Practical implementation of mutually unbiased bases using quantum circuits

U. Seyfarth,[1] L. L. Sánchez-Soto,[1,2,3] and G. Leuchs[1,2]

[1]*Max-Planck-Institut für die Physik des Lichts, Günther-Scharowsky-Straße 1, Bau 24, 91058 Erlangen, Germany*

[2]*Department für Physik, Universität Erlangen-Nürnberg, Staudtstraße 7, Bau 2, 91058 Erlangen, Germany*

[3]*Departamento de Óptica, Facultad de Física, Universidad Complutense, 28040 Madrid, Spain*

(Received 14 December 2014; published 2 March 2015)

The number of measurements necessary to perform the quantum state reconstruction of a system of qubits grows exponentially with the number of constituents, creating a major obstacle for the design of scalable tomographic schemes. We work out a simple and efficient method based on cyclic generation of mutually unbiased bases. The basic generator requires only Hadamard and controlled-phase gates, which are available in most practical realizations of these systems. We show how complete sets of mutually unbiased bases with different entanglement structures can be realized for three and four qubits. We also analyze the quantum circuits implementing the various entanglement classes.

DOI: 10.1103/PhysRevA.91.032102 PACS number(s): 03.65.Wj, 03.65.Aa, 03.67.Ac, 03.67.Lx

I. INTRODUCTION

Modern quantum science is nearing precise control and manipulation of quantum states so as to achieve results beyond the limits of conventional technologies. Quantum-enhanced devices are already on the market and point to a transformation of measurement, communication, and computation.

For the successful completion of these tasks, verification of each stage in the experimental procedures is of utmost importance; quantum tomography is the appropriate tool for that purpose [1]. The main challenge of this technique is simple to state: given a system in a state represented by the density matrix ϱ and an informationally complete measurement [2–4], the state ϱ must be inferred from the distinct measurement outcomes.

For a d-dimensional quantum system (a qudit, in the modern parlance of quantum information) this amounts to determining $d^2 - 1$ independent real numbers. A von Neumann measurement (the only ones we consider here) fixes at most $d - 1$ real parameters, so $d + 1$ different tests have to be performed to reconstruct the state. This means that $d^2 + d$ histograms have to be recorded. The approach is, thus, suboptimal because this number is higher than the number of parameters in the density matrix. This redundancy is optimized when the bases in which the measurements are performed are mutually unbiased [5,6].

At a fundamental level, mutually unbiased bases (MUBs) are intimately related to the nature of quantum information and provide the most accurate statement of complementarity. The idea emerged in the pioneering work of Schwinger [7] and has gradually turned into a primitive of quantum theory: apart from the role in quantum tomography, they are instrumental in addressing a number of enthralling questions [8].

However, tomography becomes harder as we explore more intricate systems. If we look at the simple, yet illustrative case of n qubits, even with MUBs, one will have to make at least $2^n + 1$ measurements before one can claim to know everything about an *a priori* unknown system. With such a scaling, it is clear that the methods rapidly become intractable for present state-of-the-art experiments [9,10].

We are thus inevitably led to the quest for tomographical techniques with better scaling. A promising class of new protocols are explicitly optimized only for particular kinds of states. This includes states with low rank [11–13], with special emphasis in some relevant cases as matrix product states (MPSs) [14,15], or multiscale entangled renormalization ansatz (MERA) states [16]. The specific but pertinent example of permutationally invariant qubits has been also examined [17–20], because they are of great import in diverse quantum information strategies [21–27].

In this paper, we devise an alternate approach to this problem. We revisit the MUB strategy but capitalize on a recently developed construction which generates the corresponding MUBs in a cyclic way [28,29]. From an experimental viewpoint, the undeniable advantage of this approach is that a single unitary operation U is enough to create all the MUBs. Furthermore, this single unitary operator can be expressed as a quantum circuits involving exclusively Hadamard and controlled-phase gates [30]. In this way, the number of gates scales only linearly in the number of qubits, which is an optimal scaling.

Our paper is organized as follows: In Sec. II we concisely sketch the rudiments of our method. For systems of qubits, it is well known that different complete sets of MUBs exist with distinct entanglement properties [31–37]. In Sec. III we work out the simple example of three qubits, showing the quantum circuits associated with the different complete sets, while the case of four qubits is worked out in the Appendix. Finally, our conclusions are briefly summarized in Sec. IV.

II. MUTUALLY UNBIASED BASES: BASIC BACKGROUND

We consider a d-dimensional quantum system with Hilbert space isomorphic to $\mathbb{C}^d$. The different outcomes of a maximal test constitute an orthogonal basis of $\mathbb{C}^d$ [38]. One can also look for orthogonal bases that, in addition, are "as different as possible." This is the idea behind MUBs and can be formally stated as follows: two orthonormal bases $\mathcal{B}_j = \{|\psi_\ell^{(j)}\rangle\}$ and $\mathcal{B}_{j'} = \{|\psi_{\ell'}^{(j')}\rangle\}$ $(j \neq j')$ are mutually unbiased when

$$\left|\langle\psi_\ell^{(j)}|\psi_{\ell'}^{(j')}\rangle\right|^2 = \frac{1}{d}, \quad \forall\, \ell,\ell' = 1,\ldots,d. \tag{2.1}$$

Unbiasedness also applies to measurements: two nondegenerate tests are mutually unbiased if the bases formed by their eigenstates are MUBs. For example, the measurements of the components of a spin $\frac{1}{2}$ along the x, y, and z axes are all unbiased.

It has been shown that the number of MUBs is at most $d+1$ [5], and that such a complete set exists whenever d is a prime or power of a prime [39]. Remarkably, there is no known answer for any other values of d, although there have been some attempts to find a solution to this problem in some simple cases, such as $d=6$ [40–45] or when d is a non-prime-integer squared [46,47].

In what follows, we concentrate on a system of n qubits, where the dimension of the space is $d=2^n$. The basic single-particle Pauli operators σ_z and σ_x are

$$\sigma_z = |1\rangle\langle 1| - |0\rangle\langle 0|, \quad \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \tag{2.2}$$

where $|0\rangle$ and $|1\rangle$ are the computational basis for a single qubit. The concept can be extended to n qubits by introducing $2n$-dimensional vectors

$$\mathbf{a} = \left(a_1^z,\dots,a_n^z;a_1^x,\dots,a_n^x\right)^T, \tag{2.3}$$

where T denotes the transpose and $a_i^z,a_j^x \in \mathbb{Z}_2$. In this way, the generalized Pauli operators can be written down as

$$ZX(\mathbf{a}) = (-i)^{a_1^z a_1^x}\sigma_z^{a_1^z}\sigma_x^{a_1^x} \otimes \cdots \otimes (-i)^{a_n^z a_n^x}\sigma^{a_n^z}\sigma^{a_n^x}. \tag{2.4}$$

In technical jargon, this set is just the Weyl–Heisenberg group (modulo its center).

The importance of these operators lies in the observation noticed in Ref. [48] that complete sets of MUBs naturally arise from a partition of the set of Pauli operators into $d+1$ subsets of $d-1$ commuting operators, called classes; they can be expressed as

$$\mathfrak{C}_j = \left\{ZX(\mathbf{a}) : \mathbf{a} = G_j\mathbf{c} : \mathbf{c} \in \mathbb{Z}_2^n\right\}. \tag{2.5}$$

In this way, each of the classes $\mathfrak{C}_j$ can be specified by the generator G_j.

Within each class $\mathfrak{C}_j$ all Pauli operators commute. If we unveil the tensor product of the Pauli operators, we can consider each Pauli operator as a joint operator that performs either a σ_z, σ_x, σ_y, or an identity operation on each single qubit separately. Within a certain class, the Pauli operators on each qubit can either commute or not, which leads to different entanglement properties. The maximal entanglement occurs when the Pauli operators of one class commute only in combination, whereas no entanglement appears when they commute on every qubit separately. All possible partitions of the operators into their subsystems give rise to different entanglement properties, where a relabelling of the different sites should not influence this classification at all. Therefore, we define a vector $\mathbf{n}$ which represents the entanglement structure of a certain set of MUBs: the entries of $\mathbf{n}$ are computed by counting the number of classes with each entanglement structure, starting from a completely factorizable system, and ending with a fully entangled one.

Different explicit constructions of MUBs in prime power dimensions have been suggested in a number of recent papers [49–55]. We follow here the approach established in Refs. [28,29], that allows a cyclic generation of the MUBs; that is, the generators appearing in each class (2.5) can be expressed as

$$G_j = C^j G_0, \tag{2.6}$$

where G_0 is a fixed generator. We skip the mathematical details involved in the derivation of the method and content ourselves with the final result, which looks very compact: the symplectic matrix C can be jotted down as

$$C = \begin{pmatrix} B + AR^{-1} & R + BA + AR^{-1}A \\ R^{-1} & R^{-1}A \end{pmatrix}, \tag{2.7}$$

where B, R, and A are $n\times n$ matrices whose properties will be specified soon. The successive powers of C can be computed as

$$C^j = \begin{pmatrix} F_{j+1}(B) + AR^{-1}F_j(B) & F_{j+1}(B)A + F_j(B)R + AR^{-1}[F_j(B)A + F_{j-1}(B)R] \\ R^{-1}F_j(B) & R^{-1}[F_j(B)A + F_{j-1}(B)R] \end{pmatrix}. \tag{2.8}$$

Here, $F_j(x)$ refer to the Fibonacci polynomials, which are a generalization of the well-known Fibonacci sequence. They are defined recursively as

$$F_{j+1}(x) = xF_j(x) + F_{j-1}(x), \tag{2.9}$$

with $F_0(x)=0$ and $F_1(x)=1$ and the coefficients therein are binary numbers in $\mathbb{Z}_2$. In many considerations in this work, we will take as the seed generator $G_0 = (\mathbb{1}_n,0_n)^T$, which leads to

$$G_j = \begin{pmatrix} F_{j+1}(B)F_j^{-1}(B)R + A \\ \mathbb{1}_m \end{pmatrix}, \quad 1 \leqslant j \leqslant d. \tag{2.10}$$

To ensure that complete sets of MUBs are generated, we have to impose additional conditions. The first one, of rather technical character, implies that the Fibonacci index [56] of the characteristic polynomial of B has to be $d+1$. In addition, R, BR, and A have to be symmetric and R has to be invertible [57].

It turns out that when $R=\mathbb{1}_m$ and $A=0_m$, the resulting complete sets exhibit an entanglement structure with three completely factorizable classes, which, following the original work [57], will be called field-based sets, as the generators represent a finite field. When R is not a polynomial in B and $A=0_m$, the generators form an additive group, where for only two of their classes the Pauli operators commute on each qubit separately: they are denoted as group-based sets, Finally, whenever R is not a polynomial in B, and A is not the product of any polynomial in B with R added to a diagonal matrix, the resulting cyclic set of MUBs has only a single class left, where the Pauli operators commute on all qubits separately. This case is denoted as semigroup-based sets, because the generator represents an additive semigroup.

III. RESULTS

The three-qubit system is the first nontrivial instance one can consider, and any complete set of MUBs exhibits $2^3 + 1 = 9$ different bases. It is well known [31,33,34,58] that each complete set of MUBs possesses one of the four different entanglement structures, either (3,0,6), (2,3,4), (1,6,2), or (0,9,0). In this particular example, in $\mathbf{n} = (n_1,n_2,n_3)$, n_1 denotes the number of separable bases (every eigenvector of theses bases is a tensor product of singe-qubit states), n_2 the number of biseparable bases (one qubit is factorized and the other two are in a maximally entangled state), and n_3 the number of nonseparable bases.

To work out the cyclic construction of these sets, we first notice that the only polynomial of order three that has full Fibonacci index (i.e., index 9) is

$$p(x) = 1 + x + x^3. \tag{3.1}$$

For field-based sets, the matrix B has to be symmetric, such as $R = \mathbb{1}_m$. The only possible solution is

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \tag{3.2}$$

or one of its permutations. This corresponds to an entanglement structure $\mathbf{n} = (3,0,6)$.

The group-based sets are richer, because polynomials of B can be shifted into R. One possible solution is generated by

$$B = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \tag{3.3}$$

which leads finally to the symplectic matrix

$$C = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{3.4}$$

This corresponds to the entanglement structure $\mathbf{n} = (2,3,4)$.

In a similar way, we find the following solution for the semigroup-based sets

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \tag{3.5}$$

which gives the matrix

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}. \tag{3.6}$$

and the corresponding entanglement structure is $\mathbf{n} = (1,6,2)$.

The set $\mathbf{n} = (0,9,0)$ cannot be worked out initially from this construction method. However, this can be easily fixed: because this set does not contain any basis that measures properties of a completely factorizable system, a sort of offset operation transforming the standard basis is needed. Therefore, the generator G_0 cannot be taken as $(\mathbb{1}_m,0_m)$ anymore, but instead its X part, which is 0_m, has to be replaced with

$$G_0^x = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \tag{3.7}$$

and so

$$C = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{3.8}$$

for the implementation of the symplectic generator.

One of the outstanding advantages of our approach is that the unitary generator can be worked out in quite a direct way as a quantum circuit involving only elementary gates. Such a decomposition can be immediately found following the standard rules [30]. In particular, this is relevant for a practical implementation. In Fig. 1 we summarize the circuits corresponding to the structures (3,0,6), (2,3,4), (1,6,2),

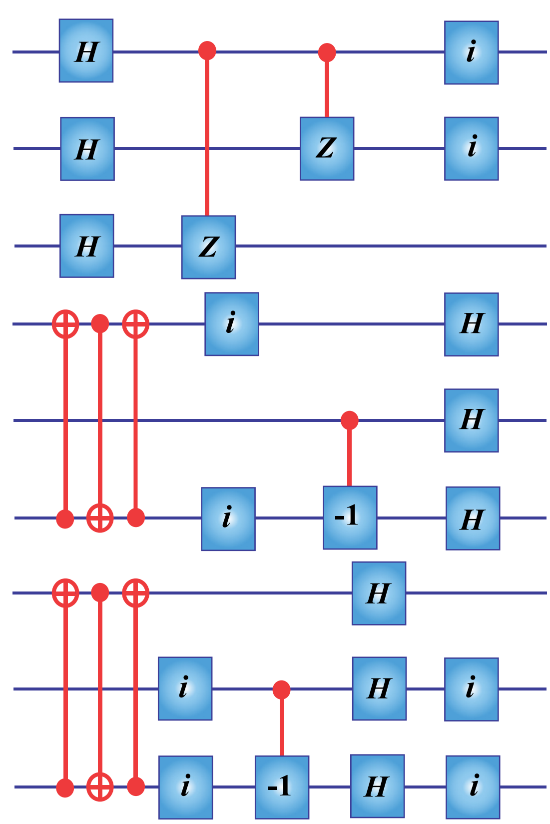

FIG. 1. (Color online) Quantum circuits implementing the generators of three-qubit MUBs with entanglement structures (from left to right) (3,0,6), (2,3,4), and (1,6,2). The notation for the gates is the standard one [30].

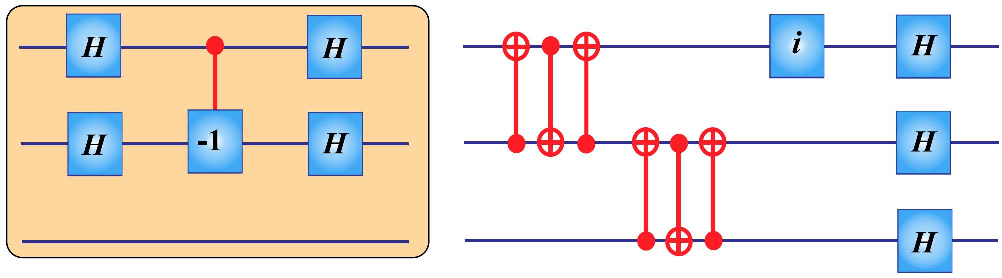

FIG. 2. (Color online) Quantum circuit implementing the generator of three-qubit MUBs with entanglement structure (0,9,0). In the left, enclosed in a box, we show the circuit for the offset generator ${G_0}^x$.

whereas in Fig. 2 we give the circuit for (0,9,0), including the offset (3.7).

The method works for any number of qubits. Since the ideas are analogous, we omit the unnecessary details although, for completeness, we give the complete solution for four qubits in the supplementary material.

IV. CONCLUSIONS

In short, we have shown the construction of cyclic MUBs for n qubits with all possible entanglement structures. On physical grounds, one could expect that the performances of these different classes with respect to entanglement-specific state properties will also be different. In our approach, this is reflected in the different complexities of the associated generator. Finally, the fact that only one generator needs to be implemented to generate the whole set of MUBs makes this method especially interesting and a potential candidate for a realistic scheme for current experimental setups.

ACKNOWLEDGMENTS

We thank Olivia di Matteo for fruitful discussions. Financial support from the EU FP7 (Grant Q-ESSENCE), the Spanish DGI (Grant FIS2011-26786) and Program UCM-Banco Santander (Grant GR3/14) is gratefully acknowledged.

APPENDIX: CYCLIC MUBs FOR FOUR QUBITS

For completeness, we show the construction of complete sets of MUBs for four qubits following our method. We must first find a matrix B with characteristic polynomial with Fibonacci index 17, which therefore creates 17 different bases. For the characteristic polynomial we have two options; namely,

$$p(x) = 1 + x + x^2 + x^3 + x^4, \tag{A1}$$

$$p'(x) = 1 + x + x^4, \tag{A2}$$

although we limit ourselves to the first solution. The entanglement structures will be indicated by the vector $\mathbf{n}$ defined according to Ref. [58].

For field-based sets, B has to be symmetric; a possible solution is given by

$$B = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{A3}$$

and leads, with $R = \mathbb{1}_4$ and $A = 0_4$, to the field-based set with the entanglement structure $\mathbf{n} = (3,0,0,2,12)$.

Seven group-based sets with different entanglement structures exist for four-qubit systems. We list them in what follows:

$\mathbf{n} = (2,0,4,2,9)$,

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{A4}$$

$\mathbf{n} = (2,1,2,1,11)$,

$$B = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}. \tag{A5}$$

$\mathbf{n} = (2,2,0,2,11)$,

$$B = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{A6}$$

$\mathbf{n} = (2,1,2,0,12)$,

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{A7}$$

$\mathbf{n} = (2,0,4,0,11)$,

$$B = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}. \tag{A8}$$

$\mathbf{n} = (2,1,2,2,10)$,

$$B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{A9}$$

$\mathbf{n} = (2,0,4,1,10)$,

$$B = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}. \tag{A10}$$

Thirteen semigroup-based sets with different entanglement structures exist. We list them in the following:
$\mathbf{n} = (1,4,0,2,10)$,

$$B = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A11}$$

$\mathbf{n} = (1,2,4,0,10)$,

$$B = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A12}$$

$\mathbf{n} = (1,0,0,8,8)$,

$$B = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A13}$$

$\mathbf{n} = (1,2,4,2,8)$,

$$B = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{A14}$$

$\mathbf{n} = (1,4,0,1,11)$,

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A15}$$

$\mathbf{n} = (1,1,6,0,9)$,

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A16}$$

$\mathbf{n} = (1,3,2,2,9)$,

$$B = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{A17}$$

$\mathbf{n} = (1,2,4,1,9)$,

$$B = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A18}$$

$\mathbf{n} = (1,3,2,0,11)$,

$$B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A19}$$

$\mathbf{n} = (1,0,8,1,7)$,

$$B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A20}$$

$\mathbf{n} = (1,1,6,1,8)$,

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A21}$$

$\mathbf{n} = (1,1,6,2,7)$,

$$B = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A22}$$

$\mathbf{n} = (1,3,2,1,10)$,

$$B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A23}$$

Thirteen extra sets with different entanglement structures exist for four-qubit systems. The corresponding generator G_0 is replaced in its X part, which is 0_m, by

$$G_0^x = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A24}$$

$\mathbf{n} = (0,5,2,2,8)$,

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}. \tag{A25}$$

$\mathbf{n} = (0,5,2,1,9)$,

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{A26}$$

$\mathbf{n} = (0,5,2,0,10)$,

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{A27}$$

$\mathbf{n} = (0,4,4,2,7)$,

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}. \tag{A28}$$

$\mathbf{n} = (0,4,4,1,8)$,

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{A29}$$

$\mathbf{n} = (0,4,4,0,9)$,

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}. \tag{A30}$$

$\mathbf{n} = (0,3,6,2,6)$,

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}. \tag{A31}$$

$\mathbf{n} = (0,3,6,1,7)$,

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}. \tag{A32}$$

$\mathbf{n} = (0,3,6,0,8)$,

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{A33}$$

$\mathbf{n} = (0,2,8,1,6)$,

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}. \tag{A34}$$

$\mathbf{n} = (0,2,8,0,7)$,

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{A35}$$

$\mathbf{n} = (0,1,10,0,6)$,

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}. \tag{A36}$$

$\mathbf{n} = (0,0,2,12,3)$,

$$C = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}. \tag{A37}$$

The associated quantum circuits can be constructed as in the paper.

[1] *Quantum State Estimation*, edited by M. G. A. Paris and J. Řeháček, Lecture Notes in Physics (Springer, Berlin, 2004), Vol. 649.

[2] E. Prugovečki, Information-theoretical aspects of quantum measurement, Int. J. Theor. Phys. **16**, 321 (1977).

[3] P. Busch and P. J. Lahti, The determination of the past and the future of a physical system in quantum mechanics, Found. Phys. **19**, 633 (1989).

[4] D. Sych, J. Řeháček, Z. Hradil, G. Leuchs, and L. L. Sánchez-Soto, Informational completeness of continuous-variable measurements, Phys. Rev. A **86**, 052123 (2012).

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

[6] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, Ann. Phys. (NY) **191**, 363 (1989).

[7] J. Schwinger, Unitary operator basis, Proc. Natl. Acad. Sci. USA **46**, 570 (1960).

[8] T. Durt, B.-G. Englert, I. Bengtsson, and K. Zyczkowski, On mutually unbiased bases, Int. J. Quantum Inf. **8**, 535 (2010).

[9] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt, 14-qubit entanglement: Creation and coherence, Phys. Rev. Lett. **106**, 130506 (2011).

[10] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan,

Observation of eight-photon entanglement, Nat. Photon. **6**, 225 (2012).
[11] D. Gross, Y. K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Quantum state tomography via compressed sensing, Phys. Rev. Lett. **105**, 150401 (2010).
[12] S. T. Flammia, D. Gross, Y.-K. Liu, and J. Eisert, Quantum tomography via compressed sensing: Error bounds, sample complexity and efficient estimators, New J. Phys. **14**, 095022 (2012).
[13] M. Guta, T. Kypraios, and I. Dryden, Rank-based model selection for multiple ions quantum tomography, New J. Phys. **14**, 105002 (2012).
[14] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y. K. Liu, Efficient quantum state tomography, Nat. Commun. **1**, 149 (2010).
[15] T. Baumgratz, D. Gross, M. Cramer, and M. B. Plenio, Scalable reconstruction of density matrices, Phys. Rev. Lett. **111**, 020401 (2013).
[16] O. Landon-Cardinal and D. Poulin, Practical learning method for multi-scale entangled states, New J. Phys. **14**, 085004 (2012).
[17] G. M. D'Ariano, L. Maccone, and M. Paini, Spin tomography, J. Opt. B: Quantum Semiclassical Opt. **5**, 77 (2003).
[18] G. Tóth, W. Wieczorek, D. Gross, R. Krischek, C. Schwemmer, and H. Weinfurter, Permutationally invariant quantum tomography, Phys. Rev. Lett. **105**, 250403 (2010).
[19] A. B. Klimov, G. Björk, and L. L. Sánchez-Soto, Optimal quantum tomography of permutationally invariant qubits, Phys. Rev. A **87**, 012109 (2013).
[20] T. Moroder, P. Hyllus, G. Tóth, C. Schwemmer, A. Niggebaum, S. Gaile, O. Gühne, and H. Weinfurter, Permutationally invariant state reconstruction, New J. Phys. **14**, 105001 (2012).
[21] D. W. Berry and H. M. Wiseman, Optimal states and almost optimal adaptive measurements for quantum interferometry, Phys. Rev. Lett. **85**, 5098 (2000).
[22] J. K. Stockton, J. M. Geremia, A. C. Doherty, and H. Mabuchi, Characterizing the entanglement of symmetric many-particle spin-1/2 systems, Phys. Rev. A **67**, 022112 (2003).
[23] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Classical and quantum communication without a shared reference frame, Phys. Rev. Lett. **91**, 027901 (2003).
[24] A. Cabello, Six-qubit permutation-based decoherence-free orthogonal basis, Phys. Rev. A **75**, 020301 (2007).
[25] J. Fiurášek, Three-qubit quantum gates and filters for linear optical quantum-information processing, Phys. Rev. A **79**, 012330 (2009).
[26] R. Demkowicz-Dobrzanski, U. Dorner, B. J. Smith, J. S. Lundeen, W. Wasilewski, K. Banaszek, and I. A. Walmsley, Quantum phase estimation with lossy interferometers, Phys. Rev. A **80**, 013825 (2009).
[27] A. Hentschel and B. C. Sanders, Ordered measurements of permutationally-symmetric qubit strings, J. Phys. A: Math. Theor. **44**, 115301 (2011).
[28] O. Kern, K. S. Ranade, and U. Seyfarth, Complete sets of cyclic mutually unbiased bases in even prime-power dimensions, J. Phys. A: Math. Theor. **43**, 275305 (2010).
[29] U. Seyfarth and K. S. Ranade, Construction of mutually unbiased bases with cyclic symmetry for qubit systems, Phys. Rev. A **84**, 042327 (2011).
[30] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[31] J. Lawrence, C. Brukner, and A. Zeilinger, Mutually unbiased binary observable sets on *n* qubits, Phys. Rev. A **65**, 032320 (2002).
[32] J. Lawrence, Mutually unbiased bases and trinary operator sets for *n* qutrits, Phys. Rev. A **70**, 012302 (2004).
[33] J. L. Romero, G. Björk, A. B. Klimov, and L. L. Sánchez-Soto, Structure of the sets of mutually unbiased bases for *n* qubits, Phys. Rev. A **72**, 062310 (2005).
[34] J. Lawrence, Entanglement patterns in mutually unbiased basis sets, Phys. Rev. A **84**, 022338 (2011).
[35] M. Wieśniak, T. Paterek, and A. Zeilinger, Entanglement in mutually unbiased bases, New J. Phys. **13**, 053047 (2011).
[36] J. Řeháček, Z. Hradil, A. B. Klimov, G. Leuchs, and L. L. Sánchez-Soto, Sizing up entanglement in mutually unbiased bases with fisher information, Phys. Rev. A **88**, 052110 (2013).
[37] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B. C. Hiesmayr, Entanglement detection via mutually unbiased bases, Phys. Rev. A **86**, 022311 (2012).
[38] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993).
[39] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets, Proc. London Math. Soc. **75**, 436 (1997).
[40] M. Grassl, On SIC-POVMs and MUBs in dimension 6, arXiv:quant-ph/0406175.
[41] P. Butterley and W. Hall, Numerical evidence for the maximum number of mutually unbiased bases in dimension six, Phys. Lett. A **369**, 5 (2007).
[42] S. Brierley and S. Weigert, Maximal sets of mutually unbiased quantum states in dimension 6, Phys. Rev. A **78**, 042312 (2008).
[43] S. Brierley and S. Weigert, Constructing mutually unbiased bases in dimension six, Phys. Rev. A **79**, 052316 (2009).
[44] P. Raynal, X. Lü, and B.-G. Englert, Mutually unbiased bases in six dimensions: The four most distant bases, Phys. Rev. A **83**, 062303 (2011).
[45] D. McNulty and S. Weigert, All mutually unbiased product bases in dimension 6, J. Phys. A: Math. Theor. **45**, 135307 (2012).
[46] C. Archer, There is no generalization of known formulas for mutually unbiased bases, J. Math. Phys. **46**, 022106 (2005).
[47] P. Wocjian and T. Beth, New construction of mutually unbiased basis in square dimensions, Quantum Inf. Comput. **5**, 93 (2005).
[48] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, A new proof for the existence of mutually unbiased bases, Algorithmica **34**, 512 (2002).
[49] A. Klappenecker and M. Rötteler, in *Finite Fields and Applications*, Lecture Notes in Computer Science, edited by G. Mullen, A. Poli, and H. Stichtenoth (Springer, Berlin, 2003), Vol. 2948, pp. 137–144.
[50] K. R. Parthasarathy, On estimating the state of a finite level quantum system, Infin. Dimens. Anal. Quantum Probab. Relat. Top. **7**, 607 (2004).
[51] A. O. Pittenger and M. H. Rubin, Mutually unbiased bases, generalized spin matrices and separability, Lin. Alg. Appl. **390**, 255 (2004).
[52] T. Durt, About mutually unbiased bases in even and odd prime power dimensions, J. Phys. A: Math. Gen. **38**, 5267 (2005).
[53] M. Planat and H. Rosu, Mutually unbiased phase states, phase uncertainties and Gauss sums, Eur. Phys. J. D **36**, 133 (2005).

[54] A. B. Klimov, L. L. Sánchez-Soto, and H. de Guise, Multicomplementary operators via finite Fourier transform, J. Phys. A: Math. Gen. **38**, 2747 (2005).
[55] O. P. Boykin, M. Sitharam, P. H. Tiep, and P. Wocjan, Mutually unbiased bases and orthogonal decompositions of Lie algebras, Quantum Inf. Comput. **7**, 371 (2007).
[56] The Fibonacci index of an irreducible polynomial $p(x)$ is the minimum integer n such that $p(x)$ divides $F_n(x)$.
[57] U. Seyfarth, L. L. Sánchez-Soto, and G. Leuchs, Structure of the sets of mutually unbiased bases with cyclic symmetry, J. Phys. A: Math. Theor. **47**, 455303 (2014).
[58] A. Garcia, J. L. Romero, and A. B. Klimov, Generation of bases with definite factorization for an n-qubit system and mutually unbiased sets construction, J. Phys. A: Math. Theor. **43**, 385301 (2010).