Unitarily inequivalent mutually unbiased bases for *n* qubits

Arun Sehrawat[*] and Andrei B. Klimov[†]

Departamento de Física, Universidad de Guadalajara, 44430 Guadalajara, Jalisco, México

(Received 11 September 2014; published 2 December 2014)

The standard construction of complete sets of mutually unbiased bases (MUBs) in prime power dimensions is based on the quadratic Gauss sums. We introduce complete MUB sets for three, four, and five qubits that are unitarily inequivalent to all existing MUB sets. These sets are constructed by using certain exponential sums, where the degree of the polynomial appearing in the exponent can be higher than 2. Every basis of these MUBs (except the computational) consists of two disjoint blocks of vectors with different factorization structures and associated with a unique hypergraph (or graph) that represents an interaction between the qubits.

DOI: 10.1103/PhysRevA.90.062308 PACS number(s): 03.67.−a

I. INTRODUCTION

The concept of mutually unbiased bases (MUBs) [1] allows us to express the fundamental idea of complementarity [2,3] probably in the clearest and most precise form. Among the several practical applications of MUBs one can mention quantum state determination and tomography [4–6], quantum key distribution [7,8], quantum error-correcting codes [9,10], and the mean king problem [11–15] (for a review of the subject, we refer the reader to [16]). In most of the relevant applications, one needs the so-called complete (or maximal) sets of MUBs. Let us recall that two orthonormal bases $\mathcal{B}^{\alpha}$ and $\mathcal{B}^{\alpha'}$, $\alpha \neq \alpha'$, of a d-dimensional Hilbert space are said to be *mutually unbiased* if $|\langle\Psi^{\alpha'}_{\beta'}|\Psi^{\alpha}_{\beta}\rangle|^2 = d^{-1}$ for every $|\Psi^{\alpha}_{\beta}\rangle \in \mathcal{B}^{\alpha}$ and $|\Psi^{\alpha'}_{\beta'}\rangle \in \mathcal{B}^{\alpha'}$, and a maximal set of pairwise unbiased bases contains only $d+1$ bases.

Ivanovic came up with the first explicit construction of complete MUB sets for prime dimensions [4]. His work was extended to prime-power cases by Wootters [5]. Fundamentally, the approaches developed in [4], [5], and [17–24] are based on properties of certain finite exponential sums of roots of unity. These exponential sums, the so-called *quadratic Gauss sums* (see chap. 5 in [25]), emerge in the evaluation of the absolute value of the inner products $|\langle\Psi^{\alpha'}_{\beta'}|\Psi^{\alpha}_{\beta}\rangle|$ of basis elements.

Although from the physical perspective, *locally* inequivalent complete MUB sets [19,26–28] represent a certain interest, they are related by global unitary transformations (*unitarily equivalent*) to each other and, particularly, to Ivanovich-Wootters (IW) MUBs [4,5]. Since unitary transformation preserves the inner product, every set unitarily equivalent to the IW MUB set will have the same Gaussian sums on which the IW framework is based. We call a set of MUBs a *Gaussian set* (GS) if the absolute value of the inner product of its vectors is a quadratic Gauss sum. Every IW set and all its unitarily equivalent sets belong to the family of GSs. It is noteworthy that there exist GSs of MUBs [29] that are unitarily inequivalent to the IW sets.

From the algebraic point of view [30,31], each (but the computational) basis of the IW MUBs is associated with a graph [32] with loops. Furthermore, the IW sets have a particular property that all the vectors of a single basis are locally equivalent to one another and, thus, carry the same factorization structure [33].

In this paper, we introduce complete sets of MUBs for three, four, and five qubits ($d = 2^n$ with $n = 3,4,5$), where the inner product between elements of different bases can be a cubic (or higher-degree) exponential sum. These sets, which henceforth we call *non-Gaussian sets* (NGSs), are unitarily inequivalent to the whole family of the GSs of MUBs.

It will be shown that about half of the MUBs of a NGS are related to the hypergraphs [34], where a hypergraph represents higher-order interactions among the qubits; every (excluding the computational) basis of a NGS is a union of two disjoint sets (*blocks*) of vectors with the same cardinality, where all the vectors are locally equivalent within each block but not across the blocks. In other words, the NGSs of MUBs possess a *two-block factorization structure*.

Section II contains some basic mathematical objects that are used to construct MUBs for qubits. In Sec. III, we present two sets of polynomials with the necessary constraints to achieve a maximal MUB set and review important points of the IW approach. Taking the three-qubit case in Sec. III A, we highlight all the major differences between the NGS and the IW set. The NGSs of MUBs for four and five qubits are delivered in Sec. III B. We close the discussion with some concluding remarks and open problems in Sec. IV. The Appendix includes the three- and four-qubit IW MUB sets with some additional details.

II. MATHEMATICAL OBJECTS

Let us consider $\mathbb{Z}_q := \{0,1,\ldots,q-1\}$, an additive Abelian group of integers modulo q, where 0 is the identity element and $\overline{c} \in \mathbb{Z}_q$ is the inverse of $c \in \mathbb{Z}_q$ if $c + \overline{c} \equiv 0(\mathrm{mod}q)$. In the particular case $q = 2$, the extension $\mathbb{Z}_2^n$ is an Abelian group of all 2^n possible n-bit strings, where each string $\lambda := (l_1,l_2,\ldots,l_n)$, $l_j \in \mathbb{Z}_2$ for all $1 \leqslant j \leqslant n$, is isomorphic to a ket $|\lambda\rangle = |l_1 l_2 \ldots l_n\rangle \in \mathcal{H}_2^n$. The collection of all such kets forms the *computational basis* $\mathcal{B}_c := \{|\lambda\rangle \mid \lambda \in \mathbb{Z}_2^n\}$ of the Hilbert space $\mathcal{H}_2^n$ for n qubits. We start the construction of a complete set of $2^n + 1$ MUBs by keeping $\mathcal{B}_c$ as its first element.

For the purpose of building the other 2^n bases, we consider monomials $c\,(l_1^{k_1}\, l_2^{k_2} \cdots l_n^{k_n})$ of n binary variables, where the coefficient $c \in \mathbb{Z}_4$ and the exponent $\kappa = (k_1,k_2,\ldots,k_n) \in \mathbb{Z}_2^n$ determines the degree of the monomial. For a nonzero c,

[*] arunsehrawat2@gmail.com

[†] klimov@cencar.udg.mx

TABLE I. Examples of first-, second-, and third-degree monomials p and the corresponding unitary operators U_p of Eqs. (3) for one, two, and three qubits. From the top, the first, second, and third U_p are the $\pi/2$-phase (P) operator, controlled-phase (CP) operator, and controlled-controlled-Z (CCZ) operator, respectively. Labels of qubits (on which the operators act) are given in the subscripts, and I and Z are the standard single-qubit Pauli operators.

$p(\lambda)$	U_p
l_i	$\mathrm{P}_i = I_i + (\omega - 1)(\vert 1\rangle\langle 1\vert)_i$
$l_i l_j$	$\mathrm{CP}_{ij} = I_i I_j + (\omega - 1)(\vert 11\rangle\langle 11\vert)_{ij}$
$2\, l_1 l_2 l_3$	$\mathrm{CCZ}_{123} = I_1 I_2 I_3 - 2\,(\vert 111\rangle\langle 111\vert)_{123}$

there exist $\frac{n!}{k!(n-k)!}$ different monomials of degree $k = \sum_{j=1}^{n} k_j$. A polynomial $p : \mathbb{Z}_2^n \to \mathbb{Z}_4$ is formed as the sum of such monomials,

$$p(\lambda) := \underset{\kappa\in\mathbb{Z}_2^n}{\boxplus} c_\kappa \left(l_1^{k_1}\, l_2^{k_2} \ldots l_n^{k_n}\right), \quad \text{with} \quad c_\kappa \in \mathbb{Z}_4; \tag{1}$$

the symbol $\boxplus$ stands for the modulo-4 summation. For every p, there is a unique polynomial

$$\overline{p(\lambda)} = \underset{\kappa\in\mathbb{Z}_2^n}{\boxplus} \overline{c_\kappa} \left(l_1^{k_1}\, l_2^{k_2} \ldots l_n^{k_n}\right), \quad \text{with} \quad \overline{c_\kappa} \in \mathbb{Z}_4, \tag{2}$$

such that $p(\lambda) \boxplus \overline{p(\lambda)} = 0$, where $\overline{c_\kappa}$ is the modulo-4 additive inverse of c_κ. To avoid cumbersome expressions we use, only in this paragraph, binary string κ for the subscript of c. In the rest of the text, labels of qubits are used instead of the index κ.

We can associate an n-qubit unitary operator and its adjoint,

$$\begin{aligned} U_p &:= \sum_{\lambda\in\mathbb{Z}_2^n} \omega^{p(\lambda)}\, |\lambda\rangle\langle\lambda|, \\ U_p^\dagger &= \sum_{\lambda\in\mathbb{Z}_2^n} \omega^{\overline{p(\lambda)}}\, |\lambda\rangle\langle\lambda|, \end{aligned} \tag{3}$$

with p and $\overline{p}$, respectively (for examples, see Table I), where ω is the imaginary unit $\sqrt{-1}$. Observe that both U_p and $U_p^\dagger$ are diagonal in the computational basis, and the arithmetic in the exponent of ω is modulo 4.

The superpositions

$$\begin{aligned} |\Psi\rangle &:= \frac{1}{\sqrt{2^n}} \sum_{\lambda\in\mathbb{Z}_2^n} \omega^{p(\lambda)}\, |\lambda\rangle, \\ \langle\Psi| &= \frac{1}{\sqrt{2^n}} \sum_{\lambda\in\mathbb{Z}_2^n} \omega^{\overline{p(\lambda)}}\, \langle\lambda| \end{aligned} \tag{4}$$

are such that $|\Psi\rangle = U_p|+\rangle$, $|+\rangle := \frac{1}{\sqrt{2^n}} \sum_{\lambda\in\mathbb{Z}_2^n} |\lambda\rangle$ and are unbiased with every element of the computational basis: $|\langle\gamma|\Psi\rangle| = \frac{1}{\sqrt{2^n}}$, $|\gamma\rangle \in \mathcal{B}_c$. We construct the rest of the 2^n MUBs as collections of kets of the form of Eqs. (4) (see the next section), where the inner product $\langle\Psi'|\Psi\rangle$ is directly proportional to the exponential sum,

$$\sum_{\lambda\in\mathbb{Z}_2^n} \omega^{p(\lambda) \boxplus \overline{p'(\lambda)}}. \tag{5}$$

III. MUBS FOR QUBITS

Let us consider two sets of polynomials, $F^{(n)} := \{f_\beta(\lambda) \mid \beta \in \mathbb{Z}_2^n\}$ and $G^{(n)} := \{g_\alpha(\lambda) \mid \alpha \in \mathbb{Z}_2^n\}$; the first set will be used to achieve the orthonormality of each basis and the second set is needed to make the bases mutually unbiased. Polynomials of both sets are of the form of Eq. (1), and $f_0 = g_0 = 0$. According to Eqs. (4), the state vector

$$\left|\Psi_\beta^\alpha\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{\lambda\in\mathbb{Z}_2^n} \omega^{g_\alpha(\lambda) \boxplus f_\beta(\lambda)}\, |\lambda\rangle \tag{6}$$

corresponds to the polynomial $g_\alpha(\lambda) \boxplus f_\beta(\lambda)$. The inner product of such vectors

$$\begin{aligned} \left\langle\Psi_{\beta'}^{\alpha'}\middle|\Psi_\beta^\alpha\right\rangle &= \frac{1}{2^n}\, S_{\beta,\beta'}^{\alpha,\alpha'}, \\ \text{where} \quad S_{\beta,\beta'}^{\alpha,\alpha'} &= \sum_{\lambda\in\mathbb{Z}_2^n} \omega^{g_\alpha(\lambda) \boxplus \overline{g_{\alpha'}(\lambda)} \boxplus f_\beta(\lambda) \boxplus \overline{f_{\beta'}(\lambda)}} \end{aligned} \tag{7}$$

is an exponential sum similar to Eq. (5).

For a string $\alpha = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}_2^n$, we define a set

$$\mathcal{B}^\alpha := \left\{\left|\Psi_\beta^\alpha\right\rangle \,\middle|\, \beta \in \mathbb{Z}_2^n\right\} \tag{8}$$

of vectors of Eq. (6). If the absolute values of the exponential sums of Eqs. (7),

$$\left|S_{\beta,\beta'}^{\alpha,\alpha'}\right| = \sqrt{2^n}\,(1 - \delta_{\alpha,\alpha'}) + 2^n\, \delta_{\alpha,\alpha'}\, \delta_{\beta,\beta'}, \tag{9}$$

where $\delta_{\alpha,\alpha'} = \prod_{m=1}^{n} \delta_{a_m,a_m'}$ is the Kronecker delta-function of $2n$ binary variables, then every $\mathcal{B}^\alpha$ of Eq. (8) is an orthonormal basis of the Hilbert space $\mathcal{H}_2^n$, and $\mathcal{B}^\alpha$ and $\mathcal{B}^{\alpha'}$ $(\alpha \neq \alpha')$ are mutually unbiased.

One can check that the orthogonality of vectors [$\alpha = \alpha'$ in Eqs. (7) and (9)] in a basis $\mathcal{B}^\alpha$ is achieved if the following conditions are fulfilled:

(i) The set $F^{(n)}$ constitutes an Abelian group under modulo-4 addition.

(ii) The elements of $F^{(n)}$ fulfill

$$\overline{f_\beta} = f_\beta \quad \text{for all} \quad \beta \in \mathbb{Z}_2^n \tag{10}$$

and

$$S_\beta = \sum_{\lambda\in\mathbb{Z}_2^n} \omega^{f_\beta(\lambda)} = \begin{cases} 2^n & \text{for} \quad \beta = 0, \\ 0 & \text{for} \quad \beta \neq 0. \end{cases} \tag{11}$$

Since $\mathbb{Z}_2^n$ is an Abelian group under modulo-2 addition (symbolized by $\oplus$), we can establish an isomorphism $(F^{(n)}, \boxplus) \to (\mathbb{Z}_2^n, \oplus)$, such that $f_\beta \boxplus f_{\beta'} = f_{\beta\oplus\beta'}$ for all $f_\beta, f_{\beta'} \in F^{(n)}$. Observe that, due to Eq. (10) ω^{f_β}, and therefore, the sums S_β are real for every β. The group $F^{(n)}$ is generated by a set $\{f_m\}_{m=1}^n$ of n nonzero polynomials such that $f_\beta(\lambda) := \boxplus_{m=1}^n b_m f_m(\lambda)$ for every $\beta = (b_1, b_2, \ldots, b_n) \in \mathbb{Z}_2^n$.

The bases $\mathcal{B}^\alpha$ and $\mathcal{B}^{\alpha'}$ are made mutually unbiased by imposing the following conditions:

(i) The polynomials $g_\alpha, g_{\alpha'} \in G^{(n)}$ are such that $g_\alpha \boxplus g_{\alpha'} = g_{\alpha''} \boxplus f_\eta$ for some $g_{\alpha''} \in G^{(n)}$, $f_\eta \in F^{(n)}$.

(ii) The elements of $G^{(n)}$ satisfy

$$\overline{g_\alpha} = g_\alpha \boxplus f_\alpha \quad \text{for all} \quad \alpha \in \mathbb{Z}_2^n \tag{12}$$

and

$$\left|S_\beta^\alpha\right| = \left|\sum_{\lambda\in\mathbb{Z}_2^n} \omega^{g_\alpha(\lambda)\boxplus f_\beta(\lambda)}\right| = \begin{cases} S_\beta & \text{for} \quad \alpha = 0,\\ \sqrt{2^n} & \text{for} \quad \alpha\neq 0,\end{cases} \tag{13}$$

where the sum S_β is defined in Eq. (11). Observe that Eq. (12) implies that the choice of the set $G^{(n)}$ depends on $F^{(n)}$, and neither $\omega^{g_\alpha \boxplus f_\beta}$ nor S_β^α is, in general, real. The set $G^{(n)}$ can be generated by n nonzero polynomials $g_m(\lambda)$, $1\leqslant m\leqslant n$, $g_\alpha(\lambda) := \boxplus_{m=1}^n a_m g_m(\lambda)$. Note that the collection $\{g_\alpha \boxplus f_\beta \mid g_\alpha\in G^{(n)}, f_\beta\in F^{(n)}\}$ forms an Abelian group of 2^{2n} polynomials under modulo-4 addition, where $F^{(n)}$ is its subgroup, and $g_\alpha \boxplus F^{(n)} = \{g_\alpha\boxplus f_\beta \mid f_\beta\in F^{(n)}\}$ are its cosets modulo $F^{(n)}$ for every $g_\alpha\in G^{(n)}$.

Then the bases $\mathcal{B}^\alpha$, Eqs. (6) and (8), along with the computational basis $\mathcal{B}_c$ build a complete MUB set for n qubits,

$$\mathbf{M}^{(n)} := \left\{\mathcal{B}^\alpha \,\middle|\, \alpha\in\mathbb{Z}_2^n\right\}\cup\mathcal{B}_c. \tag{14}$$

Both the IW sets (see the Appendix) and the NGSs (see Secs. III A and III B) of MUBs for qubits can be constructed using the above procedure.

For an IW set, $g_\alpha\boxplus f_\beta$ can be, at most, a quadratic polynomial, Eqs. (A1), and hence the sum $S_{\beta,\beta'}^{\alpha,\alpha'}$ of Eq. (7) always has the Gaussian form, Eq. (A2). Every $\mathcal{B}^\alpha$ of an IW set is associated with a unique graph [30,31] with loops (see Fig. 2). A unitarily equivalent set to an IW MUBs, of course, may contain higher-degree polynomials $g_\alpha\boxplus f_\beta$ (for instance, take the unitary operator CCZ from Table I to have an equivalent set); nevertheless, the sums $S_{\beta,\beta'}^{\alpha,\alpha'}$ of Eq. (7) will be the same Gaussian sums as for the IW construction, because unitary transformations do not change the inner products.

In contrast to the family of the GSs of MUBs, higher-degree polynomials, employed to construct the NGSs of MUBs, lead to cubic (and of higher order) sums $S_{\beta,\beta'}^{\alpha,\alpha'}$. Thus, the NGSs are unitarily inequivalent to the GSs, and about half of the bases of a NGS are related to hypergraphs [34] (see Fig. 1).

Let us proceed with the explicit constructions of the NGSs of MUBs for qubits. Obviously, there are no inequivalent sets of the form (6), (8), and (14) to the two-qubit IW MUB set, since $S_{\beta,\beta'}^{\alpha,\alpha'}$ of Eq. (7) cannot be more than quadratic. However, for $n\geqslant 3$ qubits, the sums can be made cubic (or of higher degree), leading to unitary inequivalent sets of MUBs.

A. NGS of MUBs for three qubits

For a system of $n=3$ qubits, a general polynomial is of the form

$$\begin{aligned} p(\lambda) = {} & c_{123}(l_1l_2l_3)\\ & \boxplus c_{12}(l_1l_2)\boxplus c_{23}(l_2l_3)\boxplus c_{31}(l_3l_1)\\ & \boxplus c_1(l_1)\boxplus c_2(l_2)\boxplus c_3(l_3), \end{aligned} \tag{15}$$

which is completely specified by the values of $c\in\mathbb{Z}_4$ coefficients. Note that Eq. (15), in which the labels of qubits appear in the subscripts of c (and l), is just a different way to express Eq. (1). Nonzero values of the coefficients c_{123}, c_{ij}, and c_i give three-, two-, and one-qubit unitary operations, respectively (see Table I).

For the three-qubit NGS of MUBs, we present the sets $F_{\mathrm{NGS}}^{(3)}$ and $G_{\mathrm{NGS}}^{(3)}$ of polynomials in Tables II and III, respectively. The hypergraphs associated with $g_\alpha\in G_{\mathrm{NGS}}^{(3)}$, which represent the unitary operations U_{g_α} of Eqs. (3), are shown in Fig. 1. Here, all the polynomials are of the form of Eq. (15) and are described by the values of the coefficients c in the tables. Nonzero polynomials f_β are expressed as modulo-4 additions of the

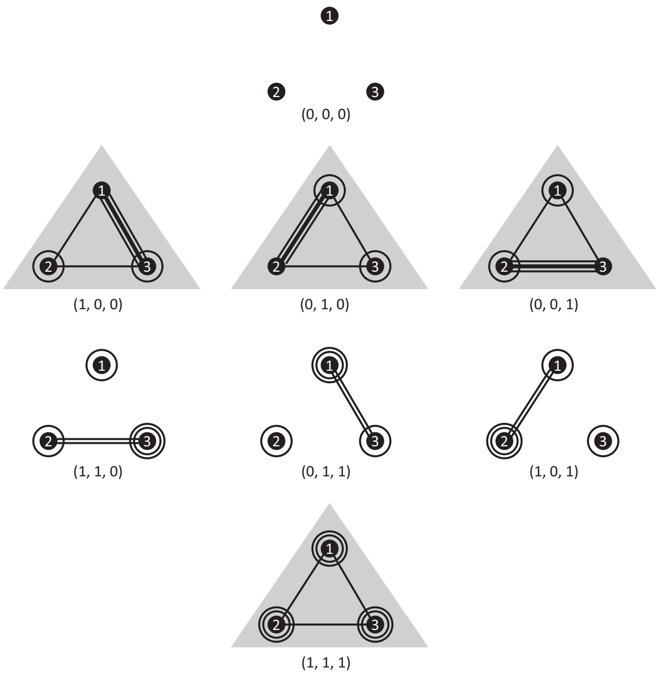

FIG. 1. The hypergraphs that represent the unitary operations U_{g_α} of Eqs. (3) associated with $g_\alpha\in G_{\mathrm{NGS}}^{(3)}$. Here, every hypergraph is marked by $\alpha=(a_1,a_2,a_3)$, and the labels of qubits are indicated at the vertices of each hypergraph. The coefficients c listed in Table III are represented as follows: the gray triangle depicting the operator CCZ_{123} from Table I corresponds to $c_{123}=2$; the bonds between the ith and the jth vertices are associated with c_{ij}, the number of bonds is equal to the value of c_{ij}, and each bond stands for the operator CP_{ij} from Table I; and one loop or two loops around the ith vertex are used for $c_i=1$ or $c_i=2$, respectively, and each loop illustrates the P_i operator from Table I.

TABLE II. The set $F_{\mathrm{NGS}}^{(3)}=\{f_\beta\}_{\beta\in\mathbb{Z}_2^3}$ for the three-qubit NGS of MUBs. Each polynomial of the set is of the form of Eq. (15) and defined by the values of its coefficients provided in the rightmost six columns. The degree of every nonzero f_β is either 2 or 1. In the first column, the labels of polynomials, binary strings $\beta=(b_1,b_2,b_3)$, are listed, and every polynomial (except the zero polynomial f_0) is described in terms of the modulo-4 sum of the generating polynomials f_1, f_2, and f_3 in the second column.

β	f_β	c_{12}	c_{23}	c_{31}	c_1	c_2	c_3
(0,0,0)	f_0	0	0	0	0	0	0
(1,0,0)	f_1	2	2	2	0	2	2
(0,1,0)	f_2	2	2	2	2	0	2
(0,0,1)	f_3	2	2	2	2	2	0
(1,1,0)	$f_1\boxplus f_2$	0	0	0	2	2	0
(0,1,1)	$f_2\boxplus f_3$	0	0	0	0	2	2
(1,0,1)	$f_3\boxplus f_1$	0	0	0	2	0	2
(1,1,1)	$f_1\boxplus f_2\boxplus f_3$	2	2	2	0	0	0

TABLE III. The set $G^{(3)}_{\text{NGS}}=\{g_\alpha\}_{\alpha\in\mathbb{Z}_2^3}$ of polynomials for the three-qubit NGS of MUBs. Here, the degree of a nonzero polynomial is either 3 or 2. The first column carries the labels $\alpha=(a_1,a_2,a_3)$, and in the second column, each member of the set (except g_0) is listed as a modulo-4 addition of the generating polynomials g_1, g_2, and g_3. The remaining columns list the values of the coefficients c of the polynomials g_α. Hypergraphs related to g_α are displayed in Fig. 1.

α	g_α	c_{123}	c_{12}	c_{23}	c_{31}	c_1	c_2	c_3
(0,0,0)	g_0	0	0	0	0	0	0	0
(1,0,0)	g_1	2	1	1	3	0	1	1
(0,1,0)	g_2	2	3	1	1	1	0	1
(0,0,1)	g_3	2	1	3	1	1	1	0
(1,1,0)	$g_1\boxplus g_2$	0	0	2	0	1	1	2
(0,1,1)	$g_2\boxplus g_3$	0	0	0	2	2	1	1
(1,0,1)	$g_3\boxplus g_1$	0	2	0	0	1	2	1
(1,1,1)	$g_1\boxplus g_2\boxplus g_3$	2	1	1	1	2	2	2

generating polynomials f_1, f_2, and f_3 in Table II. Similarly, the nonzero polynomial g_α as the modulo-4 addition of g_1, g_2, and g_3 is given in Table III. It follows from the tables and Fig. 1 that, under the permutation of qubits $1\to 2\to 3\to 1$, the polynomials are transformed as $f_1\to f_2\to f_3\to f_1$ and $g_1\to g_2\to g_3\to g_1$.

One can verify that the sets $F^{(3)}_{\text{NGS}}$ and $G^{(3)}_{\text{NGS}}$ fulfill the requirements given in Eqs. (10)–(13). Thus, $\mathbf{M}^{(3)}_{\text{NGS}}$ from Eq. (14) is a complete set of three-qubit NGS of MUBs, where every $\mathcal{B}^\alpha_{\text{NGS}}$ is constructed by taking f_β and g_α from Tables II and III, respectively.

The three-qubit IW MUBs $\mathbf{M}^{(3)}_{\text{IW}}$ are defined by the polynomials of $F^{(3)}_{\text{IW}}$ and $G^{(3)}_{\text{IW}}$ listed in Tables VIII and IX. In Fig. 2, the graphs linked to $G^{(3)}_{\text{IW}}$ are displayed. The sums $S^{\alpha,\alpha'}_{\beta,\beta'}$, defined in Eq. (7), satisfy Eq. (9) for both $\mathbf{M}^{(3)}_{\text{NGS}}$ and $\mathbf{M}^{(3)}_{\text{IW}}$. Moreover, the sums are always quadratic for the IW MUBs, while they can be cubic for the NGS of MUBs. Therefore, $\mathbf{M}^{(3)}_{\text{NGS}}$ is unitarily inequivalent to $\mathbf{M}^{(3)}_{\text{IW}}$ and to every GS of MUBs.

For the IW MUBs, every nonzero $f_\beta\in F^{(3)}_{\text{IW}}$ is a linear polynomial (see Table VIII in the Appendix), therefore, all the vectors within each basis of $\mathbf{M}^{(3)}_{\text{IW}}$ are locally equivalent to each other and, thus, bear the same factorization structure (and quantity of quantum entanglement). While for the NGS of MUBs, half of the polynomials of $F^{(3)}_{\text{NGS}}$ are quadratic (see Table II), with the same quadratic part $2(l_1l_2\boxplus l_2l_3\boxplus l_3l_1)$, and the rest of the nonzero polynomials f_β are linear. Thus, $F^{(3)}_{\text{NGS}}$ is divided into two disjoint subsets of the same cardinality: one contains all the quadratic polynomials and the other contains the rest. As a result, every basis $\mathcal{B}^\alpha_{\text{NGS}}$ consists of two blocks of vectors corresponding to the subsets of $F^{(3)}_{\text{NGS}}$. The state vectors are locally equivalent within each block, but not across blocks. In other words, every basis of $\mathbf{M}^{(3)}_{\text{NGS}}$ (except the computational) possesses a two-block factorization structure.

There are two more important differences between $\mathbf{M}^{(3)}_{\text{IW}}$ and $\mathbf{M}^{(3)}_{\text{NGS}}$:

(i) Any three nonzero polynomials from Table VIII generate (by modulo-4 addition) the same $F^{(3)}_{\text{IW}}$. Furthermore, any choice of three degree 2 polynomials from Table IX leads to a set similar to $G^{(3)}_{\text{IW}}$ in the sense that we get the same $\mathbf{M}^{(3)}_{\text{IW}}$. On the other hand, for $\mathbf{M}^{(3)}_{\text{NGS}}$, one cannot get the quadratic polynomials of $F^{(3)}_{\text{NGS}}$ by adding the linear polynomials from Table II and get the cubic polynomials of $G^{(3)}_{\text{NGS}}$ by summing the quadratic polynomials from Table III. In particular, the choice of the generating set $\{g_m\}_{m=1}^3$ is unique in the case of NGS but not in the IW case.

(ii) Every basis in $\mathbf{M}^{(3)}_{\text{IW}}$ is a common eigenbasis of a disjoint class of 2^3-1 mutually commuting (except the identity) operations of the three-qubit Pauli group [18]: for $\mathcal{B}_c$ and $\mathcal{B}^0_{\text{IW}}$, the disjoint classes are obtained by multiplying the operators from $\{ZII,IZI,IIZ\}$ and $\{XII,IXI,IIX\}$, respectively, where I, X, Y, and Z are the standard single-qubit Pauli

TABLE IV. The set $F^{(4)}_{\text{NGS}}=\{f_\beta\}_{\beta\in\mathbb{Z}_2^4}$ for the four-qubit NGS of MUBs. All the polynomials of $F^{(4)}_{\text{NGS}}$ are of the form of Eq. (18) and presented in the same way as $F^{(3)}_{\text{NGS}}$ in Table II. Here, every nonzero f_β is of either degree 3 or degree 1.

β	f_β	c_{123}	c_{124}	c_{134}	c_{234}	c_{12}	c_{34}	c_{14}	c_{23}	c_{13}	c_{24}	c_1	c_2	c_3	c_4
(0,0,0,0)	f_0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(1,0,0,0)	f_1	2	2	2	2	2	2	2	2	2	2	0	2	2	2
(0,1,0,0)	f_2	2	2	2	2	2	2	2	2	2	2	2	0	2	2
(0,0,1,0)	f_3	2	2	2	2	2	2	2	2	2	2	2	2	0	2
(0,0,0,1)	f_4	2	2	2	2	2	2	2	2	2	2	2	2	2	0
(1,1,0,0)	$f_1\boxplus f_2$	0	0	0	0	0	0	0	0	0	0	2	2	0	0
(0,0,1,1)	$f_3\boxplus f_4$	0	0	0	0	0	0	0	0	0	0	0	0	2	2
(1,0,0,1)	$f_1\boxplus f_4$	0	0	0	0	0	0	0	0	0	0	2	0	0	2
(0,1,1,0)	$f_2\boxplus f_3$	0	0	0	0	0	0	0	0	0	0	0	2	2	0
(1,0,1,0)	$f_1\boxplus f_3$	0	0	0	0	0	0	0	0	0	0	2	0	2	0
(0,1,0,1)	$f_2\boxplus f_4$	0	0	0	0	0	0	0	0	0	0	0	2	0	2
(1,1,1,0)	$f_1\boxplus f_2\boxplus f_3$	2	2	2	2	2	2	2	2	2	2	0	0	0	2
(1,1,0,1)	$f_1\boxplus f_2\boxplus f_4$	2	2	2	2	2	2	2	2	2	2	0	0	2	0
(1,0,1,1)	$f_1\boxplus f_3\boxplus f_4$	2	2	2	2	2	2	2	2	2	2	0	2	0	0
(0,1,1,1)	$f_2\boxplus f_3\boxplus f_4$	2	2	2	2	2	2	2	2	2	2	2	0	0	0
(1,1,1,1)	$f_1\boxplus f_2\boxplus f_3\boxplus f_4$	0	0	0	0	0	0	0	0	0	0	2	2	2	2

TABLE V. The set $G_{\mathrm{NGS}}^{(4)} = \{g_\alpha\}_{\alpha\in\mathbb{Z}_2^4}$ for the four-qubit NGS of MUBs. The degree of a nonzero g_α is $\leqslant 3$. The polynomials of $G_{\mathrm{NGS}}^{(4)}$ are described in the same fashion as the polynomials of $G_{\mathrm{NGS}}^{(3)}$ in Table III and are of the form of Eq. (18).

α	g_α	c_{123}	c_{124}	c_{134}	c_{234}	c_{12}	c_{34}	c_{14}	c_{23}	c_{13}	c_{24}	c_1	c_2	c_3	c_4
(0,0,0,0)	g_0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
(1,0,0,0)	g_1	3	3	3	3	3	3	1	3	1	1	0	1	1	1
(0,1,0,0)	g_2	3	3	3	3	3	3	3	1	1	1	1	0	1	1
(0,0,1,0)	g_3	1	1	1	1	3	1	1	3	1	1	1	1	0	1
(0,0,0,1)	g_4	1	1	1	1	3	1	3	1	1	1	1	1	1	0
(1,1,0,0)	$g_1 \boxplus g_2$	2	2	2	2	2	2	0	0	2	2	1	1	2	2
(0,0,1,1)	$g_3 \boxplus g_4$	2	2	2	2	2	2	0	0	2	2	2	2	1	1
(1,0,0,1)	$g_1 \boxplus g_4$	0	0	0	0	2	0	0	0	2	2	1	2	2	1
(0,1,1,0)	$g_2 \boxplus g_3$	0	0	0	0	2	0	0	0	2	2	2	1	1	2
(1,0,1,0)	$g_1 \boxplus g_3$	0	0	0	0	2	0	2	2	2	2	1	2	1	2
(0,1,0,1)	$g_2 \boxplus g_4$	0	0	0	0	2	0	2	2	2	2	2	1	2	1
(1,1,1,0)	$g_1 \boxplus g_2 \boxplus g_3$	3	3	3	3	1	3	1	3	3	3	2	2	2	3
(1,1,0,1)	$g_1 \boxplus g_2 \boxplus g_4$	3	3	3	3	1	3	3	1	3	3	2	2	3	2
(1,0,1,1)	$g_1 \boxplus g_3 \boxplus g_4$	1	1	1	1	1	1	1	3	3	3	2	3	2	2
(0,1,1,1)	$g_2 \boxplus g_3 \boxplus g_4$	1	1	1	1	1	1	3	1	3	3	3	2	2	2
(1,1,1,1)	$g_1 \boxplus g_2 \boxplus g_3 \boxplus g_4$	0	0	0	0	0	0	0	0	0	0	3	3	3	3

operators (the tensor product sign ⊗ between two single-qubit operators is omitted throughout the paper). For $\alpha \neq 0$, $\mathcal{B}_{\mathrm{IW}}^{\alpha}$ can be realized by applying unitary operators U_{g_α} of Eqs. (3) on $\mathcal{B}_{\mathrm{IW}}^{0}$, where $g_\alpha \in G_{\mathrm{IW}}^{(3)}$. In the IW case, every U_{g_α} is a composition of operators from the Clifford group, which is the normalizer of the Pauli group.

For $\mathbf{M}_{\mathrm{NGS}}^{(3)}$, $\mathcal{B}_{\mathrm{NGS}}^{0}$ can be obtained by applying the unitary transformation

$$\begin{aligned} V = XXX &- (\,|000\rangle\langle 111| + |111\rangle\langle 000|\,) \\ &+ (\,|000\rangle\langle 000| + |111\rangle\langle 111|\,) \end{aligned} \tag{16}$$

to $\mathcal{B}_{\mathrm{IW}}^{0}$. One can observe that V is not an element of the Clifford group, and (under conjugation) it maps the Pauli operators to some linear combinations of operators from the Pauli group:

$$\begin{aligned} V\big(XII\big)V^\dagger &= \tfrac{1}{2}(XII - XZZ + IXX - IYY), \\ V\big(IXI\big)V^\dagger &= \tfrac{1}{2}(IXI - ZXZ + XIX - YIY), \\ V\big(IIX\big)V^\dagger &= \tfrac{1}{2}(IIX - ZZX + XXI - YYI). \end{aligned} \tag{17}$$

The disjoint class of $2^3 - 1$ commuting operators (defining the basis $\mathcal{B}_{\mathrm{NGS}}^{0}$) is created by multiplying the operators from the right-hand side of Eqs. (17). The commuting operators, except $V\big(XXX\big)V^\dagger = XXX$, cannot be reduced into the tensor products of single-qubit operators.

Similarly to the IW MUBs, for $\alpha \neq 0$, $\mathcal{B}_{\mathrm{NGS}}^{\alpha}$ can be obtained by applying the unitary operator U_{g_α} from Eqs. (3) to $\mathcal{B}_{\mathrm{NGS}}^{0}$, where $g_\alpha \in G_{\mathrm{NGS}}^{(3)}$. Note that U_{g_α} does not belong to the Clifford group when g_α is a cubic polynomial. In other words, every basis in $\mathbf{M}_{\mathrm{NGS}}^{(3)}$ is a common eigenbasis (with eigenvalues ±1) of a disjoint class of $2^3 - 1$ commuting unitary operators not, in general, belonging to the Pauli group, although every operator is a linear combination of the Pauli operators.

B. NGSs of MUBs for four and five qubits

Although we do not yet have a general procedure to construct a full NGS of MUBs for n qubits, in this subsection we show that our scheme is not limited to the three-qubit case only. Here, we present the NGSs for four and five qubits in the same manner as used in the previous subsection.

TABLE VI. The generating set $\{f_m\}_{m=1}^{5}$ of $F_{\mathrm{NGS}}^{(5)}$ for the five-qubit NGS of MUBs. As in Tables II and IV, the polynomials are expressed here in terms of c coefficients. The second column states that all five coefficients $c_{i_1i_2i_3i_4}$ associated with the four-degree monomials $\big(l_{i_1}l_{i_2}l_{i_3}l_{i_4}\big)$ have the same value **2** for every f_m. Therefore, all the generating polynomials of $F_{\mathrm{NGS}}^{(5)}$ are of degree 4. The third column shows that all 10 coefficients $c_{i_1i_2i_3} = \mathbf{2}$ for every f_m; these coefficients are related to the third-degree monomials $\big(l_{i_1}l_{i_2}l_{i_3}\big)$. In the remaining columns, the values of coefficients are explicitly listed.

f_m	$\{c_{i_1i_2i_3i_4}\}$	$\{c_{i_1i_2i_3}\}$	c_{12}	c_{23}	c_{34}	c_{45}	c_{51}	c_{13}	c_{24}	c_{35}	c_{41}	c_{52}	c_1	c_2	c_3	c_4	c_5
f_1	**2**	**2**	2	2	2	2	2	2	2	2	2	2	0	2	2	2	2
f_2	**2**	**2**	2	2	2	2	2	2	2	2	2	2	2	0	2	2	2
f_3	**2**	**2**	2	2	2	2	2	2	2	2	2	2	2	2	0	2	2
f_4	**2**	**2**	2	2	2	2	2	2	2	2	2	2	2	2	2	0	2
f_5	**2**	**2**	2	2	2	2	2	2	2	2	2	2	2	2	2	2	0

TABLE VII. The generating set $\{g_m\}_{m=1}^{5}$ of $G_{\rm NGS}^{(5)}$ for the five-qubit NGS of MUBs. As f_m polynomials are listed in Table VI, g_m polynomials are listed here. Since $c_{12345}=2$ for every g_m, all the generating polynomials are quintic. Here, for every g_m, all 5 coefficients $c_{i_1i_2i_3i_4}=\mathbf{1}$ (second column), and all 10 coefficients $c_{i_1i_2i_3}=\mathbf{3}$ (third column).

g_m	c_{12345}	$\{c_{i_1i_2i_3i_4}\}$	$\{c_{i_1i_2i_3}\}$	c_{12}	c_{23}	c_{34}	c_{45}	c_{51}	c_{13}	c_{24}	c_{35}	c_{41}	c_{52}	c_1	c_2	c_3	c_4	c_5
g_1	2	**1**	**3**	1	3	1	3	1	3	3	1	1	1	0	1	1	1	1
g_2	2	**1**	**3**	1	1	3	1	3	1	3	3	1	1	1	0	1	1	1
g_3	2	**1**	**3**	3	1	1	3	1	1	1	3	3	1	1	1	0	1	1
g_4	2	**1**	**3**	1	3	1	1	3	1	1	1	3	3	1	1	1	0	1
g_5	2	**1**	**3**	3	1	3	1	1	3	1	1	1	3	1	1	1	1	0

For $n=4$ qubits, a general polynomial is of the form

$$\begin{aligned} p(\lambda) = {}& c_{1234}(l_1l_2l_3l_4) \\ & \boxplus c_{123}(l_1l_2l_3) \boxplus c_{124}(l_1l_2l_4) \boxplus c_{134}(l_1l_3l_4) \boxplus c_{234}(l_2l_3l_4) \\ & \boxplus c_{12}(l_1l_2) \boxplus c_{13}(l_1l_3) \boxplus c_{24}(l_2l_4) \\ & \boxplus c_{14}(l_1l_4) \boxplus c_{23}(l_2l_3) \boxplus c_{34}(l_3l_4) \\ & \boxplus c_1(l_1) \boxplus c_2(l_2) \boxplus c_3(l_3) \boxplus c_4(l_4) \qquad (18) \end{aligned}$$

and is determined by the values of its coefficients $c \in \mathbb{Z}_4$. The sets $F_{\rm NGS}^{(4)}$ and $G_{\rm NGS}^{(4)}$ are listed in Tables IV and V, respectively. Both sets of polynomials obey all the constraints imposed by Eqs. (10)–(13), and the corresponding $\mathbf{M}_{\rm NGS}^{(4)}$ [see Eq. (14) for a definition] is a complete four-qubit NGS of MUBs.

In spite of the similarities, the four-qubit case is slightly different from the three-qubit case. There are no degree 4 polynomials in the MUB construction (see Tables IV and V). The generating polynomials are transformed as $f_1 \leftrightarrow f_2$, $f_3 \leftrightarrow f_4$ and $g_1 \leftrightarrow g_2$, $g_3 \leftrightarrow g_4$ under the qubit permutation $1 \leftrightarrow 2$, $3 \leftrightarrow 4$. Unlike $G_{\rm NGS}^{(3)}$, the number of degree 3 polynomials in $G_{\rm NGS}^{(4)}$ is not exactly half of the total number (compare Tables III and V).

Half of the polynomials from $F_{\rm NGS}^{(4)}$ are cubic, so that $\mathbf{M}_{\rm NGS}^{(4)}$ also has a two-block factorization structure. Additionally, some elements of $G_{\rm NGS}^{(4)}$ are cubic polynomials, and the cubic nature of the sums $S_{\beta,\beta'}^{\alpha,\alpha'}$ evidences the unitary inequivalence of $\mathbf{M}_{\rm NGS}^{(4)}$ and $\mathbf{M}_{\rm IW}^{(4)}$ (and any other GS of MUBs). The four-qubit IW MUBs $\mathbf{M}_{\rm IW}^{(4)}$ can be composed by using the generating sets of $F_{\rm IW}^{(4)}$ and $G_{\rm IW}^{(4)}$ given in Tables X and XI, correspondingly.

For $n=5$ qubits, we list in Tables VI and VII only the generating sets for $F_{\rm NGS}^{(5)}$ and $G_{\rm NGS}^{(5)}$. The rest of the polynomials can be retrieved by adding the generating polynomials under modulo-4 arithmetic. Here several properties observed in the three-qubit case reappear: for instance, the qubit permutation $1 \to 2 \to 3 \to 4 \to 5 \to 1$ leads to the following changes in the polynomials: $f_1 \to f_2 \to f_3 \to f_4 \to f_5 \to f_1$ and $g_1 \to g_2 \to g_3 \to g_4 \to g_5 \to g_1$ (see Tables VI and VII). Half of the elements in $F_{\rm NGS}^{(5)}$ are quartic polynomials, and the rest (nonzero) are linear, and thus, a two-block factorization structure occurs. Also, half of the polynomials of $G_{\rm NGS}^{(5)}$ are of degree 5, which leads to quintic exponential sums $S_{\beta,\beta'}^{\alpha,\alpha'}$, Eqs. (7).

IV. OUTLOOK

The standard construction of complete MUB sets in prime power dimensions is naturally related to the underlying finite field structure, which is reflected on both the algebraic [6,10,16,20,23,26,33] and the geometric [27,30,31] levels. The semifield approach [29] leads to MUBs that are unitarily inequivalent, but algebraically similar, to the IW MUBs: they are eventually connected to graphs [32]; all elements of a given basis have the same factorization structure, and the inner products of vectors are the quadratic Gauss sum [25].

The inclusion of higher-order interactions (for instance, the CCZ operator) opens the possibility of constructing sets of MUBs with different mathematical and physical properties.

We have shown in the particular examples of three, four, and five qubits that it is possible to find non-Gaussian complete sets of MUBs which not only are unitarily inequivalent to the entire family of the Gaussian MUB sets, but also have a different factorization structure *inside* each (except the computational) basis. Since there is an intimate relation between MUBs and the optimal measurements [4,5], we expect that the present research may offer a new look at the complementarity problem in finite-dimensional systems.

Finally, this approach to the construction of MUBs in the many-qubit case provides an incentive to expand the study of higher-order exponential sums (Weil sums [35]) and their application in quantum information theory.

ACKNOWLEDGMENTS

This work was supported by Grant No. 106525 from CONACyT, Mexico.

APPENDIX: THE IW MUBS

The existence of a complete set of MUBs [4,5] is demonstrated for any prime-power dimension using a finite Galois

TABLE VIII. The set $F_{\rm IW}^{(3)} = \{f_\beta\}_{\beta\in\mathbb{Z}_2^3}$ of polynomials for the three-qubit IW MUBs. All the polynomials are of the kind of Eq. (15) and are expressed as in Table II. Every nonzero polynomial is linear here.

β	f_β	c_1	c_2	c_3
(0,0,0)	f_0	0	0	0
(1,0,0)	f_1	2	0	0
(0,1,0)	f_2	0	2	0
(0,0,1)	f_3	0	0	2
(1,1,0)	$f_1 \boxplus f_2$	2	2	0
(0,1,1)	$f_2 \boxplus f_3$	0	2	2
(1,0,1)	$f_3 \boxplus f_1$	2	0	2
(1,1,1)	$f_1 \boxplus f_2 \boxplus f_3$	2	2	2

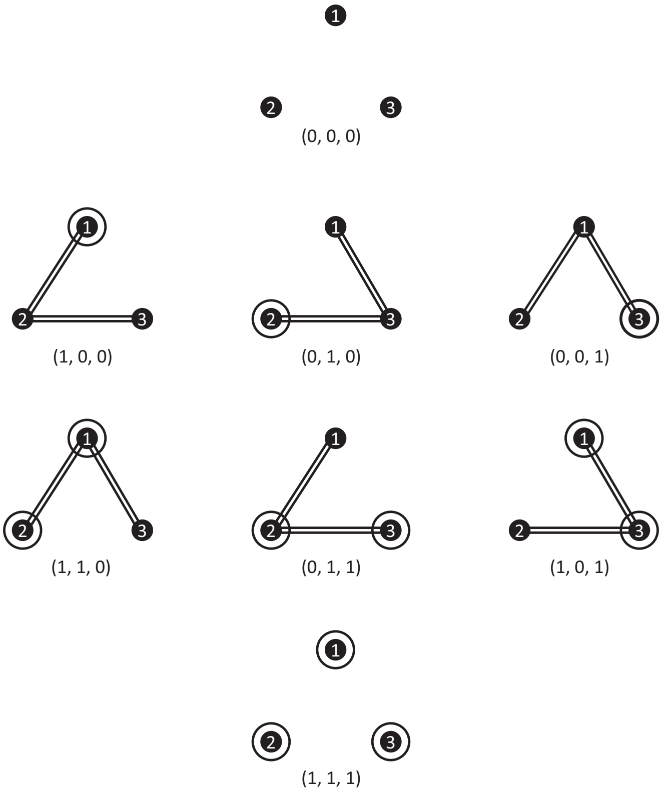

FIG. 2. Graphs illustrating the unitary operations U_{g_α} of Eqs. (3), where $g_\alpha \in G^{(3)}_{\rm IW}$. Like Fig. 1, the graphs—tagged $\alpha = (a_1,a_2,a_3)$—can be explained with the use of Table IX. The vertices of each graph are marked by the labels of qubits. Since there is no cubic polynomial in $G^{(3)}_{\rm IW}$, no gray triangle appears here as in Fig. 1. In Table IX, c_{ij} is either 2 or 0, therefore, we have either two bonds or none between a pair of vertices. In a graph, a vertex has either a loop or no loop, depending on the value, 1 or 0, of the corresponding c_i in Table IX. A single bond and single loop depict the operators CP and P in Table I, respectively.

field [25]. Here, we present the construction of the IW sets for three and four qubits using the formulation given in Sec. III. For an IW set one has

$$f_\beta(\lambda) = 2\,\beta^{\mathsf T}\lambda \quad \text{and}$$
$$g_\alpha(\lambda) = \lambda^{\mathsf T}\big(\oplus_{m=1}^{n}\, a_m A^{(m)}\big)\,\lambda, \tag{A1}$$

where $\beta^{\mathsf T}$ and $\lambda^{\mathsf T}$ are the transpose of binary column vectors β and λ, respectively; $\{A^{(m)}\}_{m=1}^{n}$ is a set of $n \times n$ nonsingular binary matrices, which can be derived from Eq. (18) in [5]; and $\alpha = (a_1,a_2,\ldots,a_n) \in \mathbb{Z}_2^n$. The IW polynomials given in Eqs. (A1) satisfy the conditions of Eqs. (10)–(13), and hence the n-qubit IW set $\mathbf{M}^{(n)}_{\rm IW}$ [defined in Eq. (14)] is obtained.

TABLE IX. The set $G^{(3)}_{\rm IW} = \{g_\alpha\}_{\alpha\in\mathbb{Z}_2^3}$ of polynomials for the three-qubit IW MUBs. Here, each g_α—described by Eq. (15) and presented as in Table III—is not more than a quadratic polynomial.

α	g_α	c_{12}	c_{23}	c_{31}	c_1	c_2	c_3
(0,0,0)	g_0	0	0	0	0	0	0
(1,0,0)	g_1	2	2	0	1	0	0
(0,1,0)	g_2	0	2	2	0	1	0
(0,0,1)	g_3	2	0	2	0	0	1
(1,1,0)	$g_1 \boxplus g_2$	2	0	2	1	1	0
(0,1,1)	$g_2 \boxplus g_3$	2	2	0	0	1	1
(1,0,1)	$g_3 \boxplus g_1$	0	2	2	1	0	1
(1,1,1)	$g_1 \boxplus g_2 \boxplus g_3$	0	0	0	1	1	1

TABLE X. The generating set $\{f_m\}_{m=1}^{4}$ of $F^{(4)}_{\rm IW}$ for the four-qubit IW MUB set. Every f_m is of degree 1, is expressed as in Table II, and is defined by Eq. (18). All other polynomials of $F^{(4)}_{\rm IW}$ are obtained by adding the generating polynomials under modulo-4 arithmetic.

f_m	c_1	c_2	c_3	c_4
f_1	2	0	0	0
f_2	0	2	0	0
f_3	0	0	2	0
f_4	0	0	0	2

The matrices $A^{(m)}$ are symmetric and such that the modulo-2 addition of any two of them is also a nonsingular matrix, $\det(A^{(m)} \oplus A^{(m')}) \neq 0$ for $m \neq m'$ [18]. Furthermore, under modulo-2 arithmetic, the collection of linear combinations $\{\oplus_{m=1}^{n} a_m A^{(m)} \mid \alpha \in \mathbb{Z}_2^n\}$ form an additive Abelian group, and excluding the 0 matrix (for $\alpha = 0$), the collection constitutes a multiplicative Abelian group. All $A^{(m)}$ (and their linear combinations) can be associated with the adjacency matrices of graphs with loops [30,31].

In the IW case, the degree of $g_\alpha(\lambda) \boxplus f_\beta(\lambda)$ cannot be more than 2 [see Eqs. (A1)]. Consequently, the exponential sums of Eq. (7) are the quadratic Gauss sums,

$$S^{\alpha,\alpha'}_{\beta,\beta'} = \sum_{\lambda\in\mathbb{Z}_2^n} \omega^{\lambda^{\mathsf T}[(\alpha-\alpha')\cdot\mathbf{A}]\,\lambda\,\boxplus\,2\,(\beta-\beta')^{\mathsf T}\lambda}, \tag{A2}$$

where $(\alpha-\alpha')\cdot\mathbf{A} = \oplus_{m=1}^{n}(a_m - a'_m)\,A^{(m)}$ is an $n \times n$ symmetric nonsingular (provided that $\alpha \neq \alpha'$) binary matrix. The Gaussian sum always meets the required absolute value given in Eq. (9).

Here, we provide Tables VIII and IX for the three-qubit sets $F^{(3)}_{\rm IW}$ and $G^{(3)}_{\rm IW}$, respectively. The polynomials from these sets satisfy the conditions stated in Eqs. (10)–(13) and comprise a complete MUB set $\mathbf{M}^{(3)}_{\rm IW}$ in agreement with Eq. (14). The graphs related to $G^{(3)}_{\rm IW}$ are shown in Fig. 2. We also provide the list of generating polynomials f_m and g_m in Tables X and XI, respectively, used to build the four-qubit IW MUBs $\mathbf{M}^{(4)}_{\rm IW}$.

TABLE XI. The generating set $\{g_m\}_{m=1}^{4}$ of $G^{(4)}_{\rm IW}$ for the four-qubit IW MUB set. Every g_m is presented as in Table III, is defined by Eq. (18), and is quadratic. If the qubits are permuted as 1 ↔ 3 and 2 ↔ 4, then the changes $g_1 \leftrightarrow g_3$ and $g_2 \leftrightarrow g_4$ occur. All other polynomials of $G^{(4)}_{\rm IW}$ are built by modulo-4 addition of the generating polynomials.

g_m	c_{12}	c_{34}	c_{14}	c_{23}	c_{13}	c_{24}	c_1	c_2	c_3	c_4
g_1	0	0	2	0	2	2	1	0	0	0
g_2	2	2	0	2	2	0	0	1	0	0
g_3	0	0	0	2	2	2	0	0	1	0
g_4	2	2	2	0	2	0	0	0	0	1

[1] J. Schwinger, Proc. Natl. Acad. Sci. U.S.A. **46**, 570 (1960).

[2] N. Bohr, Phys. Rev. **48**, 696 (1935).

[3] K. Kraus, Phys. Rev. D **35**, 3070 (1987).

[4] I. D. Ivanovic, J. Phys. A: Math. Gen. **14**, 3241 (1981).

[5] W. K. Wootters and B. D. Fields, Ann. Phys. NY **191**, 363 (1989).

[6] W. K. Wootters, Found. Phys. **36**, 112 (2006).

[7] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).

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

[9] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).

[10] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).

[11] L. Vaidman, Y. Aharonov, and D. Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987).

[12] B.-G. Englert and Y. Aharonov, Phys. Lett. A **284**, 1 (2001).

[13] P. K. Aravind, Naturforschung. A: Phys. Sci. **58a**, 85 (2003).

[14] O. Schulz, R. Steinhübl, M. Weber, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, Phys. Rev. Lett. **90**, 177901 (2003).

[15] G. Kimura, H. Tanaka, and M. Ozawa, Phys. Rev. A **73**, 050301 (2006).

[16] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, Int. J. Quantum. Inform. **8**, 535 (2010).

[17] S. Chaturvedi, Phys. Rev. A **65**, 044301 (2002).

[18] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and V. Vatan, Algorithmica **34**, 512 (2002).

[19] J. Lawrence, C. Brukner, and A. Zeilinger, Phys. Rev. A **65**, 032320 (2002).

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

[21] T. Durt, J. Phys. A **38**, 5267 (2005).

[22] M. Planat and H. Rosu, Eur. Phys. J. D **36**, 133 (2005).

[23] A. B. Klimov, L. L. Sánchez-Soto, and H. de Guise, J. Phys. A: Math. Gen. **38**, 2747 (2005).

[24] M. R. Kibler and M. Planat, Int. J. Mod. Phys. B **20**, 1802 (2006).

[25] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications* (Cambridge University Press, Cambridge, 1986).

[26] A. B. Klimov, J. L. Romero, G. Björk, and L. L. Sánchez-Soto, J. Phys. A: Math. Theor. **40**, 3987 (2007).

[27] A. B. Klimov, J. L. Romero, G. Björk, and L. L. Sánchez-Soto, Ann. Phys. **324**, 53 (2009).

[28] J. L. Romero, G. Björk, A. B. Klimov, and L. L. Sánchez-Soto, Phys. Rev. A **72**, 062310 (2005).

[29] W. M. Kantor, J. Math. Phys. **53**, 032204 (2012).

[30] A. B. Klimov, C. Muñoz, and L. L. Sánchez-Soto, J. Phys. A: Math. Theor. **45**, 215303 (2012).

[31] C. Spengler and B. Kraus, Phys. Rev. A **88**, 052323 (2013).

[32] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).

[33] A. Garcia, J. L. Romero, and A. B. Klimov, J. Phys. A **43**, 385301 (2010)

[34] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, New J. Phys. **15**, 113022 (2013).

[35] N. M. Korobov, *Exponential Sums and Their Applications.* Vol. 80, Mathematics and Its Applications (Springer, Berlin, 1992) [Soviet Series].