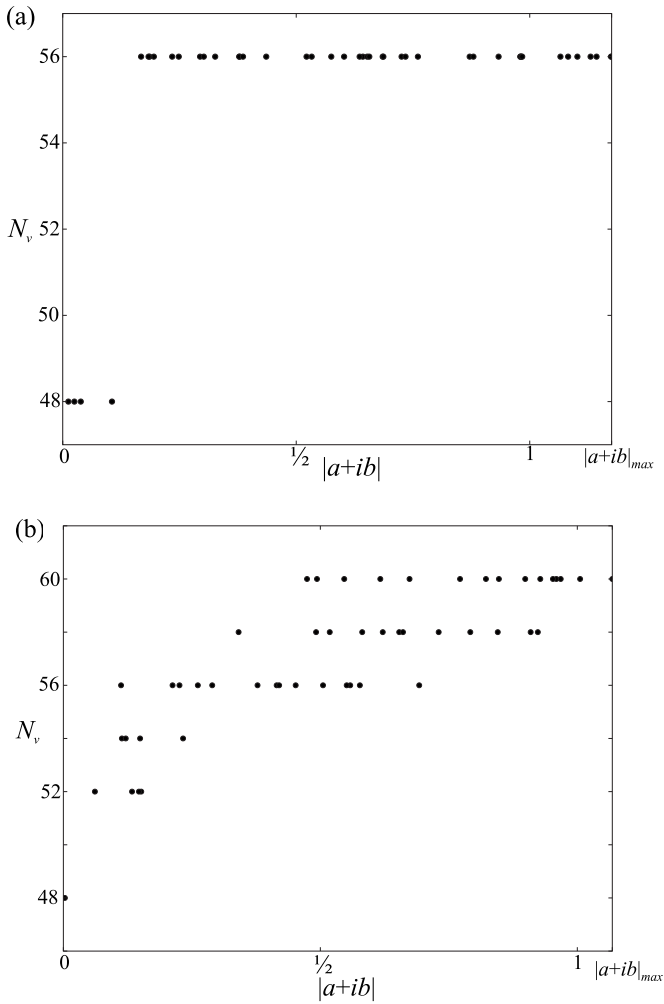
point $t=0$, while there are 120 near $t=1/4$. These numbers are consistent with the rigorous bounds obtained in Sec. IV B if we recall that $M(0)=M(1/2) \approx F(0,0)$ and $M(1/4) \approx D(0)$ hold (cf. Fig. 1). Across the entire parameter range, the number of MU vectors is a piecewise constant function 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 can be arranged between 1 and 16 additional bases, a plot of which also resembles a step function. Crucially, they can never be arranged to form two bases that are MU to each other and therefore the points in Fig. 3 cannot be included in a set of four MU bases. Table III lists the results obtained for both a regular grid

$$\Gamma_M = \{a/144 : a = 1, 2, \ldots, 71; \ a \neq 36\} \qquad (23)$$

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

FIG. 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 $B(\theta')$; the maximum modulus $|a+ib|_{max}$ is defined by Eq. (A14).

Szöllősi matrices $X^T(a,b)$ are similar to those of the set $X(a,b)$.

The results for the symmetric, Hermitean, and Szöllősi families provide approximate bounds on the number of MU bases which can be constructed from their members. None of the Hadamard matrices considered can be extended to a set of four MU bases. We consider it unlikely that the approximation made would systematically suppress other MU vectors with properties invalidating this conclusion.

V. 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 5980 calculations required between 4 and 16 GB of memory and, alto-
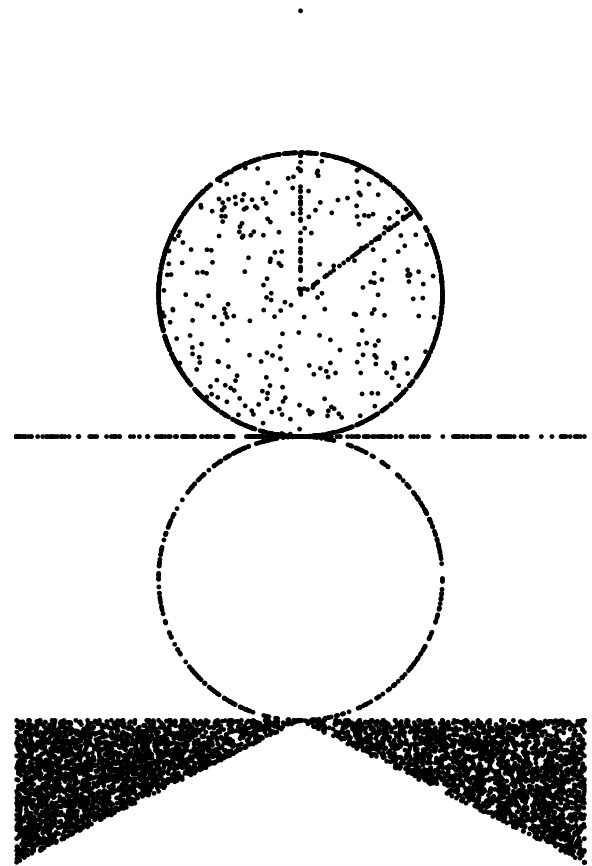

FIG. 5. The set of all Hadamard matrices H which have been considered (cf. Fig. and Tables I–III): for each H, a second MU Hadamard matrix can always be found except for the isolated spectral matrix S; consequently, triples of MU bases are the norm while quartets of MU bases do not exist.

gether, would have lasted approximately 29 000 h 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 the spectral matrix S is the only Hadamard matrix which cannot be extended to a triple of MU bases. Furthermore, if four (seven) MU bases were to exist in dimension six three (six) Hadamard matrices different from the ones shown in Fig. 5 would be required. This clearly conforms with the numerically obtained evidence that no four MU basis exist [12].

There is one caveat that we must make regarding the results for the nonaffine families. In general, the program was unable to construct the associated Gröbner bases for the symmetric, Hermitean and Szöllősi families. For these Hadamard matrices, we cannot guarantee that we have found *all* MU vectors although we consider it unlikely that the approximation made would systematically suppress the missing vectors.

The symmetrical presentation of known Hadamard matrices in Fig. 1 is justified by the results of our calculations: both the number of vectors N_v and the values of their inner products (i.e., the number N_t) are symmetric about the line passing through $F(0,0)$ and S. We will now explain why this symmetry exists.

First, let H be a member of the Diţă, symmetric or Fourier families and consider a vector $|v\rangle$ that is MU to both I and H. Since multiplication by an overall unitary leaves the MU conditions [Eq. (2)] invariant, we have the equivalence between sets

$$\{I, H, |v\rangle\} \approx \{H^\dagger, I, H^\dagger|v\rangle\} = \{I, H^\dagger, |v'\rangle\} \qquad (27)$$

where $|v'\rangle = H^\dagger|v\rangle$. It follows that $|v'\rangle$ is MU to I and $H^\dagger$, and since $D^\dagger(x) \approx D(-x)$, $M^\dagger(t) \approx M(-t)$. and $F^\dagger(x_1, x_2) \approx F^T(x_1, x_2)$, the number of solutions N_v is symmetric about the line through $F(0,0)$ and S. Further, since $H^\dagger$ is unitary and it is applied to all vectors, this transformation leaves the inner products between two MU vectors invariant and, therefore, the number of triples N_t is also symmetric.

We need an additional transformation to explain the symmetry found for the Hermitean matrices since $B^\dagger(\theta) = B(\theta)$: under complex conjugation a Hermitean matrix transforms according to

$$B^*(\theta) = B(1 - \theta), \qquad (28)$$

as follows from the explicit form of $B(\theta)$ given in Eq. (A7). Now consider a vector $|v\rangle$ which is MU to the columns $b(\theta)$ of the matrix $B(\theta)$; then

$$|\langle b(\theta)|v\rangle|^2 = |\langle b(\theta)|v\rangle^*|^2 = |\langle b^*(\theta)|v^*\rangle|^2 = |\langle b(1-\theta)|v^*\rangle|^2, \qquad (29)$$

and therefore $|v^*\rangle$ is MU to each column of $B(1-\theta)$. Thus, the vectors MU to $B(\theta)$ are the complex conjugates of those MU to $B(1-\theta)$ which implies that the number N_v of MU vectors (and their properties) will not change upon a reflection about the point $\theta = 1/2$. Although we did not pay attention to the existence of these exact symmetries when introducing the approximations for the nonaffine Hadamard matrices, the results obtained do respect them.

The set of Hadamard matrices in $\mathbb{C}^6$ may depend on four parameters [13], a conjecture which recently gained some numerical support [31]. 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 starting from nearly 6,000 different Hadamard matrices. This result adds 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.

After the submission of this article it has been shown [32] that for all parameter values **x**, the Fourier family, $F(\mathbf{x})$, only admits triples of MU bases.

APPENDIX 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 catalog [15].

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. III B 2).

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

$$D_0 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i & -i & i \\ 1 & i & -1 & i & -i & -i \\ 1 & -i & i & -1 & i & -i \\ 1 & -i & -i & i & -1 & i \\ 1 & i & -i & -i & i & -1 \end{pmatrix}, \qquad (A1)$$

embedded in a continuous one-parameter set of Hadamard matrices, the Diţă family [cf. Sec. III B 2].

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

$$C = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & iz & -z & -i & -z^* & iz^* \\ iz^* & 1 & iz & -z & -i & -z^* \\ -z^* & iz^* & 1 & iz & -z & -i \\ -i & -z^* & iz^* & 1 & iz & -z \\ -z & -i & -z^* & iz^* & 1 & iz \\ iz & -z & -i & -z^* & iz^* & 1 \end{pmatrix}, \qquad (A2)$$

where

$$z = \frac{1 - \sqrt{3}}{2} + i \sqrt{\frac{\sqrt{3}}{2}}. \qquad (A3)$$

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

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

$$S = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega & \omega^2 & \omega^2 \\ 1 & \omega & 1 & \omega^2 & \omega^2 & \omega \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^2 & \omega & 1 & \omega \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 \end{pmatrix}, \qquad (A4)$$

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].

2. Affine families

There are three affine families of Hadamard matrices, characterized by property (5) that they can be written as a

nontrivial Hadamard product. The *Diţă family* [18] is given by $D(x) = D_0 \circ \mathrm{Exp}[2\pi i R(x)]$, $|x| \le 1/8$, with D_0 from Eq. (A1) and

$$R(x) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x & x & 0 \\ 0 & 0 & -x & 0 & 0 & -x \\ 0 & 0 & -x & 0 & 0 & -x \\ 0 & 0 & 0 & x & x & 0 \end{pmatrix}; \qquad (A5)$$

the componentwise exponential $\mathrm{Exp}[\cdot]$ 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 $F(\mathbf{x}) = F_6 \circ \mathrm{Exp}[2\pi i R(\mathbf{x})]$, where

$$R(\mathbf{x}) \equiv R(x_1, x_2) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_1 & x_2 & 0 & x_1 & x_2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_1 & x_2 & 0 & x_1 & x_2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_1 & x_2 & 0 & x_1 & x_2 \end{pmatrix}; \qquad (A6)$$

the parameters (x_1, x_2) take values in a fundamental region given by a triangle with vertices $(0,0)$, $(1/6,0)$, and $(1/6,17/12)$.

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.

3. Nonaffine families

Nonaffine Hadamard matrices are not parametrized in form (5). The *Hermitean family* [20] provides a one-parameter example of such a set,

$$B(\theta) = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & x^* & -y & y & x^* \\ 1 & -x & 1 & y & z^* & t^* \\ 1 & y^* & y^* & 1 & t^* & t^* \\ 1 & y^* & z & -t & 1 & x^* \\ 1 & x & -t & t & -x & 1 \end{pmatrix}, \qquad (A7)$$

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

$$z = \frac{1 + 2y - y^2}{y(-1 + 2y + y^2)},$$

$$x = \frac{1 + 2y + y^2 \pm \sqrt{2(1 + 2y + 2y^3 + y^4)}}{1 + 2y - y^2};$$

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

$$2\pi\theta_0 = \cos^{-1}(1 - \sqrt{3}). \qquad (A8)$$

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

$$M(t) = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & x & x & -x & -x \\ 1 & x & d & a & b & c \\ 1 & x & a & d & c & b \\ 1 & -x & b & c & p & q \\ 1 & -x & c & b & q & p \end{pmatrix}, \qquad (A9)$$

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

$$1 + x + d + a + b + c = 0,$$

$$x^2 - 2x - 2a - 2d - 1 = 0,$$

$$1 - x + b + c + p + q = 0,$$

$$x^2 + 2b + 2c + 1 = 0. \qquad (A10)$$

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

$$r_{5,6} = -\Sigma \pm i \frac{\Sigma}{|\Sigma|} \sqrt{1 - |\Sigma|^2} \qquad (A11)$$

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

Finally, there is the nonaffine *Szöllősi family* [22]

$$X(a,b) \equiv H(x,y,u,v)$$

$$= \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x^2y & xy^2 & \dfrac{xy}{uv} & uxy & vxy \\ 1 & \dfrac{x}{y} & x^2y & \dfrac{x}{u} & \dfrac{x}{v} & uvx \\ 1 & uvx & uxy & -1 & -uxy & -uvx \\ 1 & \dfrac{x}{u} & vxy & -\dfrac{x}{u} & -1 & -vxy \\ 1 & \dfrac{x}{v} & \dfrac{xy}{uv} & -\dfrac{xy}{uv} & -\dfrac{x}{v} & -1 \end{pmatrix}. \qquad (A12)$$

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

$$f_\alpha(z) \equiv z^3 - \alpha z^2 + \alpha^* z - 1, \qquad (A13)$$

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

$$D(\alpha) \equiv |\alpha|^4 + 18|\alpha|^2 - 8\,\mathrm{Re}[\alpha^3] - 27. \qquad (A14)$$

It is possible to reduce $\mathbb{D}$ to a smaller fundamental region [23] since, first, the transformation $\alpha \rightarrow -\alpha$ maps Hadamard matrices to equivalent ones and, second, Eq. (A13) is invariant under the substitutions $\alpha \rightarrow \omega\alpha$ and $y \rightarrow \omega y$ 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

$$0 \leq \arg(\alpha) \leq \frac{\pi}{3}. \qquad (A15)$$

The *transposed Szöllősi family* $X^T(a,b)$ is obtained by transposing $X(a,b)$ or by using the equivalence $H(x,y,u,v)^T \approx H(x,y,v,u)$. Figure 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.

APPENDIX 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

$$
\begin{aligned}
p_\pm = &-5 \pm 2x_5 + 2x_4 \pm 2x_3 + 2x_2 \pm 2x_1 + x_5^2 \pm 2x_4x_5 + x_4^2 \\
&+ 2x_3x_5 \pm 2x_3x_4 + x_3^2 + 2x_2x_5 + 2x_2x_4 \pm 2x_2x_3 + x_2^2 \\
&+ 2x_1x_5 \pm 2x_1x_4 + 2x_1x_3 \pm 2x_1x_2 + x_1^2 + y_5^2 \pm 2y_4y_5 + y_4^2 \\
&+ 2y_3y_5 \pm 2y_3y_4 + y_3^2 \pm 2y_2y_5 + 2y_2y_4 \pm 2y_2y_3 + y_2^2 \\
&+ 2y_1y_5 \pm 2y_1y_4 + 2y_1y_3 \pm 2y_1y_2 + y_1^2,
\end{aligned}
$$

$$
\begin{aligned}
q_\pm = &-5 + x_5 - x_4 - 2x_3 - x_2 \\
&+ x_1 \mp \sqrt{3}y_5 \mp \sqrt{3}y_4 \pm \sqrt{3}y_2 \pm \sqrt{3}y_1 + x_5^2 + x_4x_5 + x_4^2 \\
&- x_3x_5 + x_3x_4 + x_3^2 - 2x_2x_5 - x_2x_4 + x_2x_3 + x_2^2 - x_1x_5
\end{aligned}
$$

$$
\begin{aligned}
&- 2x_1x_4 - x_1x_3 + x_1x_2 + x_1^2 \pm \sqrt{3}y_5x_4 \pm \sqrt{3}y_5x_3 \mp \sqrt{3}y_5x_1 \\
&+ y_5^2 \mp \sqrt{3}y_4x_5 \pm \sqrt{3}y_4x_3 \pm \sqrt{3}y_4x_2 + y_4y_5 \\
&+ y_4^2 \mp \sqrt{3}y_3x_5 \mp \sqrt{3}y_3x_4 \pm \sqrt{3}y_3x_2 \pm \sqrt{3}y_3x_1 - y_3y_5 \\
&+ y_3y_4 + y_3^2 \mp \sqrt{3}y_2x_4 \mp \sqrt{3}y_2x_3 \pm \sqrt{3}y_2x_1 - 2y_2y_5 \\
&- y_2y_4 + y_2y_3 + y_2^2 \pm \sqrt{3}y_1x_5 \mp \sqrt{3}y_1x_3 \mp \sqrt{3}y_1x_2 - y_1y_5 \\
&- 2y_1y_4 - y_1y_3 + y_1y_2 + y_1^2,
\end{aligned}
$$

$$
\begin{aligned}
r_\pm = &-5 - x_5 - x_4 + 2x_3 - x_2 \\
&- x_1 \mp \sqrt{3}y_5 \mp \sqrt{3}y_4 \pm \sqrt{3}y_2 \mp \sqrt{3}y_1 + x_5^2 - x_4x_5 + x_4^2 \\
&- x_3x_5 - x_3x_4 + x_3^2 + 2x_2x_5 - x_2x_4 - x_2x_3 + x_2^2 - x_1x_5 \\
&+ 2x_1x_4 - x_1x_3 - x_1x_2 + x_1^2 \pm \sqrt{3}y_5x_4 \pm \sqrt{3}y_5x_3 \pm \sqrt{3}y_5x_1 \\
&+ y_5^2 \mp \sqrt{3}y_4x_5 \pm \sqrt{3}y_4x_3 \mp \sqrt{3}y_4x_2 - y_4y_5 \\
&+ y_4^2 \pm \sqrt{3}y_3x_5 \mp \sqrt{3}y_3x_4 \pm \sqrt{3}y_3x_2 \mp \sqrt{3}y_3x_1 - y_3y_5 \\
&- y_3y_4 + y_3^2 \pm \sqrt{3}y_2x_4 \mp \sqrt{3}y_2x_3 \pm \sqrt{3}y_2x_1 + 2y_2y_5 - y_2y_4 \\
&- y_2y_3 + y_2^2 \mp \sqrt{3}y_1x_5 \mp \sqrt{3}y_1x_3 \mp \sqrt{3}y_1x_2 - y_1y_5 + 2y_1y_4 \\
&- y_1y_3 - y_1y_2 + y_1^2. \qquad (B1)
\end{aligned}
$$

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

$$x_1^2 + y_1^2 + x_2^2 + y_2^2 + x_3^2 + y_3^2 + x_4^2 + y_4^2 + x_5^2 + y_5^2 = 5, \quad (B2)$$

one finds

$$p_+ + p_- = 0,$$

$$p_+ - p_- - q_+ + q_- + r_+ - r_- = 0,$$

$$2p_+ - 2p_- + q_+ - q_- - r_+ + r_- = 0,$$

$$p_+ \pm p_- \mp r_+ - r_- = 0, \qquad (B3)$$

giving Eq. (16).

[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. J. 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, *Proceedtings of the ERATO Conference on Quantum Information Science (EQUIS)*, 2004, edited by J. Gruska, eprint arXiv:quant-ph/0406175.
[8] A. Klappenecker and M. Roetteler, Lect. Notes Comput. Sci.

2948, 262 (2004).
[9] P. Wocjan and T. Beth, Quantum Inf. Comput. **5**, 93 (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 Syst. Inf. Dyn. **13**, 133 (2006).
[15] W. Tadej and K. Życzkowski, *On-line Catalgue of Known Hadamard Matrices* (http://chaos.if.uj.edu.pl/karol/hadamard/).
[16] G. E. Moorhouse, *The 2-Transitive Complex Hadamard Matrices*, 2001 (http://www.uwyo.edu/moorhouse/pub).
[17] T. Tao, Math. Res. Lett. **11**, 251 (2004).

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

[19] M. Matolcsi and F. Szöllősi, e-print arXiv:0702043.

[20] K. Beauchamp and R. Nicoara, e-print arXiv:0609076.

[21] U. Haagerup, *Proceedings of the Operator Algebras and Quantum Field Theory Conference*, Rome, 1996, edited by S. Doplicher.

[22] F. Szöllősi, e-print arXiv:0811.3930.

[23] I. Bengtsson (private communication).

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

[25] B. Buchberger, Ph.D. thesis, University of Innsbruck, 1965 (unpublished); M. Abramson J. Symb. Comput. **41**, 471 (2006).

[26] B. Buchberger, in *LMS Lecture Note Series, 251*, edited by B. Buchberger and F. Winkler, 1998).

[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] A. Kostrikin and P. Tiep, *Orthogonal Decompositions and Integral Lattices, de Gruyter Expositions in Mathematics 15* (Walter de Gruyter, Berlin, 1994).

[30] F. Rouillier Appl. Algebra Eng. Commun. Comput. **9**, 433 (1999).

[31] A. J. Skinner, V. A. Newell, and R. Sanchez, J. Math. Phys. **50**, 012107 (2009).

[32] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi, M. Weiner, e-print arXiv:0902.0882.