Mutually unbiased bases with free parameters

Dardo Goyeneche*
National Quantum Information Center of Gdańsk, 81-824 Sopot, Poland;
Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-233 Gdańsk, Poland;
Departamento de Fisíca, Universidad de Concepción, Casilla 160-C, Concepción, Chile;
and Center for Optics and Photonics, Universidad de Concepción, Casilla 4012, Concepción, Chile

Santiago Gómez
Departamento de Fisíca, Universidad de Concepción, Casilla 160-C, Concepción, Chile
and Center for Optics and Photonics, Universidad de Concepción, Casilla 4012, Concepción, Chile
(Received 26 July 2015; published 14 December 2015)

We present a systematic method to introduce free parameters in sets of mutually unbiased bases. In particular, we demonstrate that any set of m real mutually unbiased bases existing in dimension $N > 2$ admits the introduction of $(m-1)N/2$ free parameters that cannot be absorbed by a global unitary operation. As consequence, there are $m = k+1$ mutually unbiased bases in every dimension $N = k^2$ with $k^3/2$ free parameters, where k is even. We explicitly construct the maximal set of triplets of mutually unbiased bases for two-qubit systems and triplets, quadruplets, and quintuplets of mutually unbiased bases with free parameters for three-qubit systems. Furthermore, we study the richness of the entanglement structure of such bases and provide the quantum circuits required to implement all these bases with free parameters in the laboratory. We also show that the free parameters introduced can be controlled by a *single* party of the system. Finally, we find the upper bound for the maximal number of real and complex mutually unbiased bases existing in every dimension. This proof is simple, short, and considers basic matrix algebra.

DOI: 10.1103/PhysRevA.92.062325 PACS number(s): 03.67.−a, 03.65.Aa, 03.65.Ud

I. INTRODUCTION

Mutually unbiased bases (MUB) have an important role in quantum mechanics. They are useful in generating quantum key distribution protocols [1–3], detection of entanglement [4], quantum random access codes [5], dense coding, teleportation, entanglement swapping, and covariant cloning (see [6] and references therein). Additionally, a maximal set of MUB allows us to univocally reconstruct quantum states [7]. Furthermore, entropic certainty [8,9] and uncertainty relations [10] have been studied for MUB. Such applications have motivated considerable effort to understand the underlying structure behind incomplete [11,12] and complete [7,13] sets of MUB. In particular, MUB play an important role in locking of classical correlations in quantum states [14–16] and a not-so-well understood role in some Bell inequalities [17]. Despite the important advances done for complete sets of MUB in prime [7] and prime power [13] dimensions, the structure of incomplete sets of MUB is still a mystery even in low prime dimensions. The full classification of MUB for two-qubit systems, i.e., all triplets, quadruplets, and quintuplets of MUB existing in dimension 4, was done in [18]. In dimensions 2, 3, and 5 the problem has a simple solution because of the existence of a unique complex Hadamard matrix up to equivalence, i.e., the Fourier matrix. For every dimension higher than 5 the classification of incomplete sets of MUB is still unknown. Indeed, it is open in the prime dimension seven, which seems to be the simplest open case.

The lack of a deeper understanding of mutually unbiased bases is due to the absence of a suitable mathematical tool to study the problem. Indeed, quadruplets of MUB having free parameters are not known and a few triplets having free parameters were accidentally found [19]. In this work we shed light on this area of research by presenting a systematic method of introducing free parameters in sets of MUB. We demonstrate that any set of m real MUB existing in every dimension $N > 2$ admits the introduction of free parameters. Our construction is not restricted to real sets of MUB. Indeed, we illustrate our method by constructing the maximal set of triplets for two-qubit systems and several triplets, quadruplets, and quintuplets of MUB having free parameters for three-qubit systems. All of these cases involve sets of complex MUB. Furthermore, we analyze the entanglement structure of these sets of MUB and provide the quantum circuits required to implement all the sets in the laboratory.

This work is organized as follows. In Sec. II we present a short introduction to mutually unbiased bases and the link to complex Hadamard matrices and we summarized the state of the art of MUB with free parameters. In Sec. III we present our method of introducing free parameters in sets of MUB. In Sec. IV we prove that any set of m real MUB existing in dimension N admits the introduction of the maximal number of parameters allowed by our method, that is, $(m-1)N/2$ free parameters. In Sec. V we construct triplets, quadruplets, and quintuplets of MUB having free parameters for three-qubit systems and study the entanglement structure of each case. In Sec. VI we summarize our main results, conclude, and discuss some open questions. Additionally, we illustrate our method by constructing triplets of MUB for two-qubit systems (see Appendix A). The explicit construction of a quadruplet and a quintuplet of MUB having free parameters for three-qubit systems is provided in Appendix B. In Appendix C we derive the quantum circuits required to generate every quadruplet

*dgoyeneche@cefop.udec.cl

and quintuplet of MUB presented in this work. Finally, in Appendix D we present a simple and short proof for the upper bound of the maximal number of real and complex MUB in every dimension by considering basic matrix algebra.

II. MUTUALLY UNBIASED BASES AND COMPLEX HADAMARD MATRICES

In this section we present some fundamental properties about MUB and complex Hadamard matrices (CHMs) required to understand the rest of the work. For a complete review about MUB and CHMs we suggest Refs. [6,20], respectively. Two orthonormal bases $\{\phi_j\}_{j=0,\ldots,N-1}$ and $\{\psi_k\}_{k=0,\ldots,N-1}$ defined in $\mathbb{C}^N$ are mutually unbiased if

$$|\langle\phi_j,\psi_k\rangle|^2=\frac{1}{N}, \tag{1}$$

for every $j,k=0,\ldots,N-1$. In general, a set of $m>2$ orthonormal bases is MUB if all the pairs of bases of the set are MUB. A set of m MUB is called extensible if there exists an $(m+1)$th basis that is mutually unbiased with respect to the rest of the bases. It has been shown that $m=N+1$ MUB exist for N prime [7] and prime power [13]. Additionally, maximal sets of MUB can be constructed in prime power dimensions by considering Gaussian sums and finite fields [21–23]. For any other dimension $N=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$ $(p_1^{r_1}<p_2^{r_2}<\cdots<p_k^{r_k})$ the maximal value of m is not known and the lower bound $m\geqslant p_1^{r_1}$ is provided by the maximal number of fully separable (i.e., tensor product) MUB [24]. Additionally, in dimensions of the form $N=k^2$ it is possible to find $m=k+1$ real MUB by considering orthogonal latin squares [25]. Let us arrange the bases $\{\phi_j\}$ and $\{\psi_k\}$ in columns of unitary matrices B_1 and B_2, respectively. If B_1 and B_2 are MUB then

$$B_1^\dagger B_2=H, \tag{2}$$

where H is a complex Hadamard matrix. An $N\times N$ matrix H is called a complex Hadamard matrix if it is unitary and all its complex entries have the same amplitude $1/\sqrt{N}$. For example, the Fourier matrix $(F_N)_{jk}=\frac{1}{\sqrt{N}}e^{2\pi ijk/N}$ is a CHM for every N, where $i=\sqrt{-1}$. Two CHMs H_1 and H_2 are equivalent if there exist permutation matrices P_1 and P_2 and diagonal unitary matrices D_1 and D_2 such that $H_2=P_1D_1H_1D_2P_2$. Therefore, MUB and CHMs are closely related: Any set of m MUB $\mathcal{S}_1=\{B_1,\ldots,B_m\}$ is unitary equivalent to a set $\mathcal{S}_2=\{\mathbb{I},H_1,\ldots,H_{m-1}\}$, where $\mathbb{I}$ represents the computational basis and $H_1,\ldots,H_{m-1}$ are CHMs. Indeed, the unitary transformation that connects $\mathcal{S}_1$ with $\mathcal{S}_2$ is $B_1^\dagger$. That is,

$$\begin{aligned}B_1^\dagger(\mathcal{S}_1)&=\{B_1^\dagger B_1,B_1^\dagger B_2,\ldots,B_1^\dagger B_m\}\\&=\{\mathbb{I},H_1,\ldots,H_{m-1}\}\\&=\mathcal{S}_2,\end{aligned} \tag{3}$$

where we considered Eq. (2). Alternatively, $B_k^\dagger(\mathcal{S}_1)$ also provides an analogous result to (3) for $k=2,\ldots,m$. A CHM H is dephased if its first row and column are composed of 1's. Note that any CHM is equivalent to a dephased CHM. In general, a set of m MUB $\{\mathbb{I},H_1,\ldots,H_{m-1}\}$ is dephased if H_1 is dephased and the resting $m-2$ CHMs have 1's in the first row. Furthermore, two sets of m MUB $\mathcal{S}_1$ and $\mathcal{S}_2$ are equivalent if there exist permutations P_1, P_2, and $\mathcal{P}$ and diagonal unitaries D_1 and D_2 such that $\mathcal{S}_2=\mathcal{P}[P_1D_1\mathcal{S}_1D_2P_2]$. Here $\mathcal{P}[\,]$ denotes a suitable permutation of entries of the vector of matrices $\{\mathbb{I},H_1,\ldots,H_{m-1}\}$. In this way, any set of m MUB can be written in a nonunique dephased form.

The full classification of CHMs and MUB has been solved up to dimension $N=5$ (see [26] and [18], respectively). For $N=6$ both problems remain open despite considerable effort made during the past 20 years [12,27–35]. Both problems of CHMs and MUB also remain open for any dimension $N>6$. For example, they are open in the prime dimension $N=7$, where a single one-parameter family of complex Hadamard matrices is known [36] and a maximal set of eight MUB is known [7] but incomplete sets of MUB are not yet characterized. Indeed, it is still an open question whether a triplet of MUB having free parameters exists in dimension $N=7$.

Let us summarize the state of the art for MUB with free parameters. First, any set of m MUB in prime dimension $N=p$ of the form $\{\mathbb{I},F_p,C_1,\ldots,C_{m-2}\}$ is isolated, where F_p is the Fourier matrix and $\{C_1,\ldots,C_{m-2}\}$ are circulant CHMs [37]. A complex Hadamard matrix is isolated if there is no family of CHMs connected with it [20]. A family of CHMs is a set of inequivalent complex Hadamard matrices depending on some free real parameters. We extend the same definition to sets of MUB: A set of m MUB is isolated if there is no family of m MUB connected with it. For example, any set of $m\leqslant N+1$ MUB in dimensions $N=2,3,5$ is isolated. In dimension $N=4$ there is a unique three-parameter triplet of MUB of the form $\{\mathbb{I},F_4^{(1)}(x),H(y,z)\}$ and quadruplets and quintuplets of MUB are isolated [18]. In dimension $N=6$ a one-parameter triplet of MUB exists [27]. Moreover, two-parameter triplets of the form $\{\mathbb{I},F_6^{(2)}(x,y),H(x,y)\}$ exist for any $x,y\in[0,2\pi)$ and seem to be unextendible for any pair x,y [12,29]. Furthermore, in dimensions $N=9$ [38] and $N=4k$ [19] one-parameter triplets of MUB can be defined by considering cyclic n roots.

All the above sets of MUB with free parameters were found by taking advantage of special properties holding in specific dimensions. So far, the existence of quadruplets of MUB having free parameters is still unknown in every dimension. In the next section we present a systematic method to introduce free parameters in sets of m MUB in dimension N.

III. MUB WITH FREE PARAMETERS

A set of $r>N$ vectors $\{v_k\}\subset\mathbb{C}^N$ is associated with a Gram matrix $G\in\mathbb{C}^{r\times r}$, where $G_{ij}=\langle v_i,v_j\rangle$; $i,j=0,\ldots,r-1$; and rank $\mathcal{R}(G)=N$. Also, from a Gram matrix G of size $r>N$ and rank N we can find a set of vectors $v_k'\in\mathbb{C}^N$ such that $G_{ij}=\langle v_i',v_j'\rangle$. Two sets of vectors $\{v_k\}$ and $\{v_k'\}$ associated with the same G can be connected by a unitary transformation. That is, both sets of vectors $\{v_k\}$ and $\{v_k'\}$ define the same geometrical structure in the complex projective space $\mathbf{CP}^{N-1}$. The vectors $\{v_k'\}$ can be found from G by considering the Cholesky decomposition, i.e., to find the unique upper triangular matrix L having positive diagonal entries such that $G=L^\dagger L$. Thus, the r vectors $\{v_k'\}$ are given by the r columns of L, where we only have to consider entries of the first N rows of L (the rest of the rows have zero entries because of

the rank restriction). In this work we are particularly interested in studying Gram matrices associated with a set of m MUB $\{\mathbb{I}, H_1, H_2, \ldots, H_{m-1}\}$ in $\mathbb{C}^N$. That is,

$$G = \begin{pmatrix} \mathbb{I} & H_1 & H_2 & \cdots & H_{m-1} \\ H_1^\dagger & \mathbb{I} & H_1^\dagger H_2 & \cdots & H_1^\dagger H_{m-1} \\ H_2^\dagger & H_2^\dagger H_1 & \mathbb{I} & \cdots & H_2^\dagger H_{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ H_{m-1}^\dagger & H_{m-1}^\dagger H_1 & H_{m-1}^\dagger H_2 & \cdots & \mathbb{I} \end{pmatrix}. \tag{4}$$

Note that this $mN \times mN$ Gram matrix G naturally defines a structure of m^2 square blocks of size N, each of them defined by a unitary matrix of the form $H_i^\dagger H_j$, where $i, j = 0, \ldots, m-1$ and $H_0 = \mathbb{I}$. The Cholesky decomposition of this Gram matrix G is given by

$$L = \begin{pmatrix} \mathbb{I} & H_1 & H_2 & \cdots & H_{m-1} \\ 0_N & 0_N & 0_N & \cdots & 0_N \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0_N & 0_N & 0_N & \cdots & 0_N \end{pmatrix}, \tag{5}$$

where 0_N is the zero matrix of size N. So the set of m MUB is clearly given by $\{\mathbb{I}, H_1, H_2, \ldots, H_{m-1}\}$, which corresponds to the first block of rows of G [see Eq. (4)]. As we will show later, this property considerably simplifies the use of our method.

In previous work [39] we found the most general way to introduce free parameters in pairs of columns (or rows) of any complex Hadamard matrix. In every dimension $N > 2$ a free parameter can be introduced in two columns C_1 and C_2 of a CHM if and only if $C_1 \circ C_2 \in \mathbb{R}^{\mathbb{N}}$. Here the circle denotes the (entrywise) Hadamard product, that is, $(C_1 \circ C_2)_j = (C_1)_j (C_2)_j$, $j = 0, \ldots, N-1$. Pairs of columns (or rows) satisfying this property were called equivalent to real (ER) pairs [39]. It is immediately realized that ER pairs only exist for even dimensions. Consequently, a family of CHMs existing in odd dimension N cannot have a free parameter appearing in only in two columns. The introduction of free parameters in ER pairs is very simple.

Construction 1. Given an ER pair of columns $\{C_1, C_2\}$, we introduce a free phase $e^{i\alpha}$ in the jth entries $(C_1)_j$ and $(C_2)_j$ if $(C_1^* \circ C_2)_j < 0$ for $j = 0, \ldots, N-1$ [39].

Here the asterisk denotes complex conjugation. Note that $\sum_{j=0}^{N-1} (C_1^* \circ C_2)_j$ is the inner product between the column vectors C_1 and C_2, which has to be zero by definition of CHMs. Let us exemplify this method by introducing two free parameters in the Fourier matrix

$$F_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}. \tag{6}$$

That is,

$$F_4(\alpha, \beta) = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1e^{i\alpha} & ie^{i\beta} & -1e^{i\alpha} & -ie^{i\beta} \\ 1 & -1 & 1 & -1 \\ 1e^{i\alpha} & -ie^{i\beta} & -1e^{i\alpha} & ie^{i\beta} \end{pmatrix}. \tag{7}$$

Here we consider the ER pairs of columns $\{C_1, C_3\}$ and $\{C_2, C_4\}$ to introduce the parameters α and β, respectively. Note that α and β are aligned along the second and fourth rows in Eq. (7). A set of $N/2$ ER pairs producing aligned free parameters in matrices of size N are called aligned ER pairs. Aligned ER pairs have one of the parameters linearly dependent (if we consider the equivalence of CHMs defined above). Thus, the parameter β of Eq. (7) is linearly dependent and thus the Fourier family in dimension 4 has only one relevant parameter [20]. In the same way, some new families of CHMs have been defined [39].

Let us now extend this method to the construction of MUB with free parameters. Here the key ingredient is the generalization of the concept of ER pairs: A set of two columns $\{C_1, C_2\}$ of a Gram matrix G associated with m MUB in dimension N is called a generalized ER (GER) pair if $C_1 \circ C_2 \in \mathbb{R}^{mN}$. The following result, natural generalization of Construction 1, is the main result of the present work.

Proposition 1. Let G be the Gram matrix of a set of m MUB in dimension N and suppose that it has $\mathcal{N}$ GER pair of columns such that both vectors of each GER pair belong to the same block of columns. Then the set of m MUB admits the introduction of $\mathcal{N}$ free parameters.

Proof. For simplicity, let us first consider the case of 3 MUB ($m = 3$) in dimension N, where the Gram matrix is given by

$$G = \begin{pmatrix} \mathbb{I} & \mathbf{H_1} & H_2 \\ H_1^\dagger & \mathbf{I} & H_1^\dagger H_2 \\ H_2^\dagger & \mathbf{H_2^\dagger H_1} & \mathbb{I} \end{pmatrix}, \tag{8}$$

and suppose that G has a GER pair of columns $\{C_i, C_j\}$ defined within a block of columns (i.e., $\mathcal{I}[i/N] = \mathcal{I}[j/N]$, where $\mathcal{I}$ means integer part). Therefore, N of the products $(C_i)_k (C_j)_k$ are zero because of the corresponding identity block $\mathbb{I}$ and only $2N$ values of these products play a role in $C_i \circ C_j$. Thus, a free parameter can be introduced in both columns C_i and C_j by applying Construction 1 to the $2N$-dimensional subvectors of C_i and C_j having $2N$ nonzero entries. Note that after introducing the parameter the Hermiticity of the Gram matrix G is destroyed. In order to restore the Hermiticity we apply the same method to the GER pairs of rows $\{R_i, R_j\}$, which exists because G is a Hermitian matrix. We remark that the same free parameter should be considered in both GER pairs $\{C_i, C_j\}$ and $\{R_i, R_j\}$. Otherwise, the resulting matrix would be not Hermitian. For further clarifications see the explicit example provided in Appendix A. Therefore, the above construction leads us to a one-parameter set of matrices satisfying (i) $G(\alpha) = U(\alpha) G U^\dagger(\alpha)$ and (ii) $|G(\alpha)_{ij}| = |G_{ij}|$ for any $\alpha \in [0, 2\pi)$. Note that (i) holds for any unitary matrix U whereas (ii) is strongly dependent on our construction. Here $U(\alpha)$ and $U^\dagger(\alpha)$ represent the introduction of the free parameter α in two columns and two rows, respectively. Furthermore, $G(\alpha)$ and $G(0)$ have the same eigenvalues for any $\alpha \in [0, 2\pi)$ and consequently $G(\alpha)$ is a one-parameter set of Gram matrices defining a one-parameter set of m MUB in dimension N. Furthermore, the explicit dependence on α in the Gram matrix G implies that the parameter cannot be absorbed by a global unitary operation acting on all the vectors. Additionally, the parameter does not appear in every entry of a row or column, which implies that α cannot be absorbed as a global phase of a vector. Finally, if G has $\mathcal{N}$ GER pairs, then we can introduce $\mathcal{N}$ free parameters in the same way. The

generalization to any set of $m > 3$ MUB is straightforward from the above explanation. ■

Let us emphasize the importance of considering both vectors of the GER pairs in the same block of columns: Suppose that we choose a GER pair formed by two columns belonging to different blocks [e.g., the fifth and ninth columns of the Gram matrix given in the example (A4)] and we introduce a free parameter. Despite this action generating a genuine Gram matrix, the set of three bases would be *not* composed of MUB with free parameters. This is simple to understand because the free parameter would appear in a single vector of the second and third bases. In this way, for $\alpha \neq 0$ we would not have orthonormal bases.

In the particular case of $m = 2$ our Proposition 1 is reduced to Construction 1, which was derived in a previous work [39]. That is, introducing free parameters in a pair of MUB is equivalent to introducing free parameters in a CHM, as suggested by Eq. (3). The explicit construction of the maximal set of triplets of MUB for two-qubit systems is shown in Appendix A. Also, a triplet, a quadruplet and a quintuplet of MUB having free parameters for three-qubit systems are given in Appendix B. We encourage to the reader to have a close look at the examples in order to have a clear understanding of our method.

IV. FAMILIES STEMMING FROM REAL MUB

As we have shown, Proposition 1 allows us to introduce free parameters in Gram matrices of MUB having GER pairs. In this section we demonstrate that any set of m real MUB existing in dimension $N > 2$ allows the introduction of the maximal number of parameters allowed by GER pairs.

Proposition 2. Any set of m real MUB in dimension $N > 2$ admit the introduction of $Nm/2$ free parameters. Furthermore, $(m-1)N/2$ of these parameters cannot be absorbed by global unitary transformations and at most one of them is linearly dependent.

Proof. Every pair of columns belonging to the same block is clearly a GER pair. Therefore, there are $Nm/2$ GER pairs allowing the introduction of $Nm/2$ free parameters. The rest of the proof is straightforward (already explained in the proof of Proposition 1). ■

Furthermore, note that there are many different ways to choose the GER pairs and consequently many sets of MUB with free parameters can be constructed. Precisely, there are $\binom{N}{2}$ different ways to choose GER pairs in each of the $m-1$ blocks of columns (the first block only provides unitary equivalent MUB), that is, a total of $(m-1)N(N-1)/2$ different ways. We do not know how many ways are inequivalent for $N > 4$. For $N = 4$ the answer is provided in Ref. [18]. In dimensions of the form $N = k^2$ it is possible to construct $m = k+1$ real MUB for every $k \in \mathbb{N}$. By combining this result with Proposition 2 we have the following result.

Corollary 1. In every dimension $N = k^2$ there exist $m = k+1$ MUB admitting $k^3/2$ free parameters.

In dimension $N = 4$ there exist $m = 3$ real MUB and then we can introduce $k^3/2 = 4$ free parameters, where the GER pairs are aligned; so one of the four parameters is linearly dependent (see Appendix A). Here the 12 possible ways to introduce free parameters produce equivalent sets [18]. These triplets are also equivalent to the solution found in Appendix A with our method. Sets of real MUB are not the only cases where a maximal number of parameters can be introduced. In the next section we construct sets of MUB with free parameters in the three-qubit space by considering complex MUB.

V. MUB FOR THE THREE-QUBIT SPACE

For three-qubit systems ($N = 2^3$) there is a maximal number of $N+1 = 9$ MUB. Indeed, four maximal sets having a different entanglement structure have been constructed [21]:

$$\mathcal{S}_1 = (2,3,4), \quad \mathcal{S}_2 = (1,6,2),$$
$$\mathcal{S}_3 = (0,9,0), \quad \mathcal{S}_4 = (3,0,6), \tag{9}$$

where the first, second, and third entries denote the number of fully separable, biseparable, and maximally entangled bases, respectively. These sets of MUB are not equivalent under Clifford operations, but they are equivalent under general unitary transformations. In this section we construct pairs, triplets, quadruplets, and quintuplets of MUB having free parameters from considering subsets of $\mathcal{S}_4$. We have chosen this particular set of MUB because it contains the highest number of maximally entangled bases and consequently it has potentially important applications in quantum information theory.

From considering Proposition 1 we find the following results for every subset of $m \leqslant 9$ MUB of $\mathcal{S}_4$ (three qubits).

(i) Every pair of MUB $\{\mathbb{I}, H_i\} \subset \mathcal{S}_4$ admits the introduction of four free parameters, where $i = 1, \ldots, 8$. This is equivalent to introducing free parameters in the CHM H_i.

(ii) Every triplet of MUB $\{\mathbb{I}, H_i, H_j\} \subset \mathcal{S}_4$ admits the introduction of eight free parameters for every $i \neq j = 1, \ldots, 8$.

(iii) Some quadruplets of MUB $\{\mathbb{I}, H_j, H_k, H_l\} \subset \mathcal{S}_4$ admit the introduction of four free parameters in *only one* of the bases, whereas the rest of the quadruplets do not admit free parameters.

(iv) Every quadruplet admitting four free parameters can be extended to a quintuplet of MUB having four free parameters. The extension of quadruplets to quintuplets is not unique.

(v) Every set of $6 \leqslant m \leqslant 9$ MUB does not admit free parameters.

The maximal number of parameters that can be introduced for every m is provided in Table I. Furthermore, the con-

TABLE I. MUB with free parameters in dimension $N = 8$. The asterisk means that GER pairs are aligned, which produces one linearly dependent parameter. Note that a set of MUB in general allows many different choices for GER pairs and some of them produce nonaligned GER pairs. In Appendix B we explain in detail all possible sets of m MUB having free parameters.

No. of MUB (m)	No. of parameters	Example
2	3	$\{\mathbb{I}, H_1\}^*$
2	4	$\{\mathbb{I}, H_1\}$
3	7	$\{\mathbb{I}, H_1, H_2\}^*$
3	8	$\{\mathbb{I}, H_1, H_2\}$
4	4	$\{\mathbb{I}, H_1, H_2, H_3\}$
5	0	$\{\mathbb{I}, H_1, H_2, H_3, H_4\}$
5	4	$\{\mathbb{I}, H_1, H_2, H_3, H_5\}^*$
6–9	0	$\{\mathbb{I}, H_i, H_j, H_k, H_l, H_m\}$

struction of every set of MUB for three qubits systems arises from Table II of Appendix B, where we present the proof of the above results. The free parameters of all quadruplets and quintuplets of MUB described in (iii) and (iv) can be generated in the laboratory by considering 7 different quantum circuits (56 cases, 8 cases per circuit; see Appendix C), which involve local, CNOT, and Toffoli gates. The generation of the fixed set of bases, i.e., the set $\mathcal{S}_4$, requires a different circuit [40] that involves local, nonlocal controlled-phase, and Toffoli gates [41]. Therefore, the sets of MUB with free parameters are generated by a composition of two different quantum circuits, which are realizable with current technology. The explicit expression of the quantum circuits is provided in Appendix C.

The sets of MUB presented above have a rich entanglement structure. For example, let us consider the quintuplet of MUB $\{\mathbb{I}, H_1(\alpha), H_2, H_3, H_5\} \subset \mathcal{S}_4$ (explicitly constructed in Appendix B). For simplicity, let us assume that the four parameters $\alpha_1, \ldots, \alpha_4$ are identical (α). Here $H_1(0)$ is a maximally entangled basis, in the sense that every vector of the basis is equivalent, up to local unitary operations, to the Greenberger-Horne-Zeilinger state $|\mathrm{GHZ}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$. On the other hand, $H_1(\pi/2)$ is a biseparable basis. Indeed, every vector of the basis is equivalent to $|\phi\rangle = |0\rangle(|00\rangle + |11\rangle)/\sqrt{2}$. That is, Alice is separated and Bob and Charlie share a maximally entangled Bell state. For any $0 < \alpha < \pi/2$ we have an intermediate amount of entanglement shared between Alice and Bob-Charlie, whereas Bob and Charlie are as entangled as they can be for any α. That is, two of the three parties (Bob and Charlie) saturate the maximal amount of entanglement allowed by the monogamy of entanglement principle [42]. Indeed, for any value of the parameter α the single-qubit reductions ρ_B and ρ_C are maximally mixed. It is highly nontrivial that the bases $H_1(0)$ (maximally entangled) and $H_1(\pi/2)$ (fully separable) can be continuously connected without losing the unbiasedness of the quintuplet of MUB $\{\mathbb{I}, H_1(\alpha), H_2, H_3, H_5\}$ for any value $\alpha \in [0, \pi/2)$. In Appendix C we show that, in this case, the parameter α is fully controlled by a local unitary operation applied by Bob (see quantum circuit G). This means that Bob can control the entanglement existing between Alice and Bob-Charlie. Of course, this quantum circuit is also composed of nonlocal gates but the remarkable property is that the parameter α can be locally controlled (by Bob) in a simple way. Table III in Appendix C shows all possible entanglement structures that can be found from quadruplets and quintuplets with free parameters arising from $\mathcal{S}_4$. The purity of the reductions ρ_A, ρ_B, and ρ_C as a function of the free parameter α for the above quintuplet is depicted in Fig. 1.

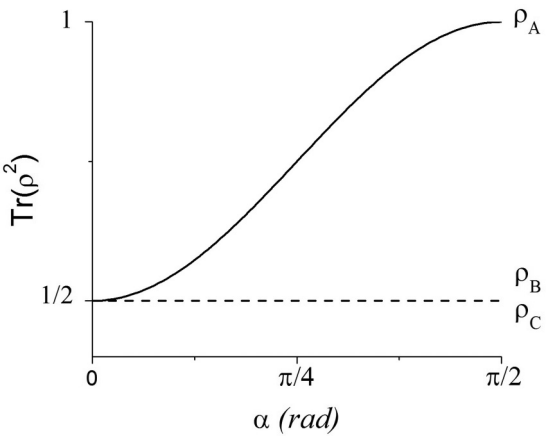


FIG. 1. Purity of the reductions to Alice (ρ_A), Bob (ρ_B), and Charlie (ρ_C) for all the states of the basis $H_1(\alpha)$. Here Bob and Charlie are as entangled as they can be for any value of α (dashed line), whereas Alice is maximally entangled with Bob and Charlie for $\alpha = 0$ (the GHZ state) and separated for $\alpha = \pi/2$ (solid line). For $\alpha = \pi/2$ Bob and Charlie share a Bell state.

VI. CONCLUSION

We have presented a systematic way of introducing free parameters in sets of m mutually unbiased bases in dimension N (see Proposition 1). In particular, for $m = 2$ our method is reduced to the introduction of free parameters in a complex Hadamard matrix (see Construction 1 and Ref. [39]). We proved that any set of m real mutually unbiased bases existing in any dimension $N > 2$ admits the introduction of free parameters (see Proposition 2). As consequence, in every dimension $N = k^2$ there are $k + 1$ MUB with $kN/2$ free parameters, where k is even (see Corollary 1). We have found the maximal set of triplets of MUB with free parameters for two-qubit systems (see Appendix A). Also, we constructed pairs, triplets, quadruplets, and quintuples of MUB having free parameters for three-qubit systems (see Appendix B). Such sets are constructed from subsets of the maximal set of MUB $\mathcal{S}_4$ [see Eq. (9)]. Additionally, we provided the complete set of quantum circuits required to implement all such quadruplets and quintuplets in the laboratory (see Appendix C). Interestingly, the free parameters introduced can be locally controlled by a single party. Finally, we presented a short and simple proof for the upper bound on the maximal number of real and complex mutually unbiased bases existing in every dimension (see Appendix D).

Finally, we present some open issues: (i) finding a triplet of MUB having a free parameter in dimension 7, (ii) finding the subset of triplets, quadruplets, and quintuplets of MUB considered in Appendix C such that they are extendible to nine MUB, (iii) whether it is possible to construct maximal sets of MUB with free parameters in some dimension $N > 8$ (this question may have a negative answer for every N but a formal proof is only known for $N \leqslant 5$ [18]), and (iv) constructing MUB with free parameters for four-qubit systems.

ACKNOWLEDGMENTS

We thank Luis Sanchez Soto and Markus Grassl for fruitful discussions and Joel Tropp for his comments concerning rank inequalities and the Hadamard product. We also thank the Max Planck Institute for the Science of Light, where part of this work was done. D.G. is also thankful to Paweł Horodecki for hospitality during his stay in Sopot, where this project was finished. This work was supported by FONDECyT Scholarship No. 3120066, PIA-CONICYT PFB0824, ICM P10-030-F, Millennium Scientific Initiative Grant No. RC130001 (Chile), and the ERC Advanced Grant QOLAPS coordinated by Ryszard Horodecki (Poland) and the Grant DEC-2011/02/A/ST1/00119 of the Polish National Centre of Science.

APPENDIX A: MUB FOR TWO QUBITS

Let us consider the simplest case where our method can be applied. In dimensions $N = 2$ (one qubit) and $N = 3$ (one qutrit) complex Hadamard matrices are isolated and consequently any set of MUB in such dimensions is isolated. On the other hand, in dimension 4 there is a family of CHMs [see Eq. (7)]. So the simplest case to introduce free parameters corresponds to $N = 4$ (i.e., two-qubit systems). The construction of $m = 2$ MUB having free parameters is reduced to find a family of CHMs and thus here we consider $m = 3$. A fixed triplet of MUB for $N = 4$ is given by the columns of the following matrices:

$$H_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{A1}$$

$$H_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & i & -i \\ 1 & -1 & -i & i \end{pmatrix}, \tag{A2}$$

$$H_3 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix}. \tag{A3}$$

The Gram matrix G associated with this set is given by $1/2$ of the matrix

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 0 & 0 & 2 & 0 & 1 & -1 & i & -i & -1 & 1 & 1 & -1 \\ 0 & 0 & 0 & 2 & 1 & -1 & -i & i & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 0 & 2 & 0 & 0 & 1 & 1 & -1 & 1 \\ 1 & -1 & -i & i & 0 & 0 & 2 & 0 & i & -i & 1 & 1 \\ 1 & -1 & i & -i & 0 & 0 & 0 & 2 & -i & i & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -i & i & 2 & 0 & 0 & 0 \\ 1 & 1 & 1 & -1 & 1 & 1 & i & -i & 0 & 2 & 0 & 0 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 0 & 0 & 2 & 0 \\ 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 0 & 0 & 0 & 2 \end{pmatrix}. \tag{A4}$$

Here we have six GER pairs of columns and rows given by {1-2;3-4;5-6;7-8;9-10;11-12}. Note that the perfect match between GER pairs of columns and rows is due to the fact that G is Hermitian. The introduction of free parameters into the GER pairs $\{C_1, C_2; C_3, C_4\}$ produces equivalent sets. From considering the remaining four GER pairs defined above we easily generate the following MUB with free parameters:

$$H_2(\alpha,\beta) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ e^{i\alpha} & -e^{i\alpha} & ie^{i\beta} & -ie^{i\beta} \\ e^{i\alpha} & -e^{i\alpha} & -ie^{i\beta} & ie^{i\beta} \end{pmatrix}, \tag{A5}$$

and

$$H_3(\gamma,\delta) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -e^{i\gamma} & e^{i\gamma} & e^{i\delta} & -e^{i\delta} \\ e^{i\gamma} & -e^{i\gamma} & e^{i\delta} & -e^{i\delta} \end{pmatrix}. \tag{A6}$$

Note that our method can be considerably simplified by introducing the free parameters in a reduced region of the Gram matrix (A4). This is because G contains much more information than the set of three MUB [see Eq. (5)]. Precisely, we can restrict our attention to introducing free parameters in the first four rows of G in Eq. (A4) according to the existing pairs of GER and Proposition 1. The rest of the rows give us the explicit expression of the inner products between the elements of the different bases, which is not interesting for our purpose. In general, we can restrict our attention to introducing parameters in the first N rows of G when we consider m MUB in dimension N.

The four parameters $\alpha,\beta,\gamma,\delta$ appearing in Eqs. (A5) and (A6) cannot be absorbed by global unitary operations. However, they are aligned, so one of them can be absorbed in a global phase of a vector of the canonical basis H_1. Therefore, we find the following three-parameter triplet of MUB in dimension $N = 4$:

$$\{\mathbb{I}, H_2(\alpha,0), H_3(\gamma,\delta)\}. \tag{A7}$$

This result has been reported as the most general triplet of MUB that can be constructed in dimension $N = 4$ [18]. Quadruplets and quintuplets of MUB do not allow free parameters in dimension 4. Indeed, quadruplets and quintuplets are isolated [18].

TABLE II. GER pairs required to construct any subset of m MUB stemming from the maximal set of nine MUB $\mathcal{S}_4$.

	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8
$H_1^\dagger$		1-3-4-8;2-5-6-7	1-4-5-7;2-3-6-8	1-2-4-7;3-5-6-8	1-4-5-6;2-3-7-8	1-6-7-8;2-3-4-5	1-2-3-7;4-5-6-8	1-2-5-8;3-4-6-7
$H_2^\dagger$	1-2-5-8;3-4-6-7		1-3-4-8;2-5-6-7	1-2-3-6;4-5-7-8	1-2-5-8;3-4-6-7	1-2-5-8;3-4-6-7	1-4-5-7;2-3-6-8	1-2-4-6;3-5-7-8
$H_3^\dagger$	1-2-4-7;3-5-6-8	1-6-7-8;2-3-4-5		1-4-5-6;2-3-7-8	1-6-7-8;2-3-4-5	1-3-4-8;2-5-6-7	1-2-4-8;3-5-6-7	1-3-4-8;2-5-6-7
$H_4^\dagger$	1-3-5-7;2-4-6-8	1-4-5-7;2-3-6-8	1-2-4-6;3-5-7-8		1-2-3-6;4-5-7-8	1-4-5-6;2-3-7-8	1-3-5-8;2-4-6-7	1-4-5-7;2-3-6-8
$H_5^\dagger$	1-2-3-6;4-5-7-8	1-2-4-6;3-5-7-8	1-2-5-8;3-4-6-7	1-3-5-7;2-4-6-8		1-3-5-7;2-4-6-8	1-6-7-8;2-3-4-5	1-6-7-8;2-3-4-5
$H_6^\dagger$	1-3-4-8;2-5-6-7	1-2-3-7;4-5-6-8	1-3-5-6;2-4-7-8	1-2-5-8;3-4-6-7	1-3-4-8;2-5-6-7		1-2-5-6;3-4-7-8	1-3-5-6;2-4-7-8
$H_7^\dagger$	1-6-7-8;2-3-4-5	1-2-5-8;3-4-6-7	1-6-7-8;2-3-4-5	1-6-7-8;2-3-4-5	1-2-4-7;3-5-6-8	1-2-3-6;4-5-7-8		1-2-3-7;4-5-6-8
$H_8^\dagger$	1-4-5-6;2-3-7-8	1-3-5-6;2-4-7-8	1-2-3-7;4-5-6-8	1-3-4-8;2-5-6-7	1-3-5-7;2-4-6-8	1-2-4-7;3-5-6-8	1-3-4-6;2-5-7-8	

APPENDIX B: MUB FOR THREE QUBITS

In this appendix we construct the maximal number of triplets, quadruplets, and quintuplets of MUB having free parameters that can be constructed from subsets of $\mathcal{S}_4$ [see Eq. (9)]. The key result is provided in Table II, where we present the complete set of GER pairs for $\mathcal{S}_4$. This is how to read Table II.

(i) The cell associated with column H_k and row $H_j^\dagger$ contains all the GER pairs allowed by the triplet $\{\mathbb{I}, H_j, H_k\}$.

(ii) The notation i-j-k-l means that every possible combination of two nonrepeated indices determines a GER pair, that is, $\{C_i,C_j\}$, $\{C_i,C_k\}$, $\{C_i,C_l\}$, $\{C_j,C_k\}$, $\{C_j,C_l\}$, and $\{C_k,C_l\}$ are GER pairs. By convention, we consider $1 \leqslant i < j < k < l \leqslant 8$.

(iii) The semicolon separates complementary sets of GER pairs (e.g., for $\{i$-j-k-l; μ-ν-κ-$\eta\}$ a mixture of greek and latin indices *does not* form a GER pair).

To construct quadruplets or quintuplets of MUB we have to find the intersection of sets of GER pairs allowed by all the subsets of triplets. If there is no intersection then free parameters cannot be introduced. Let us construct a triplet of MUB by following the above rules (i)–(v): Suppose that we want to introduce free parameters in the triplet $\{H_1, H_2, H_3\}$ [see Eq. (8)]. In order to introduce free parameters in H_1 we have to find common GER pairs in the cells associated with $H_2^\dagger H_1$ (i.e., column 2, row 3 of Table II: {1-2-5-8;3-4-6-7}) and $H_3^\dagger H_1$ (i.e., column 2, row 4: {1-2-4-7;3-5-6-8}). This is equivalent to finding GER pairs appearing in the Gram matrix of $\{H_1, H_2, H_3\}$. Thus, the unique set of common GER pairs is given by $\{C_1,C_2\}$, $\{C_3,C_6\}$, $\{C_4,C_7\}$, and $\{C_5,C_8\}$. Analogously, we can find the GER pairs for the second and third blocks of G, that is, $\{C_1,C_8\}$,$\{C_2,C_5\}$,$\{C_3,C_4\}$,$\{C_6,C_7\}$ and $\{C_1,C_4\}$,$\{C_2,C_6\}$,$\{C_3,C_8\}$,$\{C_5,C_7\}$, respectively. Thus, we have the conditions to introduce 12 free parameters in the Gram matrix of the fixed set $\{H_1, H_2, H_3\}$. As noted in Appendix A, the Cholesky decomposition allows us to simplify the introduction of free parameters by only considering the first N rows of G. Our 12-parameter set of $m = 3$ MUB is given by

$$H_1(\alpha_1,\alpha_2,\alpha_3,\alpha_4) = \begin{pmatrix} -i & -i & i & i & -i & i & i & -i \\ -i & -i & -i & i & i & -i & i & i \\ -ie^{i\alpha_1} & ie^{i\alpha_1} & ie^{i\alpha_2} & -ie^{i\alpha_3} & -ie^{i\alpha_4} & -ie^{i\alpha_2} & ie^{i\alpha_3} & ie^{i\alpha_4} \\ ie^{i\alpha_1} & -ie^{i\alpha_1} & ie^{i\alpha_2} & ie^{i\alpha_3} & -ie^{i\alpha_4} & -ie^{i\alpha_2} & -ie^{i\alpha_3} & ie^{i\alpha_4} \\ e^{i\alpha_1} & -e^{i\alpha_1} & -e^{i\alpha_2} & -e^{i\alpha_3} & -e^{i\alpha_4} & e^{i\alpha_2} & e^{i\alpha_3} & e^{i\alpha_4} \\ e^{i\alpha_1} & -e^{i\alpha_1} & e^{i\alpha_2} & -e^{i\alpha_3} & -e^{i\alpha_4} & e^{i\alpha_2} & e^{i\alpha_3} & -e^{i\alpha_4} \\ -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \tag{B1}$$

$$H_2(\beta_1,\beta_2,\beta_3,\beta_4) = \begin{pmatrix} -1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -ie^{i\beta_1} & -ie^{i\beta_2} & -ie^{i\beta_3} & ie^{i\beta_3} & ie^{i\beta_2} & ie^{i\beta_4} & -ie^{i\beta_4} & ie^{i\beta_1} \\ -i & i & i & i & i & -i & -i & -i \\ -e^{i\beta_1} & -e^{i\beta_2} & e^{i\beta_3} & -e^{i\beta_3} & e^{i\beta_2} & -e^{i\beta_4} & e^{i\beta_4} & e^{i\beta_1} \\ -e^{i\beta_1} & e^{i\beta_2} & e^{i\beta_3} & -e^{i\beta_3} & -e^{i\beta_2} & e^{i\beta_4} & -e^{i\beta_4} & e^{i\beta_1} \\ -i & -i & i & i & -i & i & i & -i \\ ie^{i\beta_1} & -ie^{i\beta_2} & ie^{i\beta_3} & -ie^{i\beta_3} & ie^{i\beta_2} & ie^{i\beta_4} & -ie^{i\beta_4} & -ie^{i\beta_1} \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \tag{B2}$$

and

$$H_3(\gamma_1,\gamma_2,\gamma_3,\gamma_4) = \begin{pmatrix} ie^{i\gamma_1} & ie^{i\gamma_2} & ie^{i\gamma_3} & -ie^{i\gamma_1} & -ie^{i\gamma_4} & -ie^{i\gamma_2} & ie^{i\gamma_4} & -ie^{i\gamma_3} \\ -e^{i\gamma_1} & e^{i\gamma_2} & e^{i\gamma_3} & e^{i\gamma_1} & e^{i\gamma_4} & -e^{i\gamma_2} & -e^{i\gamma_4} & -e^{i\gamma_3} \\ -1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -i & -i & i & -i & i & -i & i & i \\ -e^{i\gamma_1} & -e^{i\gamma_2} & e^{i\gamma_3} & e^{i\gamma_1} & -e^{i\gamma_4} & e^{i\gamma_2} & e^{i\gamma_4} & -e^{i\gamma_3} \\ -ie^{i\gamma_1} & ie^{i\gamma_2} & -ie^{i\gamma_3} & ie^{i\gamma_1} & -ie^{i\gamma_4} & -ie^{i\gamma_2} & ie^{i\gamma_4} & ie^{i\gamma_3} \\ -i & i & i & -i & -i & i & -i & i \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{B3}$$

Here only eight parameters are relevant because four of them do not appear in the inner products and thus they can be absorbed by a unitary transformation applied to the entire set of vectors of the MUB. That is, the α, β, or γ can be considered as zero without loss of generality. Moreover, given that the parameters are aligned, we have seven independent parameters. This triplet can be straightforwardly extended to a quadruplet of MUB by adding the computational basis $H_9 \in \mathcal{S}_4$. In order to construct a quintuplet we have to find a suitable fifth basis. One way to do this is by considering H_5 (see Table II). For this choice we have a nonempty set of GERs and four parameters can be introduced in H_1 (see Table II, the column starting with H_1). The remaining four bases $\mathbb{I}$, H_2, H_3, and H_5 are fixed, where $H_2 = H_2(0,0,0,0)$, $H_3 = H_3(0,0,0,0)$, and H_5 is given by

$$H_5 = \begin{pmatrix} 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -i & -i & -i & i & i & -i & i & i \\ -i & -i & i & i & -i & i & i & -i \\ i & -i & -i & -i & -i & i & i & i \\ -i & i & -i & i & -i & i & -i & i \\ -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{B4}$$

We encourage the reader to verify that there is no intersection between the set of GER pairs for H_2, H_3, and H_5 (see Table II) and consequently no more free parameters can be introduced. Therefore, the four-parameter quintuplet is given by

$$\{\mathbb{I}, H_1(\alpha_1,\alpha_2,\alpha_3,\alpha_4), H_2, H_3, H_5\}. \tag{B5}$$

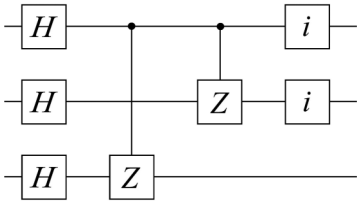


FIG. 2. Quantum circuit required to construct the fixed set of nine MUB $\mathcal{S}_4$ [40].

APPENDIX C: QUANTUM CIRCUITS FOR QUADRUPLETS AND QUINTUPLETS OF MUB

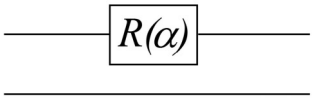
Every quadruplet and quintuplet of MUB with free parameters for three-qubit systems has been generated from considering subsets of $\mathcal{S}_4$ [see Eq. (9)]. These subsets can be implemented in the laboratory by considering suitable quantum circuits that can be implemented with current technology. First, we have to consider the generation of the fixed bases (subset of $\mathcal{S}_4$) and then the introduction of the free parameters. Therefore, the full quantum circuit is the composition of two different circuits. The generation of the set $\mathcal{S}_4$ is given by the quantum circuit depicted in Fig. 2. This circuit was recently derived [40]. The free parameters can be introduced by considering one of the seven quantum circuits shown below (A–G). Table III shows the quantum circuit required to generate every quadruplet and quintuplet of MUB. Here, every set of four numbers $ijkl$ denotes the four CHMs H_i, H_j, H_k, and H_l. The fifth basis is given by $H_9 = \mathbb{I}$, which is implicit in the table. Thus, the quintuplet associated with $ijkl$ is $\{\mathbb{I}, H_i, H_j, H_k, H_l\}$. By removing one basis we get a quadruplet having free parameters. The seven quantum circuits are

TABLE III. Quantum circuit required to construct every quadruplet and quintuplet of MUB stemming from $\mathcal{S}_4$. The four numbers $ijkl$ denote the quintuplet $\{\mathbb{I}, H_i, H_j, H_k, H_l\}$, whereas the bold numbers denote which basis carries the parameters. Quadruplets are constructed by removing any basis from quintuplets.

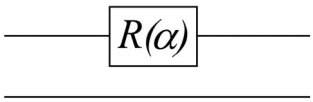
Circuit A	Circuit B	Circuit C	Circuit D	Circuit E	Circuit F	Circuit G
12**4**6	12**3**4	123**6**	134**5**	12**4**5	12**3**7	**1**235
125**7**	127**8**	12**5**8	136**7**	**1**267	**1**248	12**6**8
1347	**1**368	13**4**8	146**8**	147**8**	135**8**	13**7**8
1356	14**6**7	**1**456	**1**578	15**6**8	14**5**7	15**6**7
2478	**2**358	23**7**8	**2**346	23**4**7	23**6**8	234**8**
256**8**	24**5**7	**2**567	**2**357	235**6**	246**7**	245**6**
34**6**8	34**5**6	**3**467	**2**458	**3**458	356**7**	345**7**
35**7**8	56**7**8	45**7**8	**2**678	367**8**	356**8**	**4**678

given by

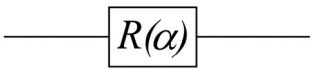
QUANTUM CIRCUIT A:



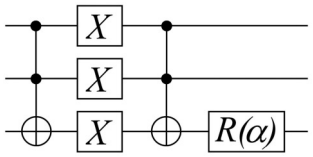
QUANTUM CIRCUIT B:



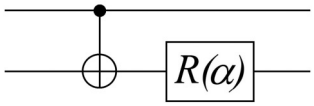
QUANTUM CIRCUIT C:



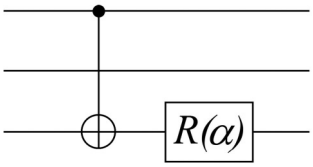
QUANTUM CIRCUIT D:



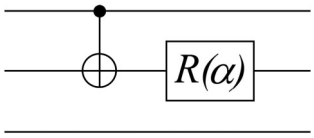
QUANTUM CIRCUIT E:



QUANTUM CIRCUIT F:



QUANTUM CIRCUIT G:



where

$$R(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \tag{C1}$$

and $\alpha \in [0,2\pi)$. Every quantum circuit (from A to G) introduces aligned free parameters in one of the bases of every quintuplet. The selection of the quadruplet or quintuplet has to be according Table II, as we already explained and exemplified in Appendix B. The aligned free parameters appear according the following table:

Circuit	A	B	C	D	E	F	G
Rows	1234	1256	1357	1467	2367	2457	3456

(C2)

Here, every set of four numbers determines the rows where the free parameters are introduced in the bases. For example, the quintuplet $\{\mathbb{I}, H_1, H_2, H_3, H_5\}$ provided in Appendix B allows the introduction of parameters in H_1. The fixed set of five bases is generated by the quantum circuit given in Fig. 2. According Table III, the free parameters can be introduced in H_1 by considering the quantum circuit G. The aligned parameters in H_1 appear in the rows 3–6 [according to (C2)]. We encourage readers to verify these properties from the explicit expressions of the quintuplet $\{\mathbb{I}, H_1, H_2, H_3, H_5\}$ provided in Appendix B.

APPENDIX D: MAXIMAL NUMBER OF MUB: A SIMPLE PROOF FOR THE UPPER BOUND

Here we present an independent proof for the upper bound of the maximal number of MUB in real and complex Hilbert spaces. This proof is simple, short, and considers basic algebra.

Proposition 2. In dimension N there are $m_R \leqslant N/2+1$ and $m_C \leqslant N+1$ MUB for real and complex Hilbert spaces, respectively.

Proof. Let G be the Gram matrix of m complex MUB in dimension N. Then

$$G \circ G^\dagger = \frac{1}{N}\mathbb{J} + \mathbb{I}, \tag{D1}$$

where the $mN \times mN$ matrix $\mathbb{J}$ has m diagonal blocks of size N, each of them having the null matrix, and the nondiagonal blocks of size N are equal to the unit matrix $\mathbf{1}$ (i.e., every entry of $\mathbf{1}$ is 1). The matrix $\mathbb{I}$ of Eq. (D1) is the identity matrix of size mN. From matrix theory it is known that given two matrices $A, B \geqslant 0$ we have the following relationship between ranks: $\mathcal{R}(A \circ B) \leqslant \mathcal{R}(A)\mathcal{R}(B)$. By considering $A = B^\dagger = G(n,d)$, the above inequality, and Eq. (D1) we have $mN - (m-1) \leqslant N^2$ or, equivalently, $m \leqslant N+1$. For the real case, we have the tighter inequality $\mathcal{R}(A \circ A) \leqslant \frac{1}{2}\mathcal{R}(A)[\mathcal{R}(A)+1]$ [43]. From combining this inequality with Eq. (D1) we have $m_R \leqslant N/2+1$. ■

This proof was inspired by the derivation of the upper bound of the maximal number of vectors in equiangular tight frames [44].

[1] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, Piscataway, 1984).

[2] D. Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, Phys. Rev. Lett. **81**, 3018 (1998).

[3] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using d-level Systems, Phys. Rev. Lett. **88**, 127902 (2002).

[4] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B. C. Hiesmayr, Entanglement detection via mutually unbiased bases, Phys. Rev. A **86**, 022311 (2012).

[5] A. Casaccino, E. Galvao, and S. Severini, Extrema of discrete Wigner functions and applications, Phys. Rev. A **78**, 022310 (2008).

[6] T. Durt, B. Englert, I. Bengtsson, and K. Życzkowski, On mutually unbiased bases, Int. J. Quantum Inf. **08**, 535 (2010).

[7] I. D. Ivanovic, J. Phys. A **14**, 3241 (1981).

[8] J. Sánchez-Ruiz, Improved bounds in the entropic uncertainty and certainty relations for complementary observables, Phys. Lett. A **201**, 125 (1995).

[9] L. Rudnicki, Z. Puchala, and K. Życzkowski, Strong majorization entropic uncertainty relations, Phys. Rev. A **89**, 052115 (2014).

[10] S. Wehner and A. Winter, Entropic uncertainty relations—A survey, New J. Phys. **12**, 025009 (2010).

[11] P. Mandayam, S. Bandyopadhyay, M. Grassl, and W. K. Wootters, Unextendible mutually unbiased bases from Pauli classes, Quantum Inf. Comput. **14**, 823 (2014).

[12] D. Goyeneche, Mutually unbiased triplets from non-affine families of complex Hadamard matrices in dimension 6, J. Phys. A: Math. Theor. **46**, 105301 (2013).

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

[14] D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. Terhal, Locking Classical Correlations in Quantum States, Phys. Rev. Lett. **92**, 067902 (2004).

[15] M. Ballester and S. Wehner, Entropic uncertainty relations and locking: Tight bounds for mutually unbiased bases, Phys. Rev. A **75**, 022319 (2007).

[16] A. Datta and S. Gharibian, Signatures of nonclassicality in mixed-state quantum computation, Phys. Rev. A **79**, 042325 (2009).

[17] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[18] S. Brierley, S. Weigert, and I. Bengtsson, All mutually unbiased bases in dimensions two to five, Quantum Inf. Comput. **10**, 803 (2010).

[19] G. Björk and R. Froberg, in *Analysis, Algebra and Computers in Mathematical Research*, edited by M. Gyllenberg and L. Persson, Lecture Notes in Pure and Applied Mathematics Vol. 156 (Dekker, New York, 1994), pp. 57–70.

[20] W. Tadej and K. Życzkowski, A concise guide to complex Hadamard matrices, Open Syst. Inf. Dyn. **13**, 133 (2006).

[21] J. Romero, G. Björk, A. Klimov, and L. Sanchez Soto, Structure of the sets of mutually unbiased bases for N qubits, Phys. Rev. A **72**, 062310 (2005).

[22] A. Klimov, J. Romero, G. Björk, and L. Sanchez Soto, Discrete phase-space structure of n-qubit mutually unbiased bases, Ann. Phys. (N.Y.) **324**, 53 (2009).

[23] A. Klimov, D. Sych, L. Sanchez Soto, and G. Leuchs, Mutually unbiased bases and generalized Bell states, Phys. Rev. A **79**, 052101 (2009).

[24] A. Klappenecker and M. Roetteler, in *Finite Fields and Applications*, edited by G. L. Mullen, A. Poli, and H. Stichtenoth, Lecture Notes in Computer Science Vol. 2948 (Springer, Berlin, 2004), pp. 137–144.

[25] T. Paterek, B. Dakic, and C. Brukner, Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models, Phys. Rev. A **79**, 012109 (2009).

[26] U. Haagerup, in *Operator Algebras and Quantum Field Theory* (International Press, Cambridge, 1996), pp. 296–322.

[27] G. Zauner, Quantum designs: Foundations of a noncommutative design theory, Ph.D. thesis, University of Wien, 1999.

[28] C. Archer, There is no generalization of known formulas for mutually unbiased bases, J. Math. Phys. **46**, 022106 (2005).

[29] P. Jaming, M. Matolcsi, and P. Móra, The problem of mutually unbiased bases in dimension 6, Cryptogr. Commun. **2**, 211 (2010).

[30] M. Grassl, in *Proceedings of the ERATO Conference on Quantum Information Science* (Tokyo, 2004), pp. 60–61.

[31] P. Butterley and W. Hall, Numerical evidence for the maximum number of mutually unbiased bases in dimension six, Phys. Lett. A **369**, 5 (2007).

[32] I. Bengtsson, W. Bruzda, A. Ericsson, J. Larsson, W. Tadej, and K. Życzkowski, MUBs and Hadamards of order six, J. Math. Phys. **48**, 052106 (2007).

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

[34] S. Brierley and S. Weigert, Mutually unbiased bases and semidefinite programming, J. Phys.: Conf. Ser. **254**, 012008 (2010).

[35] P. Jaming, M. Matolcsi, P. Mora, F. Szöllösi, and M. Weiner, A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6, J. Phys. A: Math. Theor. **42**, 245305 (2009).

[36] M. Petrescu, Existence of continuous families of complex Hadamard matrices of certain prime dimensions, Ph.D thesis, University of California, Los Angeles, 1997.

[37] U. Haagerup, Cyclic p-roots of prime lengths p and related complex Hadamard matrices, arXiv:0803.2629.

[38] J.-C. Faugère, in *Proceedings of the Fifth Asian Symposium on Computer Mathematics*, edited by K. Shirayanagi and K. Yokoyama, Lecture Notes Series on Computing Vol. 9 (World Scientific, Singapore, 2001), pp. 1–12.

[39] D. Goyeneche, A new method to construct families of complex Hadamard matrices in even dimensions, J. Math. Phys. **54**, 032201 (2013).

[40] U. Seyfarth, L. L. Sanchez-Soto, and G. Leuchs, Practical implementation of mutually unbiased bases using quantum circuits, Phys. Rev. A **91**, 032102 (2015).

[41] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Elementary gates for quantum computation, Phys. Rev. A **52**, 3457 (1995).

[42] V. Coffman, J. Kundu, and W. K. Wootters, Distributed entanglement, Phys. Rev. A **61**, 052306 (2000).

[43] J. Tropp (private communication).

[44] M. Sustik, J. Tropp, I. Dhillon, and R. Heath, On the existence of equiangular tight frames, Linear Algebra Appl. **426**, 619 (2007).