Invariants of the local Clifford group

Maarten Van den Nest,* Jeroen Dehaene, and Bart De Moor
EAST-SCD, K. U. Leuven, Kasteelpark Arenberg 10, B-3001 Leuven, Belgium

(Received 8 October 2004; published 16 February 2005)

We study the algebra of complex polynomials which remain invariant under the action of the local Clifford group under conjugation. Within this algebra, we consider the linear spaces of homogeneous polynomials degree by degree and construct bases for these vector spaces for each degree, thereby obtaining a generating set of polynomial invariants. Our approach is based on the description of Clifford operators in terms of linear operations over GF(2). Such a study of polynomial invariants of the local Clifford group is mainly of importance in quantum coding theory, in particular in the classification of binary quantum codes. Some applications in entanglement theory and quantum computing are briefly discussed as well.

DOI: 10.1103/PhysRevA.71.022310 PACS number(s): 03.67.Lx

I. INTRODUCTION

The (local) Clifford group plays an important role in numerous theoretical investigations, as well as applications, in quantum information theory, quantum computing and quantum error correction [1–7]. The Clifford group $\mathcal{C}_1$ on one qubit consists of all 2×2 unitary operators which map the Pauli group $\mathcal{G}_1=\langle\sigma_1,\sigma_2,\sigma_3\rangle$ to itself under conjugation, where $\sigma_1,\sigma_2,\sigma_3$ are the Pauli matrices. In other words, $\mathcal{C}_1$ is the normalizer of $\mathcal{G}_1$ in the unitary group U (2). The local Clifford group $\mathcal{C}_n^l$ on n qubits, which is our topic of interest in the following, is the n-fold tensor product of $\mathcal{C}_1$ with itself.

In this paper we study the *invariant algebra* of the local Clifford group, defined as follows: let $\{\rho_{ij}\}$ be a set of 2^{2n} variables, which are assembled in a $2^n\times 2^n$ matrix $\rho=(\rho_{ij})$. The invariant algebra of $\mathcal{C}_n^l$ then consists of all complex polynomials $F(\rho)=F(\rho_{11},\rho_{12},\ldots,\rho_{2^n2^n})$ which remain invariant under the substitutions $\rho\rightarrow U\rho U^\dagger$, for every $U\in\mathcal{C}_n^l$.[1] It is our goal to construct a generating set of this algebra.

This research started out as the groundwork for the study of equivalence classes of binary quantum stabilizer codes, the latter being a large and extensively studied class of quantum codes [8]. A stabilizer code is a joint eigenspace of a set of commuting observables in the Pauli group on n qubits and is described by the projector $\rho_{\mathcal{S}}$ on this subspace. Two stabilizer codes $\rho_{\mathcal{S}}$ and $\rho_{\mathcal{S}'}$ on n qubits are called equivalent if there exists a local unitary operator $U\in\mathrm{U}(2)^{\otimes n}$ such that $U\rho_{\mathcal{S}}U^\dagger$ is equal to $\rho_{\mathcal{S}'}$ modulo a permutation of the n qubits. A natural question to ask is how the equivalence class of a code can be characterized by a minimal set of invariants—i.e., (polynomial) functions $F(\rho_{\mathcal{S}})$ in the entries of the matrix $\rho_{\mathcal{S}}$ which take on equal values for equivalent codes. This is, however, a difficult and unsolved problem. Therefore, given the explicit connections between stabilizer codes, the Pauli group and the Clifford group, it seems natural to consider a restricted version of this equivalence relation, where only operators $U\in\mathcal{C}_n^l$ are considered, and this is where the invariant algebra of $\mathcal{C}_n^l$ comes into play. What is more, it is to date unclear whether this restriction *is* in fact a restriction at all: indeed, the question exists whether every two equivalent stabilizer codes are also equivalent in this second, restricted sense. A possible way towards solving this problem is through a study of invariants (cf. also [9]). Moreover, the problem of recognizing local unitary and/or local Clifford equivalence of certain classes of multipartite pure quantum states (stabilizer states, graph states) has recently gained attention both in entanglement theory [3,5,6] and in the one-way quantum computing model [10]. These examples make for a number of application domains of the present work.

From a somewhat different perspective, the invariant theory of the Clifford group is also of interest from a purely mathematical point of view. Runge [11] and Nebe, Rains, and Sloane [12,13] published a series of papers in which they investigate the connection between the invariants of the (entire) Clifford group (and generalizations thereof) and the so-called generalized weight polynomials of a class of self-dual *classical* binary codes. Their work is a considerable generalization of a central result in classical coding theory, known as Gleason's theorem [14], which states that the invariant algebra of $\mathcal{C}_1$ is generated by the weight enumerators of the class of doubly even self-dual classical codes (the definition of the invariant algebra of $\mathcal{C}_1$ is here somewhat different than ours; cf. footnote[1]). It is interesting that the Clifford group—a group which appears naturally in a quantum theoretical setting—has such a connection, through invariant theory, with the theory of *classical* codes. It is not known whether this link is a mere coincidence or a manifestation of some deeper result [15]. This remark may serve as another justification of the present research.

In our study of the invariant algebra of $\mathcal{C}_n^l$, we will make extensive use of the description of this group in terms of binary linear algebra—i.e., algebra over the field $\mathrm{GF}(2)=\mathbb{F}_2$. It is indeed well known that n-qubit (local) Clifford operations can be represented elegantly by a certain class of $2n\times 2n$ linear operators over $\mathbb{F}_2$ [1,4] and this binary picture makes the (local) Clifford group particularly manageable in the following. In order to obtain a generating set of the in-

*Electronic address: mvandenn@esat.kuleuven.ac.be

[1] To be exact, in the literature the invariant algebra of a $N\times N$ matrix group G is usually defined as the set of all polynomials $p(x)=p(x_1,\ldots,x_1)$ such that $p(Ax)=p(x)$ for every $A\in G$. Our definition is a variant of this.

variant algebra, we will adopt the following basic strategy: note that each invariant polynomial F (simply called *invariant*) can be written as a sum of its homogeneous components, each of which is an invariant as well. One can therefore always find a generating set of the invariant algebra which consists of homogeneous invariants only. Furthermore, the set of homogeneous invariants of fixed degree is a finite-dimensional vector space, as one can easily verify (which gives the algebra of invariants the structure of a graded algebra). Therefore, a natural approach to our problem is to consider these spaces of homogeneous invariants degree by degree and to construct a basis of invariants for each degree. This construction will yield a generating (yet infinite) set of the invariant algebra.

II. LOCAL CLIFFORD GROUP

The *Clifford group* $\mathcal{C}_1$*on one qubit* is the following group of unitary 2×2 matrices:

$$\mathcal{C}_1 = \left\langle \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \right\rangle .$$

The order of $\mathcal{C}_1$ is finite and equal to 192. Up to overall phase factors, the Clifford group consists of all unitary operators which map the *Pauli group* to itself under conjugation; here, the Pauli group $\mathcal{G}_1$ (on one qubit) consists of the identity σ_0 and the three pauli matrices

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

all having four possible overall phase factors equal to ± 1 or $\pm i$. In other words, up to these overall phase factors, the group $\mathcal{C}_1$ is the normalizer of $\mathcal{G}_1$ in the unitary group U (2). Note that these phases are not relevant in the following, since we are considering the action of the Clifford group under conjugation as explained in the Introduction. It follows that every $U \in \mathcal{C}_1$ is, for our purposes, completely described by a permutation $\pi \in S_3$, where S_3 is the symmetric group on three letters, and a set of three phases $\alpha_1, \alpha_2, \alpha_3 = \pm 1$, such that

$$U\sigma_i U^\dagger = \alpha_i \sigma_{\pi(i)} (i = 1,2,3).$$

Moreover, since $\sigma_1\sigma_2 \sim \sigma_3$, one has $\alpha_1\alpha_2\alpha_3 = 1$ and it is therefore sufficient to keep track of only two of the α_i's (say, α_1 and α_3). Another useful characterization of the Clifford group is obtained by considering the mapping

$$\sigma_0 = \sigma_{00} \mapsto (0,0),$$

$$\sigma_1 = \sigma_{01} \mapsto (0,1),$$

$$\sigma_3 = \sigma_{10} \mapsto (1,0),$$

$$\sigma_2 = \sigma_{11} \mapsto (1,1), \qquad (1)$$

which establishes a homomorphism between the groups $\mathcal{G}_1$ and $\mathbb{F}_2^2$. Here, $\mathbb{F}_2$ is the finite field of two elements (0 and 1), where arithmetics are performed modulo 2. In this representation of Pauli matrices by pairs of bits, a Clifford operation corresponds to an invertible linear transformation $Q \in \mathrm{GL}(2,\mathbb{F}_2)$ (instead of a permutation $\pi \in S_3$) and a couple of phases α_1 and α_3. It is this second description of Clifford operations in terms of binary linear transformations which is most often used in the literature in quantum information theory and quantum computing, and we will do the same.

The *local Clifford group* $\mathcal{C}_n^l$ on n qubits is the n-fold tensor product of $\mathcal{C}_1$ with itself—i.e.,

$$\mathcal{C}_n^l = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_1 (n \text{ times}).$$

Analogous to the case of one qubit, the group $\mathcal{C}_n^l$ can be most easily described by its action on the Pauli group $\mathcal{G}_n$ on n qubits, defined by

$$\mathcal{G}_n = \mathcal{G}_1 \otimes \cdots \otimes \mathcal{G}_1 (n \text{ times}).$$

Using the mapping (1), the elements of $\mathcal{G}_n$ can be represented as $2n$-dimensional binary vectors as follows:

$$\sigma_{u_1v_1} \otimes \cdots \otimes \sigma_{u_nv_n} = \sigma_{(u,v)} \mapsto (u,v) \in \mathbb{F}_2^{2n},$$

where $(u,v) = (u_1, \ldots, u_n, v_1, \ldots, v_n)$. As in the case of one single qubit, local Clifford operations map $\mathcal{G}_n$ to itself under conjugation. Therefore, n-qubit local Clifford operations as well can be described in terms of linear operations over $\mathbb{F}_2$. One can readily verify that, in this binary picture, an operator $U \in \mathcal{C}_n^l$ corresponds to an invertible $2n \times 2n$ binary matrix Q of the block form

$$Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix},$$

where the $n \times n$ matrices A,B,C,D are diagonal, and a set of $2n$ phases $\alpha_i = \pm 1$, defined by

$$U\sigma_{e_i}U^\dagger = \alpha_i \sigma_{Qe_i}, \qquad (2)$$

where e_i is the ith canonical basis vector in $\mathbb{F}_2^{2n}$, for every $i = 1, \ldots, 2n$. Denoting the diagonal entries of A,B,C,D, respectively, by a_i, b_i, c_i, d_i, respectively, the n submatrices

$$Q^{(i)} \coloneqq \begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix} \in \mathrm{GL}(2,\mathbb{F}_2)$$

correspond to the tensor factors of U. The group of all such Q is isomorphic to $\mathrm{GL}(2,\mathbb{F}_2)^n$ (and S_3^n).

III. INVARIANT POLYNOMIALS AND MATRIX ALGEBRAS

Let $\{\rho_{ij}\}$ be a set of 2^{2n} variables, which are assembled in a $2^n \times 2^n$ matrix $\rho = (\rho_{ij})$. Any homogeneous polynomial $F(\rho)$ of degree $r \in \mathbb{N}_0$ can be written as a trace

$$F(\rho) = \mathrm{Tr}(A_F \rho^{\otimes r})$$

for some complex $2^{nr} \times 2^{nr}$ matrix A_F. To see this, simply note that the tensor product $\rho^{\otimes r}$ contains all monomials of degree r in the entries ρ_{ij}. The coefficients of these monomials in the polynomial F are encoded in the entries of A_F (note, however, that the correspondence $F \leftrightarrow A_F$ is not one to one). It can easily be verified that $F(U\rho U^{\dagger})=F(\rho)$ for every $U\in\mathcal{C}_n^l$ if and only if there exists an A_F such that

$$U^{\otimes r}A_F(U^{\otimes r})^{\dagger}=A_F \tag{3}$$

for every $U\in\mathcal{C}_n^l$. Therefore, the study of invariant homogeneous polynomials of fixed degree r is transformed to the study of the algebra $\mathcal{A}_{n,r}$ of matrices A_F which satisfy Eq. (3). In this section, we will construct a linear basis of this algebra. This will yield a generating set of homogeneous invariants of degree r.[2] First we consider the simplest case of one single qubit, i.e. $n=1$, and then we move to the general case of arbitrary n.

A. One qubit

Let $r\in\mathbb{N}_0$ and let $\mathcal{R}_r$ be the averaging operator which maps a $2^r\times 2^r$ matrix A to

$$\mathcal{R}_r(A) := \frac{1}{|\mathcal{C}_1|}\sum_{U\in\mathcal{C}_1}U^{\otimes r}A(U^{\otimes r})^{\dagger}.$$

Note that $\mathcal{R}_r$ is the orthogonal projector of the space of $2^r\times 2^r$ matrices onto the subspace $\mathcal{A}_{1,r}$. Therefore, a spanning (though in general nonminimal) set of $\mathcal{A}_{1,r}$ is obtained by fixing a vector space basis of $2^r\times 2^r$ matrices and calculating its image under $\mathcal{R}_r$. In this context, a natural choice for such a basis is the set $\{\sigma_{(u,v)}|u,v\in\mathbb{F}_2^r\}$ of Pauli operators on r qubits (all having an overall phase equal to 1). Before calculating the images $\mathcal{R}_r(\sigma_{(u,v)})$ in lemma 1, we need some definitions: firstly, let the group $\mathrm{GL}(2,\mathbb{F}_2)$ act on $\mathbb{F}_2^{2r}$ as follows:

$$Q\in\mathrm{GL}(2,\mathbb{F}_2):(u,v)\in\mathbb{F}_2^{2r}\mapsto(\overline{u},\overline{v})\in\mathbb{F}_2^{2r}, \tag{4}$$

where $(\overline{u},\overline{v})$ is defined by

$$\begin{bmatrix}\overline{u_j}\\ \overline{v_j}\end{bmatrix}=Q\begin{bmatrix}u_j\\ v_j\end{bmatrix},$$

for every $j=1,\ldots,r$, where $u_j,v_j,\overline{u_j},\overline{v_j}$, respectively, are the components of $u,v,\overline{u},\overline{v}$. Second, let the binary vector space $\mathcal{V}_r$ consist of all $(u,v)\in\mathbb{F}_2^{2r}$ such that

$$\sum_{j=1}^{r}(u_j,v_j)=(0,0).$$

We are now in a position to state the following lemma.

Lemma 1. *Let $r\in\mathbb{N}_0$. Let $(u_0,v_0)\in\mathbb{F}_2^{2r}$ and denote by Γ the orbit of this vector under the action* (4). *Then*

$$\mathcal{R}_r(\sigma_{(u_0,v_0)})=\begin{cases}c\sum_{(u,v)\in\Gamma}\sigma_{(u,v)} & \text{if } (u_0,v_0)\in\mathcal{V}_r\\ 0 & \text{otherwise},\end{cases}$$

where c is a constant.

Proof. Let $U\in\mathcal{C}_1$ be an arbitrary Clifford operation. The action of U on the Pauli matrices is parametrized by coefficients $\alpha_{01},\alpha_{10},\alpha_{11}=\pm 1$ with $\alpha_{01}\alpha_{10}\alpha_{11}=1$ and a linear operator $Q\in\mathrm{GL}(2,\mathbb{F}_2)$ such that $U\sigma_{(a,b)}U^{\dagger}=\alpha_{ab}\sigma_{Q(a,b)}$ for every $(a,b)\in\mathbb{F}_2^2\backslash\{0\}$. Defining the integers n_x,n_y,n_z by

$$n_x=|\{j|(u_{0j},v_{0j})\ =(0,1)\}|,$$

$$n_y=|\{j|(u_{0j},v_{0j})\ =(1,1)\}|,$$

$$n_z=|\{j|(u_{0j},v_{0j})\ =(1,0)\}|,$$

the operator $U^{\otimes r}$ maps $\sigma_{(u_0,v_0)}$ to

$$\alpha_{01}^{n_x}\alpha_{10}^{n_z}\alpha_{11}^{n_y}\sigma_{(\overline{u_0},\overline{v_0})}=\alpha_{01}^{n_x+n_y}\alpha_{10}^{n_z+n_y}\sigma_{(\overline{u_0},\overline{v_0})} \tag{5}$$

under conjugation, where $(\overline{u_0},\overline{v_0})\in\Gamma$ is the image of (u_0,v_0) under the action (4) of Q. The crucial observation is now that the coefficient of $\sigma_{(\overline{u_0},\overline{v_0})}$ in Eq. (5) is always positive (and thus equal to 1) if and only if both the numbers n_x+n_y and n_z+n_y are even. Note that this occurs if and only if n_x,n_y, and n_z are all even or all odd or, equivalently, if and only if $(u_0,v_0)\in\mathcal{V}_r$, as one can readily verify. It follows that

$$\mathcal{R}_r(\sigma_{(u_0,v_0)})\sim\sum_{(u,v)\in\Gamma}\sigma_{(u,v)}$$

if $(u_0,v_0)\in\mathcal{V}_r$. If $(u_0,v_0)\notin\mathcal{V}_r$, one can easily see that the different terms in the sum $\mathcal{R}_r(\sigma_{(u_0,v_0)})$ interfere such as to yield zero. This ends the proof.

Using the result in lemma 1, we can construct a basis of $\mathcal{A}_{1,r}$. Denote by $\mathcal{O}_r$ the set of all orbits Γ of the elements in $\mathcal{V}_r$ (note that $\mathcal{O}_r$ forms a partition of $\mathcal{V}_r$). For every $\Gamma\in\mathcal{O}_r$, define the matrix

$$A_{\Gamma}:=\sum_{(u,v)\in\Gamma}\sigma_{(u,v)}. \tag{6}$$

By construction, the matrices A_{Γ} linearly generate the algebra $\mathcal{A}_{1,r}$. Moreover, this set of matrices is linearly independent: indeed, this follows immediately from the linear independence of the Pauli operators $\sigma_{(u,v)}$. Therefore, we can conclude that the A_{Γ}'s are a basis of $\mathcal{A}_{1,r}$. In order to calculate the dimension $|\mathcal{O}_r|$ of $\mathcal{A}_{1,r}$, we use the Cauchy-Frobenius orbit-counting lemma, which states that the number of orbits of a finite group G acting on a set X is equal to the average number of fixed points; i.e., the number of orbits is equal to

$$\frac{1}{|G|}\sum_{g\in G}|\mathcal{F}(g)|, \tag{7}$$

where $|\mathcal{F}(g)|$ is the number of fixed points in the set X of the group element g. Let us therefore calculate the number of fixed points of an arbitrary matrix $Q\in\mathrm{GL}(2,\mathbb{F}_2)$ acting on $\mathcal{V}_r$. First, it is trivial that the identity has $|\mathcal{V}_r|=4^{r-1}$ fixed points. Second, there are three elements in $\mathrm{GL}(2,\mathbb{F}_2)$ of order 2. Consider, e.g., the matrix

$$Q_0=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}.$$

When acting on $\mathbb{F}_2^2$, this operator fixes exactly two vectors: namely, (0,0) and (1,1). Therefore, when Q_0 acts on $\mathcal{V}_r$, the set $\mathcal{F}(Q_0)$ consists of all vectors of the form

[2] This set will, however, not be linearly independent in general, due to fact that the description of an invariant $F(\rho)$ by a trace $\mathrm{Tr}(A_F\rho^{\otimes r})$ is nonunique. Bases of invariant polynomials are discussed below.

$$\alpha_1(1,0,\ldots,0;1,0,\ldots,0) + \alpha_2(0,1,\ldots,0;0,1,\ldots,0) + \cdots + \alpha_r(0,0,\ldots,1;0,0,\ldots,1), \tag{8}$$

where $\alpha_i \in \{0,1\}$ for every $i=1,\ldots,r$ and where exactly an even number of α_i's are nonzero. Therefore, the cardinality of $\mathcal{F}(Q_0)$ is equal to the number of even subsets of $\{1,\ldots,r\}$—i.e., $|\mathcal{F}(Q_0)|=2^{r-1}$. Note that an analogous argument holds for the other two matrices of order 2. Finally, there are two elements in $\mathrm{GL}(2,\mathbb{F}_2)$ of order 3, which fix only the zero vector. Gathering these results in the formula (7), we find that the number $|\mathcal{O}_r|$ of orbits is equal to

$$\frac{1}{6}(4^{r-1} + 3 \times 2^{r-1} + 2).$$

We have proven the following.

Theorem 1. Let $r \in \mathbb{N}_0$. The set $\{A_\Gamma\}_{\Gamma\in\mathcal{O}_r}$ is a vector space basis of the algebra $\mathcal{A}_{1,r}$. The dimension $|\mathcal{O}_r|$ of $\mathcal{A}_{1,r}$ is equal to

$$\frac{1}{3}(2^{2r-3} + 3 \times 2^{r-2} + 1). \tag{9}$$

Thus, we have obtained the desired result of constructing a basis of matrices of the algebra $\mathcal{A}_{1,r}$. It will be useful to have an explicit parametrization of the orbits $\Gamma \in \mathcal{O}_r$. Such a parametrization could, e.g., be used to enumerate all the matrices A_Γ for a given degree. Also when we will move from the matrix algebra $\mathcal{A}_{1,r}$ to the polynomials $\mathrm{Tr}(A_\Gamma \rho^{\otimes r})$ in Sec. IV, a more operational description of the A_Γ's will turn out to be very useful. To this end, for each $(u,v) \in \mathbb{F}_2^{2r}$, define the sets

$$\eta_0(u,v) = \{j | (u_j,v_j) = (0,0)\},$$

$$\eta_x(u,v) = \{j | (u_j,v_j) = (0,1)\},$$

$$\eta_y(u,v) = \{j | (u_j,v_j) = (1,1)\},$$

$$\eta_z(u,v) = \{j | (u_j,v_j) = (1,0)\}.$$

Then the following characterization is easily verified: two vectors $(u,v),(u',v') \in \mathbb{F}_2^{2r}$ belong to the same orbit if and only if

(a) $\eta_0(u,v)=\eta_0(u',v')$ and

(b) there exists a permutation π of $\{x,y,z\}$ such that $\eta_x(u',v')=\eta_{\pi(x)}(u,v)$, $\eta_y(u',v')=\eta_{\pi(y)}(u,v)$, and $\eta_z(u',v')=\eta_{\pi(z)}(u,v)$.

This implies that any orbit Γ of the action (4) can completely be described by

(a′) a set $\eta_0(\Gamma) \subseteq \{1,\ldots,r\}$ and

(b′) a partition $\mathcal{P}(\Gamma)=\{\eta_1,\eta_2,\eta_3\}$ of $\{1,\ldots,r\}\setminus\eta_0(\Gamma)$ into three (possibly empty) subsets, such that $(u,v)\in\Gamma$ if and only if $\eta_0(u,v)=\eta_0(\Gamma)$ and $\{\eta_x(u,v),\eta_y(u,v),\eta_z(u,v)\}=\mathcal{P}(\Gamma)$. Moreover, $\Gamma\in\mathcal{O}_r$ if and only if the numbers $|\eta_1|,|\eta_2|,|\eta_3|$ are either all even or all odd (cfr. proof of lemma 1). Let us illustrate this characterization with two simple examples.

(i) $r=1$: there is one orbit in $\mathcal{O}_1$: namely, $\Gamma_0=\{(0,0)\}\in\mathcal{O}_1$. This orbit is characterized by $\eta_0(\Gamma_0)=\{1\}$ and $\mathcal{P}(\Gamma_0)=\{\emptyset,\emptyset,\emptyset\}$.

(ii) $r=2$: there are two orbits in $\mathcal{O}_2$: namely, $\Gamma=\{(0,0;0,0)\}$ and

$$\Gamma' = \{(0,0;1,1),(1,1;0,0),(1,1;1,1)\} = \{(u,v) \in \mathbb{F}_2^4 | (u_1,v_1) = (u_2,v_2) \neq (0,0)\}.$$

The orbits Γ and Γ' are described by

$$\eta_0(\Gamma) = \{1,2\}, \quad \mathcal{P}(\Gamma) = \{\emptyset,\emptyset,\emptyset\}$$

and

$$\eta_0(\Gamma') = \emptyset, \quad \mathcal{P}(\Gamma') = \{\{1,2\},\emptyset,\emptyset\}.$$

B. Multiple qubits

For arbitrary n, the result in theorem 1 can immediately be used to construct a basis of $\mathcal{A}_{n,r}$. To see this, let us first consider the algebra of $2^{nr}\times 2^{nr}$ matrices A which satisfy

$$U_1^{\otimes r} \otimes \cdots \otimes U_n^{\otimes r} A (U_1^{\otimes r} \otimes \cdots \otimes U_n^{\otimes r})^\dagger = A,$$

for every $U_1,\ldots,U_n \in \mathcal{C}_1$. It is straightforward to show that this algebra is the n-fold tensor product of $\mathcal{A}_{1,r}$ with itself. Therefore, a basis of this algebra is given by the matrices $A_{\Gamma_1}\otimes\cdots\otimes A_{\Gamma_n}$, where Γ_i ranges over all orbits in $\mathcal{O}_r$, for every $i=1,\ldots,n$. In order to obtain a basis of $\mathcal{A}_{n,r}$, one simply has to conjugate this basis with the permutation matrix P, defined by

$$P|i_{11}\ldots i_{1r};i_{21}\ldots i_{2r};\ldots;i_{n1}\ldots i_{nr}\rangle = |i_{11}\ldots i_{n1};i_{12}\ldots i_{n2};\ldots;i_{1r}\ldots i_{nr}\rangle, \tag{10}$$

where $i_{ab}\in\{0,1\}$ and $|i_{11}\ldots\rangle$ are the standard basis vectors in $\mathbb{C}^{2^{nr}}$. Indeed, the matrix P performs the appropriate permutation of tensor factors, mapping $U_1^{\otimes r}\otimes\cdots\otimes U_n^{\otimes r}$ to $(U_1\otimes\cdots\otimes U_n)^{\otimes r}$ under conjugation. This leads to the following result.

Theorem 2. Let $r\in\mathbb{N}$. For every n-tuple $\gamma=(\Gamma_1,\ldots,\Gamma_n)$ of orbits $\Gamma_i\in\mathcal{O}_r$, define the matrix

$$A_\gamma := P A_{\Gamma_1} \otimes \cdots \otimes A_{\Gamma_n} P^T. \tag{11}$$

Then the set $\{A_\gamma\}_\gamma$ forms a vector space basis of $\mathcal{A}_{n,r}$. The dimension of $\mathcal{A}_{n,r}$ is equal to $|\mathcal{O}_r|^n$.

Following the discussion at the end of Sec. III A, the matrices A_γ can be described in an alternative way than Eq. (11), using the description of orbits $\Gamma\in\mathcal{O}_r$ by couples $(\eta_0(\Gamma),\mathcal{P}(\Gamma))$. Defining the *support* of a vector $w\in\mathbb{F}_2^{2n}$ to be the set

$$\mathrm{supp}(w) = \{i \in \{1,\ldots,n\} | (w_i,w_{n+i}) \neq (0,0)\}, \tag{12}$$

one obtains the following.

Theorem 3. Let $\gamma=(\Gamma_1,\ldots,\Gamma_n)$ be an n-tuple of orbits $\Gamma_i\in\mathcal{O}_r$. For every $j,k\in\{1,\ldots,r\}$, $j<k$, define the sets $\omega^{(j)}$ and $\omega^{(jk)}$ by

$$\omega^{(j)} = \{i \in \{1,\ldots,n\} | j \in \eta_0(\Gamma_i)\},$$

$$\omega^{(jk)} = \{i \in \{1,\ldots,n\} | j,k \in \eta_0(\Gamma_i) \text{ or } j \text{ and } k \text{ belong to the same subset of } \mathcal{P}(\Gamma_i)\}. \qquad (13)$$

Then $A_\gamma = \Sigma \sigma_{w^{(1)}} \otimes \cdots \otimes \sigma_{w^{(r)}}$, where the sum runs over all ordered r-tuples $(w^{(1)},\ldots,w^{(r)}) \in (\mathbb{F}_2^{2n})^{\times r}$ satisfying

$$\mathrm{supp}(w^{(j)}) = \overline{\omega}^{(j)}, \qquad (14)$$

$$\mathrm{supp}(w^{(j)} + w^{(k)}) = \overline{\omega}^{(jk)}, \qquad (15)$$

for every $j,k \in \{1,\ldots,r\}, j<k$, where $\overline{\omega}^{(j)}, \overline{\omega}^{(jk)}$ denote the complements of the sets $\omega^{(j)} \omega^{(jk)}$ in $\{1,\ldots,n\}$.

Proof. By definition, A_γ is equal to

$$\sum \sigma_{w^{(1)}} \otimes \cdots \otimes \sigma_{w^{(r)}},$$

where the sum runs over all ordered r-tuples $(w^{(1)},\ldots,w^{(r)}) \in (\mathbb{F}_2^{2n})^{\times r}$ such that

$$(w_i^{(1)},\ldots,w_i^{(r)},w_{n+1}^{(1)},\ldots,w_{n+1}^{(r)}) \in \Gamma_i, \qquad (16)$$

for every $i=1,\ldots,n$. The proof of the theorem then follows immediately from the characterization of the orbits Γ_i by the couples $(\eta_0(\Gamma_i),\mathcal{P}(\Gamma_i))$, for every $i=1,\ldots,n$. □

Example 1. Let us consider this result for the case of smallest nontrivial degree—i.e., $r=2$. Let $\gamma^{(2)}=(\Gamma_1,\ldots,\Gamma_n)$ be an n-tuple of orbits $\Gamma_i \in \mathcal{O}_2$. Recall that $\mathcal{O}_2$ contains exactly two orbits Γ and Γ', as defined in the last paragraph of Sec. III A. Let ω be the subset of $\{1,\ldots,n\}$ which consists of all i such that $\Gamma_i=\Gamma$. Following the definitions stated in theorem 3, we have $\omega^{(1)}=\omega=\omega^{(2)}$ and $\omega^{(12)}=\{1,\ldots,n\}$. Consequently,

$$A_{\gamma^{(2)}} = \sum_{w \in \mathbb{F}_2^{2n}, \mathrm{supp}(w)=\overline{\omega}} \sigma_w \otimes \sigma_w.$$

This shows that the matrices $A_{\gamma^{(2)}}$ are parametrized by the subsets ω of $\{1,\ldots,n\}$ in a one-to-one correspondence.

While the result in theorem 3 is in fact no more than a reformulation of Eq. (11), it is interesting in that it relates the matrices A_γ [and thus the corresponding invariant polynomials $\mathrm{Tr}(A_\gamma \rho^{\otimes r})$ as well] to the notion of the support of a binary vector, which is of central importance in quantum coding theory. Note that the definition (12) of support is indeed the same as is used in the theory of quantum codes.

IV. BASES OF INVARIANTS

It follows from theorem 2 that the polynomials

$$p_{n,r}^{\gamma}(\rho) \coloneqq \mathrm{Tr}(A_\gamma \rho^{\otimes r}), \qquad (17)$$

in the variables $\rho_{ij}(i,j=0,\ldots,2^n-1)$ linearly generate the space of homogeneous invariants of $\mathcal{C}_n^l$ of degree r. However, different A_γ's may correspond to the same polynomial and therefore linear dependences within the set of the polynomials (17) can exist in general. We now set out to pinpoint a basis of polynomials for each degree r. As in the preceding section, we start by considering the simplest case of one qubit and then move to the general case.

A. One qubit

Let $\rho=(\rho_{ij})$, where $i,j=0$, 1, be a matrix of variables. Fix an orbit $\Gamma \in \mathcal{O}_r$ with $\eta_0(\Gamma) \equiv \eta_0$ and $\mathcal{P}(\Gamma) \equiv \{\eta_1,\eta_2,\eta_3\}$. It will be convenient to introduce the linear forms $x_{ij}(\rho)\colon = \mathrm{Tr}(\rho\sigma_{ij})$, where $i,j=0$, 1 or, more explicitly,

$$x_{00}(\rho) = \rho_{00} + \rho_{11},$$

$$x_{01}(\rho) = \rho_{01} + \rho_{10},$$

$$x_{10}(\rho) = \rho_{00} + \rho_{11},$$

$$x_{11}(\rho) = i(\rho_{01} - \rho_{10}). \qquad (18)$$

Conversely, the ρ_{ij}'s can be written as linear forms in the variables $x=(x_{ij})$ as follows:

$$\rho(x) = \frac{1}{2}\sum_{i,j=0}^{1} x_{ij}\sigma_{ij}.$$

We will consider $\mathrm{Tr}[A_\Gamma \rho(x)^{\otimes r}]$ to be a polynomial in the variables x. This yields

$$\mathrm{Tr}[A_\Gamma \rho(x)^{\otimes r}] = \frac{1}{2^r}\sum_{(u,v)\in\Gamma} x_{u_1 v_1}\ldots x_{u_r v_r}$$
$$= \frac{1}{2^r}\sum_{(u,v)\in\Gamma} x_{00}^{n_0(u,v)} x_{01}^{n_x(u,v)} x_{10}^{n_z(u,v)} x_{11}^{n_y(u,v)}, \qquad (19)$$

where we have used the definitions $n_0(u,v)=|\eta_0(u,v)|$ etc. Note that

$$n_0(u,v) = |\eta_0|$$

and

$$\{n_x(u,v),n_y(u,v),n_z(u,v)\} = \{|\eta_1|,|\eta_2|,|\eta_3|\}$$

for every $(u,v) \in \Gamma$. It readily follows that Eq. (19) is equal to

$$x_{00}^{|\eta_0|}\sum_{\pi\in S_3} x_{01}^{|\eta_{\pi(1)}|} x_{10}^{|\eta_{\pi(2)}|} x_{11}^{|\eta_{\pi(3)}|} \qquad (20)$$

up to a normalization factor. Expression (20) shows that the polynomial $\mathrm{Tr}(A_\Gamma \rho^{\otimes r})$ only depends on the number $|\eta_0|$ and the set $\{|\eta_1|,|\eta_2|,|\eta_3|\}$. In other words, if Γ and Γ' are two orbits such that

$$|\eta_0(\Gamma)| = |\eta_0(\Gamma')|$$

and

$$\{|\eta_1(\Gamma)|,|\eta_2(\Gamma)|,|\eta_3(\Gamma)|\} = \{|\eta_1(\Gamma')|,|\eta_2(\Gamma')|,|\eta_3(\Gamma')|\},$$

then (and only then) the polynomials $\mathrm{Tr}(A_\Gamma \rho^{\otimes r})$ and $\mathrm{Tr}(A_{\Gamma'} \rho^{\otimes r})$ coincide. This equivalence relation on $\mathcal{O}_r$ leads to the following definition: for each 4-tuple $\lambda=(\lambda_0,\lambda_1,\lambda_2,\lambda_3)$ of non-negative integers λ_i such that $\lambda_1,\lambda_2,\lambda_3$ are either all even or all odd, $\lambda_0+\lambda_1+\lambda_2+\lambda_3=r$ and $\lambda_1 \geqslant \lambda_2 \geqslant \lambda_3$, we define an invariant p_r^λ of $\mathcal{C}_1$ of degree r as follows:

$$p_r^{\lambda} = x_{00}^{\lambda_0} \sum_{x \in S_3} x_{01}^{\lambda_{\pi(1)}} x_{10}^{\lambda_{\pi(2)}} x_{11}^{\lambda_{\pi(3)}}. \tag{21}$$

Recall that p_r^{λ} is to be regarded as a polynomial in the variables ρ via Eq. (18). By construction, the set of all these polynomials generates the space of invariants of degree r. What is more, the p_r^{λ}'s are linearly independent. This immediately follows from the fact that each monomial in the variables x_{ij} occurs in exactly one polynomial p_r^{λ} and that the polynomials $x_{ij}(\rho)$ are algebraically independent. We have therefore proven:

Theorem 4. The polynomials p_r^{λ} form a basis of the vector space of homogeneous invariants of $\mathcal{C}_1$ of degree r.

B. Multiple qubits

The construction of bases of invariants for arbitrary n will be a generalization of the one-qubit case. Starting from a $2^n \times 2^n$ matrix ρ of variables, we again perform a change of variables, defining $x_w \equiv x_w(\rho) = \mathrm{Tr}(\rho\sigma_w)$, for every $w \in \mathbb{F}_2^{2n}$. Analogous to the one-qubit case, the converse relation reads $\rho(x) = (1/2^n)\Sigma_w x_w \sigma_w$. Note that the polynomials $\{x_w(\rho)\}$ are algebraically independent; this follows from the fact that the variables x and the variables ρ are related by an invertible linear transformation. Now, letting $\gamma = (\Gamma_1, \ldots, \Gamma_n)$ be an n-tuple of orbits $\Gamma_i \in \mathcal{O}_r$, the invariant $p_{n,r}^{\gamma}$, regarded as a polynomial in the variables x, is equal to

$$\sum_{(w^{(1)},\ldots,w^{(r)}) \in \gamma} x_{w^{(1)}} \ldots x_{w^{(r)}} \tag{22}$$

up to a normalization. Here, $(w^{(1)}, \ldots, w^{(r)}) \in \gamma$ is a shorthand notation to express that $(w^{(1)}, \ldots, w^{(r)})$ is an r-tuple of vectors $w^{(j)} \in \mathbb{F}_2^{2n}$ satisfying

$$(w_i^{(1)}, \ldots, w_i^{(r)}, w_{n+i}^{(1)}, \ldots, w_{n+i}^{(r)}) \in \Gamma_i, \tag{23}$$

for every $i = 1, \ldots, n$. As in the case of one single qubit, the correspondence between the polynomial $p_{n,r}^{\gamma}$ and the matrix A_{γ} is nonunique. Indeed, suppose that $\mu \in S_r$ is an arbitrary permutation and define the n-tuple $\gamma^{\mu} = (\Gamma_1^{\mu}, \ldots, \Gamma_n^{\mu})$ such that

$$j \in \eta_a(\Gamma_i^{\mu}) \text{ iff } \mu^{-1}(j) \in \eta_a(\Gamma_i) \tag{24}$$

for every $j \in \{1, \ldots, r\}$ and $a \in \{0,1,2,3\}$. Equivalently, one has $(w^{(1)}, \ldots, w^{(r)}) \in \gamma^{\mu}$ if and only if $(w^{(\mu(1))}, \ldots, w^{(\mu(r))}) \in \gamma$. Then

$$p_{n,r}^{\gamma} = p_{n,r}^{\gamma^{\mu}}, \tag{25}$$

which immediately follows from Eq. (22). Conversely, if γ and γ' are two n-tuples of orbits such that $p_{n,r}^{\gamma} = p_{n,r}^{\gamma'}$, then there exists a permutation $\mu \in S_r$ such that $\gamma' = \gamma^{\mu}$, as one can easily verify. We now claim that a basis $\{p_{n,r}^{\gamma_1}, p_{n,r}^{\gamma_2}, \ldots\}$ of the space of invariants of $\mathcal{C}_n^r$ is obtained by fixing a set $\{\gamma_1, \gamma_2, \ldots\}$ of n-tuples of orbits such that (i) the polynomials $p_{n,r}^{\gamma_i}$ are pairwise different, and (ii) for every n-tuple γ of orbits, $p_{n,r}^{\gamma} = p_{n,r}^{\gamma_i}$ for some $i = 1, 2, \ldots$.

The claim is proven as follows: first, it follows from the construction of the invariants $p_{n,r}^{\gamma}$ and item (ii) that the polynomials $p_{n,r}^{\gamma_i}$ generate the space of homogeneous invariants of degree r. Second, the linear independence of the $p_{n,r}^{\gamma_i}$'s follows from (i). For, suppose there exist complex coefficients a_i, not all equal to zero, such that

$$\sum_i a_i p_{n,r}^{\gamma_i} = 0. \tag{26}$$

As each monomial $\Pi_{j=1}^r x_{w^{(j)}}$, where $w^{(j)} \in \mathbb{F}_2^{2n}$, occurs in exactly one invariant $p_{n,r}^{\gamma_i}$, this yields a nontrivial linear combination of these monomials adding up to zero, which is a contradiction; indeed, the monomials $\Pi_{j=1}^r x_{w^{(j)}}$ are linearly independent, as the polynomials $\{x_w(\rho)\}$ are algebraically independent.

We now set out to construct a set of invariants which satisfies (i) and (ii). According to the discussion above, there is an equivalence relation $\sim$ on the set $\mathcal{O}_r^n$ of n-tuples of orbits, such that $\gamma \sim \gamma'$ if and only if there exists a permutation $\mu \in S_r$ such that $\gamma' = \gamma^{\mu}$. A set of invariants which satisfies the desired conditions is obtained by choosing any set $\{\gamma_1, \gamma_2, \ldots\}$ of orbits such that every equivalence class is represented by exactly one n-tuple γ_i.

Recall that an n-tuple $\gamma = (\Gamma_1, \ldots, \Gamma_n) \in \mathcal{O}_r^n$ is described by n couples $\boldsymbol{(}\eta_0(\Gamma_i), \mathcal{P}(\Gamma_i)\boldsymbol{)}$, where $\eta_0(\Gamma_i) \subseteq \{1, \ldots, r\}$ and $\mathcal{P}(\Gamma_i)$ is a partition of $\{1, \ldots, r\} \setminus \eta_0(\Gamma_i)$ into three subsets. While such a system of n couples compactly describes γ, it will be useful to represent γ in a different way, which contains some redundant information but has the advantage of being more transparent: we describe γ by an $n \times r$ matrix M with entries in the set {0, 1, 2, 3}, satisfying

$$M_{ij} = 0 \text{ iff } j \in \eta_0(\Gamma_i),\ 0 \neq M_{ij} = M_{ik} \text{ iff } j \text{ and } k \text{ belong to the same subset in the partition } \mathcal{P}(\Gamma_i), \tag{27}$$

for every $i = 1, \ldots, n$ and $j, k = 1, \ldots, r$. It is clear that this description exhibits some degeneracy, as any permutation of {1, 2, 3} in any row of M yields a (generally) different matrix which also satisfies Eq. (27). However, the equivalence relation $\sim$ is translated into a simple kind of equivalence transformation of matrices. Indeed, two n-tuples $\gamma, \gamma' \in \mathcal{O}_r^n$, described by $n \times r$ matrices M and M', respectively, belong to the same equivalence class of the relation $\sim$ if and only if M' is equal to M modulo a permutation $\mu \in S_r$ of its columns and n row-wise permutations π_i of {1, 2, 3}, and we write $M \sim M'$.

Seeing that we are looking for suitable representatives of each equivalence class, it is appropriate to look for normal forms of the matrices M under the above action of the permutations μ and π_i. There is in fact a lot of freedom to define sensible normal forms. One possible definition is stated below in definition 4. First we need some preliminary definitions:

Definition 1. Let $d \in \mathbb{N}_0$. Let $u = (u_1, u_2, \ldots, u_d)$ and $v = (v_1, v_2, \ldots, v_d)$ be two d-dimensional vectors with nonnegative integer components. A lexicographical ordering relation $\leqslant_{\mathrm{lex}}$ is defined as follows: $u \leqslant_{\mathrm{lex}} v$ if $u = v$ or if there exists $j(1 \leqslant j \leqslant d)$ such that $u_i = v_i$ if $i < j$ and $u_j < v_j$.

Definition 2. Let u be a d-dimensional vector with entries in {0, 1, 2, 3}. For every $a \in \{0,1,2,3\}$, define $\eta_a(u) = \{j \in \{1, \ldots, d\} | u_j = a\}$.

Definition 3. Let M be an $n \times r$ matrix with entries in the set {0, 1, 2, 3}. Let M_i^T denote the ith row of M. Let $m = (m_1, \ldots, m_{i_0})$ be an i_0-dimensional vector with entries in {0, 1, 2, 3}, where $i_0 \leqslant n$. Then the set $\eta_m(M) \subseteq \{1, \ldots r\}$ is defined as follows:

$$\eta_m(M) = \cap_{i \leqslant i_0} \eta_{m_i}(M_i^T). \qquad (28)$$

For every $a \in \{1,2,3\}$, the vector $u_{i_0+1}^{(a)}(M)$ with components $u_{i_0+1}^{(a)}(M)_m$, where m ranges over all i_0-dimensional vectors with components in {0, 1, 2, 3}, is defined by

$$u_{i_0+1}^{(a)}(M)_m = |\{j \in \eta_m(M) | M_{i_0+1,j} = a\}| \qquad (29)$$

[the indices m of the components of $u_{i_0+1}^{(a)}(M)$ are ordered according to the lexicographical ordering relation].

Definition 4. Let M be an $n \times r$ matrix with entries in the set {0, 1, 2, 3}. Then M is in normal form if it satisfies the following conditions.

(i) The columns K_j of M are ordered nondecreasingly—i.e., $K_1 \leqslant_{\text{lex}} \cdots \leqslant_{\text{lex}} K_r$.

(ii) $|\eta_3(M_1^T)| \leqslant |\eta_2(M_1^T)| \leqslant |\eta_1(M_1^T)|$ and for every $i = 2, \ldots, n$,

$$u_i^{(3)}(M) \leqslant_{\text{lex}} u_i^{(2)}(M) \leqslant_{\text{lex}} u_i^{(1)}(M). \qquad (30)$$

(iii) For every $i = 1, \ldots, n$ the three numbers $|\eta_1(M_i^T), |\eta_2(M_i^T)|, |\eta_3(M_i^T)|$ are either all even or all odd.

Example 2. The following 3×11 matrix is in normal form:

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 3 & 3 \\ 0 & 1 & 2 & 1 & 1 & 1 & 2 & 3 & 3 & 2 & 2 \\ 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 3 & 1 & 2 \end{bmatrix}. \qquad (31)$$

Indeed, conditions (i) and (iii) are easily checked, as well as the first part of condition (ii). As for the second part of (ii), let us calculate the vector

$$u_2^{(a)}(M) = ((u_2^{(a)})_0, (u_2^{(a)})_1, (u_2^{(a)})_2, (u_2^{(a)})_3) \qquad (32)$$

and the vector $u_3^{(a)}(M)$, equal to

$$((u_3^{(a)})_{00}, (u_3^{(a)})_{01}, (u_3^{(a)})_{02}, (u_3^{(a)})_{03}, (u_3^{(a)})_{10}, (u_3^{(a)})_{11}, \ldots).$$

Using definition (29), we find

$$u_2^{(1)} = (1,3,*,*), \quad u_2^{(2)} = (1,1,*,*), \quad u_2^{(3)} = (0,0,*,*)$$

and

$$u_3^{(1)} = (1,0,0,*,\ldots),$$

$$u_3^{(2)} = (0,1,0,*,\ldots),$$

$$u_3^{(3)} = (0,0,1,*,\ldots), \qquad (33)$$

where the entries denoted with * are (in this example) irrelevant to order the vectors lexicographically, and condition (ii) follows.

One can easily verify that each equivalence class contains exactly one normal form. Note that, given an $n \times r$ normal form M, one recovers the corresponding tuple $\gamma_M = (\Gamma_1, \ldots, \Gamma_n) \in \mathcal{O}_r^n$ as follows:

$$\eta_0(\Gamma_i) = \eta_0(M_i^T),$$

$$\mathcal{P}(\Gamma_i) = \{\eta_1(M_i^T), \eta_2(M_i^T), \eta_3(M_i^T)\}. \qquad (34)$$

For instance, the tuple γ corresponding to the normal form in example 2 is defined by

$$\eta_0(\Gamma_1) = \{1,2,3\}, \quad \mathcal{P}(\Gamma_1) = \{\{4,5,6,7\},\{8,9\},\{10,11\}\},$$

$$\eta_0(\Gamma_2) = \{1\}, \quad \mathcal{P}(\Gamma_2) = \{\{2,4,5,6\},\{3,7,10,11\},\{8,9\}\},$$

$$\eta_0(\Gamma_3) = \{4,8\}, \quad \mathcal{P}(\Gamma_3) = \{\{1,5,10\},\{2,6,11\},\{3,7,9\}\}.$$

We have proven our main result:

Theorem 5. For every $n \times r$ normal form M, denote the corresponding n-tuple of orbits by γ_M. Then the set of all invariants $p_{n,r}^{\gamma_M}$ forms a basis of the space of homogeneous invariants of $\mathcal{C}_n^l$ of degree r.

Thus, we have obtained our initial objective of constructing for every n and for every r a basis of the space of invariants of $\mathcal{C}_n^l$ of degree r. Note that for the case $n=1$ we indeed recover the result obtained in the previous section.

It is interesting to investigate the behavior of the dimensions $d_{n,r}$ of these spaces for large n and r. Lower and upper bounds for $d_{n,r}$ are the following.

Lemma 2. Let $n, r \in \mathbb{N}_0$. Then

$$\frac{1}{6^n r!}(4^{r-1} + 3 \cdot 2^{r-1} + 2)^n \leqslant d_{n,r} \leqslant \binom{r + 4^n - 1}{r}.$$

Proof. Let $\mathcal{M}_{n \times r}$ denote the set of all $n \times r$ matrices M with entries in the set {0,1,2,3}, such that for every $i = 1, \ldots, n$ the three numbers

$$|\eta_1(M_i^T) ,|\eta_2(M_i^T)|,|\eta_3(M_i^T)| \qquad (35)$$

are either all even or all odd. Recall that $d_{n,r}$ is equal to the number of orbits of the group $S_r \times S_3^n$ acting on this set as defined above. Using the Cauchy-Frobenius lemma, the number of orbits is equal to

$$\frac{1}{6^n r!} \sum_{(\mu,\pi_i)} \mathcal{F}(\mu, \pi_i), \qquad (36)$$

where $\mathcal{F}(\mu, \pi_i)$ denotes the number of fixed points in $\mathcal{M}_{n \times r}$ of the element $(\mu, \pi_i) = (\mu, \pi_1, \ldots, \pi_n)$, where $\mu \in S_r$ and $\pi_i \in S_3$. First, note that restricting the sum to all group elements where μ is equal to the identity yields the desired lower bound, using a highly similar argument to the one used to calculate $|O_r|^n$ above. In order to obtain the upper bound, we will calculate the number $N_{n,r}$ of orbits of the group S_r acting on the set of *all* $n \times r$ matrices with entries in the set {0, 1, 2, 3} by permuting columns. Note that this number is indeed an upper bound for $d_{n,r}$. The Cauchy-Frobenius lemma yields

$$N_{n,r} = \frac{1}{r!} \sum_{\mu \in S_r} (4^n)^{c(\mu)}, \qquad (37)$$

where $c(\mu)$ denotes the number of cycles in the permutation μ. Consequently,

$$N_{n,r} = \frac{1}{r!}\sum_{k=0}^{r} t(r,k)4^{nk}, \tag{38}$$

where $t(r,k)$ is defined as the number of permutations in S_r which have exactly k cycles. Note that this number is related to the *Stirling number $s(r,k)$ of the first kind* by the relation $t(r,k)=(-1)^{r+k}s(r,k)$ [16]. Using the identity [16]

$$\sum_{k=0}^{r} s(r,k)x^k = (-1)^r r!\binom{r-x-1}{r}, \tag{39}$$

we find that

$$N_{n,r} = \binom{r+4^n-1}{r}, \tag{40}$$

which completes the proof.

While these bounds are in fact quite rough, they are sufficient to gain qualitative insight into the limit behavior of the dimensions $d_{n,r}$ when n or r are large. Let us first examine $\lim_{r\to\infty} d_{n,r}$ for fixed n. Denote $\lambda = 4^n - 1$. Then, using the Stirling approximation $\ln(a!) \approx a\ln a - a$, the upper bound reads

$$\begin{aligned}\ln\binom{r+\lambda}{r} &= \ln(r+\lambda)! - \ln r! - \ln\lambda!\\ &\approx (r+\lambda)\ln(r+\lambda) - r\ln r - \ln\lambda! - \lambda\\ &= \ln\left(1+\frac{\lambda}{r}\right)^r + \lambda\ln(r+\lambda) - \ln\lambda! - \lambda\\ &\approx \lambda\ln(r+\lambda) - \ln\lambda!,\end{aligned} \tag{41}$$

where in the last line we have used $(1+(\lambda/r))^r \approx \exp(\lambda)$ when r is large. Finally, we obtain

$$d_{n,r} \leqslant \frac{1}{\lambda!}(r+\lambda)^{\lambda}. \tag{42}$$

We have proven the following.

Theorem 6. For every fixed $n\in\mathbb{N}_0$, the dimension $d_{n,r}$ tends polynomially in r to infinity. In other words, for every n there exists a polynomial $p_n(r)$ in r such that $d_{n,r} = \mathcal{O}(p_n(r))$. Note that a similar result does not hold for $\lim_{n\to\infty} d_{n,r}$ for fixed r. Indeed, the lower bound in lemma 2 shows that

$$d_{n,r} \geqslant \mathcal{O}\left(\frac{1}{r!}\left(\frac{4^r}{6}\right)^n\right), \tag{43}$$

which is nonpolynomial in n if $r \geqslant 2$.

V. INVARIANTS OF DEGREES 1, 2, AND 3

In this section we investigate the invariants of $\mathcal{C}_n^l$ of low degrees in more detail. In particular, we will show the following result.

Theorem 7. Every invariant of $\mathcal{C}_n^l$ of degree 1, 2, or 3 is an invariant of $U(2)^{\otimes n}$ (which also acts by conjugation) and vice versa.

One of the implications in the theorem is trivial. Indeed, every invariant of $U(2)^{\otimes n}$ is an invariant of $\mathcal{C}_n^l$, as the latter is a subgroup of the former. Let us now prove the reverse implication.

Let ρ be a $2^n \times 2^n$ matrix of variables. First, it follows from theorems 1 and 2 that $\mathcal{C}_n^l$ has only one invariant of degree 1: namely, $\mathrm{Tr}(\rho)$, which is trivially an invariant of $U(2)^{\otimes n}$.

In order to examine the invariants of degrees 2 and 3, it will be convenient to introduce the following functions.

Definition 5. Let $\omega \subseteq \{1,\ldots,n\}$. Define the functions $\delta_\omega, \epsilon_\omega : \mathbb{F}_2^{2n} \to \mathbb{C}$ by

$$\delta_\omega(w) = 1 \text{ if } \mathrm{supp}(w) = \omega \text{ and } \delta_\omega(w) = 0 \text{ otherwise},$$

$$\epsilon_\omega(w) = 1 \text{ if } \mathrm{supp}(w) \subseteq \omega \text{ and } \epsilon_\omega(w) = 0 \text{ otherwise}.$$

It is straightforward to show the relations

$$\epsilon_\omega = \sum_{\omega'\subseteq\omega} \delta_{\omega'},$$

$$\delta_\omega = (-1)^{|\omega|}\sum_{\omega'\subseteq\omega} (-1)^{|\omega'|}\epsilon_{\omega'}, \tag{44}$$

the first of which is trivial and the second of which can easily be verified by substitution in the first one.

Now, regarding $r=2$, using example 1 we find that the polynomials

$$\begin{aligned}p_\omega(\rho) &= \sum_{w\in\mathbb{F}_2^{2n},\mathrm{supp}(w)=\omega} \mathrm{Tr}(\sigma_w \otimes \sigma_w \rho^{\otimes 2})\\ &= \sum_{w\in\mathbb{F}_2^{2n},\mathrm{supp}(w)=\omega} \mathrm{Tr}\{(\sigma_w\rho)^2\},\end{aligned} \tag{45}$$

where ω ranges over all 2^n subsets of $\{1,\ldots,n\}$, form a generating set of the space of invariants of degree 2. Moreover, using the techniques of the previous section, one can easily show that the p_ω's are linearly independent and therefore the dimension of this space is 2^n. Interesting variants of Eq. (45) are the polynomials

$$q_\omega(\rho) = \sum_{w\in\mathbb{F}_2^{2n},\mathrm{supp}(w)\subseteq\omega} \mathrm{Tr}\{(\sigma_w\rho)^2\} = \mathrm{Tr}\{(\mathrm{Tr}_{\bar{\omega}}\rho)^2\}, \tag{46}$$

where the operation $\mathrm{Tr}_{\bar{\omega}}$ denotes the partial trace over all qubits outside the set ω. The polynomials q_ω are manifestly invariant under the entire local unitary group. In fact, it is well known that these polynomials are generators of the space of invariants of $U(2)^{\otimes n}$ of degree two [17]. Moreover, one has the relations

$$q_\omega = \sum_{\omega'\subseteq\omega} p_{\omega'},$$

$$p_\omega = (-1)^{|\omega|}\sum_{\omega'\subseteq\omega} (-1)^{|\omega'|} q_{\omega'}, \tag{47}$$

which follow immediately from Eqs. (44). In particular, the second expression in Eqs. (47) shows that every polynomial p_ω is an invariant of $U(2)^{\otimes n}$, implying that the sets $\{p_\omega\}$ and $\{q_\omega\}$ span the same space, which yields the desired result for theorem 6 for $r=2$. Furthermore, it follows from Eqs. (47)

that polynomials q_ω are a basis as well, being a generating set of cardinality 2^n in a 2^n-dimensional space.

A similar result can be proven for the invariants of degree 3. Theorem 2 shows that the space of invariants of $\mathcal{C}_n^l$ of degree 3 is spanned by all polynomials

$$p_{n,3}^{\gamma} = \sum_{(w^{(1)},w^{(2)},w^{(3)}) \in \gamma} \mathrm{Tr}(\sigma_{w^{(1)}} \otimes \sigma_{w^{(2)}} \otimes \sigma_{w^{(3)}} \rho^{\otimes 3}),$$

where γ ranges over all elements in $\mathcal{O}_3^n$. Note that, for every $\gamma \in \mathcal{O}_3^n$, one has $w^{(1)}+w^{(2)}+w^{(3)}=0$ whenever $(w^{(1)},w^{(2)},w^{(3)}) \in \gamma$, by definition of $\mathcal{O}_3^n$. Using the description of γ by sets $\omega^{(i)}$ and $\omega^{(ij)}$ introduced in theorem 3, it follows that

$$p_{n,3}^{\gamma} = \sum \mathrm{Tr}(\sigma_{w^{(1)}} \otimes \sigma_{w^{(2)}} \otimes \sigma_{w^{(1)}+w^{(2)}} \rho^{\otimes 3}), \qquad (48)$$

where the sum runs over all couples $(w^{(1)},w^{(2)}) \in (\mathbb{F}_2^{2n})^{\times 2}$ such that

$$\mathrm{supp}(w^{(1)}) = \omega_1, \quad \mathrm{supp}(w^{(2)}) = \omega_2$$

$$\mathrm{supp}(w^{(1)} + w^{(2)}) = \omega_{12}, \qquad (49)$$

for some $\omega_1, \omega_2, \omega_{12} \subseteq \{1, \ldots, n\}$. Using Eqs. (44), a straightforward calculation shows that $p_{n,3}^{\gamma}$ is, up to an overall sign, equal to

$$\sum (-1)^{|\omega_1'|+|\omega_2'|+|\omega_{12}'|} \mathrm{Tr}\{(\mathrm{Tr}_{\overline{\omega_1'}}\rho)(\mathrm{Tr}_{\overline{\omega_2'}}\rho)(\mathrm{Tr}_{\overline{\omega_{12}'}}\rho)\}, \qquad (50)$$

where the sum runs over all $\omega_1' \subseteq \omega_1, \omega_2' \subseteq \omega_2$ and $\omega_{12}' \subseteq \omega_{12}$. As the summands in Eq. (50) are manifestly invariant under the action of $\mathrm{U}(2)^{\otimes n}$, the polynomial $p_{n,3}^{\gamma}$ is an invariant of the local unitary group and the proof of theorem 7 is completed.

VI. CONCLUSION

We have performed a systematic study of the invariant algebra of the local Clifford group $\mathcal{C}_n^l$ using the description of this group in terms of binary arithmetic. Our approach was to consider the spaces of homogeneous invariants degree per degree and to construct bases of these spaces for each degree r. In order to study these spaces of homogeneous invariants, we transformed the problem to the study of certain algebras $\mathcal{A}_{n,r}$ of matrices, such that every matrix in an algebra $\mathcal{A}_{n,r}$ corresponds to an invariant polynomial of degree r. We then constructed bases $\{A_\gamma\}_{\gamma \in \mathcal{O}_r^n}$ of these algebras, which yielded generating, though linearly dependent, sets $\{p_{n,r}^{\gamma}\}_\gamma$ of homogeneous invariants. We subsequently showed how a basis of invariants could be pinpointed amongst these polynomials for each degree r, which was the main result of this paper.

As stated in the Introduction, we believe that these results are relevant in a number of fields in quantum information theory, with in particular, the classification of binary quantum codes. In forthcoming work we will apply the present results to this problem.

ACKNOWLEDGMENTS

Research supported by Research Council KUL: GOA-Mefisto 666, GOA-Ambiorics, several grants; Flemish Government: FWO: projects, G.0240.99 (multilinear algebra), G.0407.02 (support vector machines), G.0197.02 (power islands), G.0141.03 (Identification and cryptography), G.0491.03 (control for intensive care glycemia), G.0120.03 (QIT), G.0452.04 (QC), G.0499.04 (robust SVM), research communities (ICCoS, ANMMM, MLDM); AWI: Bil. Int. Collaboration Hungary/ Poland; IWT: GBOU (McKnow) Belgian Federal Government: Belgian Federal Science Policy Office: IUAP V-22 (Dynamical Systems and Control: Computation, Identification and Modelling, 2002-2006), PODO-II (CP/01/40: TMS and Sustainibility); EU: FP5-Quprodis; ERNSI; Eureka 2063-IMPACT; Eureka 2419-FliTE; Contract Research/agreements: ISMC/IPCOS, Data4s, TML, Elia, LMS, IPCOS, Mastercard; QUIPRO-CONE; QUPRODIS.

[1] I. Chuang and M. Nielsen *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[2] J. Dehaene, M. Van den Nest, and B. De Moor, Phys. Rev. A **67** 022310, (2003).
[3] M. Hein, J. Eisert, and H. J. Briegel, e-print quant-ph/0307130.
[4] J. Dehaene and B. De Moor, Phys. Rev. A **68**, 042318 (2003).
[5] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A **69**, 022316 (2004).
[6] M. Van den Nest, J. Dehaene, and B. De Moor, e-print quant-ph/0405023.
[7] D. Gottesman, e-print quant-ph/9807006.
[8] D. Gottesman, Ph.D. thesis, Caltech, 1997, e-print quant-ph/9705052.
[9] M. Van den Nest, J. Dehaene, and B. De Moor, e-print quant-ph/0404106.
[10] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[11] B. Runge, Discrete Math. **148**, 175, (1996).
[12] G. Nebe, E. Rains, and N. J.A. Sloane, e-print math.NT/0311046.
[13] G. Nebe, E. Rains, and N. J.A. Sloane, e-print math.CO/0001038.
[14] A. M. Gleason, in *Actes, congres international de Mathematiques* (Gautier-Villars, Paris, 1970), Vol. 3, pp. 211–215.
[15] E. Rains and N. J.A. Sloane, in edited by V. S. Pless and W. C. Huffman, *Handbook of Coding Theory*, (1998), pp. 177–254.
[16] Eric W. Weisstein, http://mathworld.wolfram.com/ Stirling-NumberoftheFirstKind.html.
[17] E. M. Rains. e-print quant-ph/9704042.