Local invariants of stabilizer codes

Maarten Van den Nest,* Jeroen Dehaene, and Bart De Moor
Katholieke Universiteit Leuven, ESAT-SCD, Belgium.

(Dated: May 3, 2004)

In [Phys. Rev. A 58, 1833 (1998)] a family of polynomial invariants which separate the orbits of multi-qubit density operators ρ under the action of the local unitary group was presented. We consider this family of invariants for the class of those ρ which are the projection operators describing stabilizer codes and give a complete translation of these invariants into the binary framework in which stabilizer codes are usually described. Such an investigation of local invariants of quantum codes is of natural importance in quantum coding theory, since locally equivalent codes have the same error-correcting capabilities and local invariants are powerful tools to explore their structure. Moreover, the present result is relevant in the context of multipartite entanglement and the development of the measurement-based model of quantum computation known as the one-way quantum computer.

PACS numbers: 03.67.-a

I. INTRODUCTION

The theory of quantum error-correcting codes constitutes a vital ingredient in the realization of quantum computing, as these codes protect the vulnerable information stored in a quantum computer from the destructive effects of decoherence. The most widely known class of error-correcting codes is that of the stabilizer codes, studied extensively in e.g. [1–3]. An n-qubit stabilizer code is defined as a simultaneous eigenspace of a set of commuting observables in the Pauli group, where the latter consists of all n-fold tensor products of the Pauli matrices and the identity. Equivalently, a code is described by the projector operator on this eigenspace. In the characterization of the the error-correcting capabilities of quantum codes, two equivalence relations arise naturally on the set of corresponding projectors: two n-qubit quantum codes described by projectors ρ and ρ' are called *globally equivalent*, or just *equivalent*, if there exists a local unitary operator $U \in U(2)^{\otimes n}$ such that $U\rho U^\dagger$ is equal to ρ' modulo a permutation of the n qubits. If $U\rho U^\dagger = \rho'$, without any additional permutation, the codes are called *locally equivalent*. As globally equivalent codes have exactly the same error-correcting capabilities and vice versa, global equivalence is in fact the true equivalence of quantum codes. However, the structure of local equivalence is more transparent and insight in this matter already provides a lot of information about the structure of quantum codes. Therefore, much of the relevant literature tackles local equivalence and we will do the same in the following.

This paper is concerned with the characterization of the local equivalence class of a stabilizer code ρ by means of local *invariants*. These are complex functions $F(\rho)$ which remain invariant under the action of all local unitary transformations, i.e.,

$$F(\rho) = F(U\rho U^\dagger)$$

for every $U \in U(2)^{\otimes n}$. In studying invariants, the general goal is to look for a minimal set of invariants which characterizes the local equivalence class of any given code. To obtain such a minimal complete set, it is well known [4] that it is sufficient to consider functions F which are polynomials in the entries of ρ. These polynomial invariants form an algebra over $\mathbb{C}$, as linear combinations and products of invariants remain invariants. Interestingly, the invariant algebra of $U(2)^{\otimes n}$ is finitely generated [5] and therefore the existence of a *finite* complete set of polynomial invariants is guaranteed. Although the problem of pinpointing such a finite set is to date unanswered, progress has been made in the past years in constructing complete though infinite families of invariants. A natural approach is to consider homogeneous invariants, since any invariant can be written as a sum of its homogeneous components, each of which needs to be an invariant as well. As the set of homogeneous invariants of fixed degree has the structure of a vector space, one wishes to construct a basis of this vector space degree per degree in order to obtain a generating (yet infinite) set of the invariant algebra. Grassl et al. [6] achieve this goal, using earlier work of Rains [7]. Their study of local invariants is general in the sense that is does not merely regard (projectors associated with) quantum codes, but in fact arbitrary n-qubit density operators ρ. Closer inspection of their basic invariants when dealing with stabilizer codes is certainly appropriate, given the very specific structure of these codes and their associated projectors. Indeed, the stabilizer formalism has an equivalent formulation in terms of algebra over GF(2) and in this framework any stabilizer code of length n and dimension k is essentially described by an $2n \times k$ binary matrix, called the generator matrix of the code. It is therefore natural to ask what the structure of the basic invariants is in relation to this binary description. In the present paper we resolve this issue: it is shown that the invariants of Grassl et al. are in a one-to-one correspondence with the di-

*Electronic address: `maarten.vandennest@esat.kuleuven.ac.be`

mensions of certain linear subspaces over GF(2) which depend solely on the binary matrix description of a code. Hence, a complete translation of the invariants into the binary stabilizer framework is obtained.

We wish to point out that the relevance of this investigation stretches beyond the domain of quantum coding theory: stabilizer codes with rank one projectors correspond to the class of pure states generally known as stabilizer states. The problem of recognizing local unitary equivalence of stabilizer states is of importance in the study of multipartite entanglement [8, 9] and in the development of the one-way quantum computer, a measurement-based model of quantum computation which uses a stabilizer state as a universal resource [10].

II. NOTATIONS

First, we fix some basic notations which will be used throughout this paper. Seeing that stabilizer codes have descriptions both as projectors on a complex Hilbert space and as binary linear spaces, we will be dealing with algebra over the fields $\mathbb{C}$ and $\mathbb{F}_2 := \mathrm{GF}(2)$, where the latter is the finite field of two elements (0 and 1), where arithmetics are performed modulo 2. The set of $p \times q$ matrices over a field $\mathbb{F} \in \{\mathbb{C}, \mathbb{F}_2\}$ will be denoted by $M_{p\times q}(\mathbb{F})$, where $p, q \in \mathbb{N}_0$. To shorten notations, the set of square $p \times p$ matrices is denoted by $M_p(\mathbb{F})$.

The group $\mathcal{S}_r$ is the symmetric group of order r. For any $n \in \mathbb{N}_0$, $\mathcal{S}_r^n$ denotes the n-fold cartesian product of $\mathcal{S}_r$ with itself, i.e., $\mathcal{S}_r^n$ consists of all n-tuples $\Pi := (\pi_1, \dots, \pi_n)$, where $\pi_i \in \mathcal{S}_r$ for every $i = 1, \dots, n$.

III. STABILIZER CODES AND LINEAR SPACES OVER GF(2)

The Pauli group $\mathcal{G}_n$ on n qubits consists of all 4×4^n n-fold tensor products of the form $\alpha\ v_1 \otimes v_2 \otimes \dots \otimes v_n$, where $\alpha \in \{\pm 1, \pm i\}$ is an overall phase factor and the 2×2-matrices v_i $(i = 1, \dots, n)$ are either the identity σ_0 or one of the Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

An n-qubit stabilizer $\mathcal{S}$ in the Pauli group is a subgroup of $\mathcal{G}_n$ which is generated by $k \le n$ commuting, independent and Hermitian observables $M_i \in \mathcal{G}_n$ $(i = 1, \dots, k)$. Here "independent" means that no product of the form $M_1^{x_1} \dots M_k^{x_k}$, where $x_i \in \{0, 1\}$, yields the identity except when all x_i are equal to zero. The stabilizer code associated with $\mathcal{S}$ is the joint eigenspace belonging to eigenvalue one of the k operators M_i. The numbers n and k are called the length and the dimension of the code, respectively. There is a one-to-one correspondence between the code associated with $\mathcal{S}$ and the matrix

$$\rho_{\mathcal{S}} = \frac{1}{2^n} \sum_{M \in \mathcal{S}} M, \tag{1}$$

as this operator is (up to a multiplicative constant) the projection operator which projects on the code space. The normalization is chosen such as to yield $\mathrm{Tr}(\rho_{\mathcal{S}}) = 1$.

We now briefly discuss the binary representation of the stabilizer formalism (for literature on this subject, see e.g. [1, 3]). Employing the mapping

$$\begin{aligned} \sigma_0 = \sigma_{00} &\ \mapsto\ (0,0) \\ \sigma_x = \sigma_{01} &\ \mapsto\ (0,1) \\ \sigma_z = \sigma_{10} &\ \mapsto\ (1,0) \\ \sigma_y = \sigma_{11} &\ \mapsto\ (1,1), \end{aligned} \tag{2}$$

the elements of $\mathcal{G}_n$ can be represented as $2n$-dimensional binary vectors as follows:

$$\sigma_{u_1 v_1} \otimes \dots \otimes \sigma_{u_n v_n} = \sigma_{(u,v)} \mapsto (u, v) \in \mathbb{F}_2^{2n},$$

where $(u, v) = (u_1, \dots, u_n, v_1, \dots, v_n)$. This parameterization establishes a group homomorphism between $\mathcal{G}_n, \cdot$ and $\mathbb{F}_2^{2n}, +$ (which disregards the overall phases of Pauli operators). In this binary representation, two Pauli operators σ_a and σ_b, where $a, b \in \mathbb{F}_2^{2n}$, commute if and only if $a^T P b = 0$, where the $2n \times 2n$ matrix

$$P = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$$

defines a symplectic inner product on $\mathbb{F}_2^{2n}$. Therefore, a code of length n and dimension k corresponds to a k-dimensional linear subspace of $\mathbb{F}_2^{2n}$ which is self-orthogonal with respect to this symplectic inner product, i.e., $a^T P b = 0$ for every a, b in this subspace. Given a set of generators of the stabilizer, we assemble their binary representations as the columns of a full rank $2n \times k$ matrix S, which is referred to as a generator matrix of the stabilizer subspace. This generator matrix satisfies $S^T P S = 0$ from the symplectic self-orthogonality property. The entire binary stabilizer subspace (or *code space*) $\mathcal{C}_S$ consists of all linear combinations of the columns of S, i.e., it is equal to

$$\mathcal{C}_S := \left\{ Sx \mid x \in \mathbb{F}_2^k \right\}. \tag{3}$$

It is important to notice what happens when some of the qubits in the system $\rho_{\mathcal{S}}$ are traced out. For every $\omega \subseteq \{1, \dots, n\}$, the partial trace $\mathrm{Tr}_{\omega^c}\ \rho_{\mathcal{S}} =: \rho_{\mathcal{S}}^{\omega}$ yields a stabilizer code on $|\omega|$ qubits, where ω^c is the complement of ω in $\{1, \dots, n\}$. Using the definition (1), it follows that

$$\rho_{\mathcal{S}}^{\omega} = \frac{1}{2^n} \sum \mathrm{Tr}_{\omega^c}\ M. \tag{4}$$

As all three Pauli matrices have zero trace, the sum can be taken over all $M \in \mathcal{S}$ which are equal to the identity

σ_0 on the ith tensor factor for every $i \in \omega^c$. Defining the *support* $\mathrm{supp}(M)$ of any $M = \alpha\ v_1 \otimes \cdots \otimes v_n \in \mathcal{G}_n$ by the subset of those $i \in \{1, \ldots, n\}$ such that $v_i \neq \sigma_0$, the sum in (4) runs over the subgroup of all $M \in \mathcal{S}$ such that $\mathrm{supp}(M) \subseteq \omega$. For such M, the partial trace $\mathrm{Tr}_{\omega^c}\ M$ removes the tensor factor σ_0 on positions $i \in \omega^c$. Transferring the definition of *supp* to the binary representation of $\mathcal{G}_n$, the binary code space $\mathcal{C}_S^\omega$ of $\rho_{\mathcal{S}}^\omega$ is obtained by considering the subspace of those $y \in \mathcal{C}_S$ such that $\mathrm{supp}(y) \subseteq \omega$ and removing form these y's the components $(y_i, y_{n+i}) = (0, 0)$ for every $i \in \omega^c$.

Stabilizer states and graph states. If the dimension of a stabilizer code is equal to its length, i.e., if $k = n$, then the code is called self-dual. It is easy to see that the code space of a self-dual code is one-dimensional or, equivalently, $\rho_{\mathcal{S}} = |\psi\rangle\langle\psi|$ for some pure state $|\psi\rangle$. The states $|\psi\rangle$ obtained in this way are known in the literature as *stabilizer states*. By definition, a stabilizer state is the unique simultaneous eigenvector with eigenvalue 1 of a set of n commuting and independent Pauli operators. A subset of the class of stabilizer states which will be of particular interest in our investigation is constituted by the so-called *graph states* [10, 11]. For these states, the defining eigenvalue equations can be constructed on the basis of a graph: when G is a simple graph on n vertices with adjacency matrix θ [14], one defines n (commuting) Pauli operators

$$K_j = \sigma_x^{(j)} \prod_{k=1}^{n} \left(\sigma_z^{(k)}\right)^{\theta_{kj}},$$

where $\sigma_x^{(i)}, \sigma_y^{(i)}, \sigma_z^{(i)}$ are the Pauli operators which have resp. $\sigma_x, \sigma_y, \sigma_z$ on the ith position in the tensor product and the identity elsewhere. The graph state $|G\rangle$ is the stabilizer state associated with the operators K_j, $j = 1, \ldots, n$. The rank one projector $|G\rangle\langle G|$ is denoted by ρ_G. Note that the binary code space of a graph state $|G\rangle$, for a graph G with adjacency matrix θ, is generated by

$$S = \begin{bmatrix} \theta \\ I \end{bmatrix}.$$

Local Clifford operations. The Clifford group $\mathcal{C}_1$ on one qubit is the normalizer of $\mathcal{G}_1$ in $U(2)$, i.e. it is the subgroup of 2×2 unitary operators which map $\mathcal{G}_1$ to itself under conjugation. The local Clifford group $\mathcal{C}_n^l := \mathcal{C}_1^{\otimes n}$ on n qubits is the n-fold tensor product of $\mathcal{C}_1$ with itself. When disregarding the overall phases of the elements in $\mathcal{G}_1$, it is easy to see there exists a one-to-one correspondence between the one-qubit Clifford operations and the 6 possible invertible linear transformations of $\mathbb{F}_2^2$, since each one-qubit Clifford operator performs one of the 6 possible permutations of the Pauli matrices and leaves the identity fixed. Generalizing to n-qubit local Clifford operations, it follows that each $U \in \mathcal{C}_n^l$ corresponds to a matrix $Q \in M_{2n}(\mathbb{F}_2)$ 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. We denote the diagonal entries of A, B, C, D, respectively, by a_i, b_i, c_i, d_i, respectively. The n submatrices

$$Q^{(i)} := \begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix}$$

correspond to the tensor factors of U. It follows from the above discussion that each of the matrices $Q^{(i)}$ is invertible. We denote the group of all such Q by C_n^l. It follows that two stabilizer codes $\rho_{\mathcal{S}}$, $\rho_{\mathcal{S}'}$ with generator matrices S, S', respectively, are equivalent under the local Clifford group if and only if there exists $Q \in C_n^l$ such that

$$\mathcal{C}_{QS} = \mathcal{C}_{S'}. \tag{5}$$

To see this, simply note that $U\rho_{\mathcal{S}}U^\dagger = \rho_{\mathcal{S}'}$ for some $U \in \mathcal{C}_n^l$ if and only $U\mathcal{S}U^\dagger = \mathcal{S}'$.

Finally, for our investigation it is important to note that any stabilizer state is locally equivalent to a (generally nonunique) graph state under the local Clifford group [12].

IV. INVARIANTS, PERMUTATIONS AND BINARY TREES

In this section, we recall the constructions of basic polynomial invariants reported in refs. [6, 7].

Let $\rho \in M_{2^n}(\mathbb{C})$ be an n-qubit density operator. Any homogeneous polynomial $F(\rho)$ of degree r in the entries of ρ can be written in a unique way as a trace

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

where $A_F \in M_{2^{nr}}(\mathbb{C})$. 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 exactly the entries of A_F. Consequently, $F(\rho)$ is an invariant of $U(2)^{\otimes n}$ if and only if

$$[A_F, U^{\otimes r}] = 0 \tag{6}$$

for every $U \in U(2)^{\otimes n}$. Therefore, the study of invariant homogeneous polynomials of fixed degree r is transformed to the study of the algebra of matrices A_F which satisfy (6). It was shown by Rains [7] that a set of matrices which linearly generate this algebra can be obtained in a one-to-one correspondence with the group $\mathcal{S}_r^n$ as follows: let $\Pi = (\mu, \nu, \xi, \ldots) \in \mathcal{S}_r^n$ be an n-tuple of permutations. The matrix $T_\Pi \in M_{2^{nr}}(\mathbb{C})$ is defined as the permutation matrix which acts on $(\mathbb{C}^{2^n})^{\otimes r}$ by permuting

FIG. 1: Binary tree on 10 nodes with maximal right paths (1, 3, 9, 10), (2), (4, 7, 8) and (5, 6). Note the canonical way in which the nodes are labelled.

the r copies of the ith qubit according to the ith permutation of Π, i.e., T_Π maps a tensor

$$\psi_{i_1,j_1,k_1\ldots;\ i_2,j_2,k_2\ldots;\ \ldots;\ i_r,j_r,k_r\ldots} \in (\mathbb{C}^{2^n})^{\otimes r}$$

to

$$\psi_{i_{\mu(1)},j_{\nu(1)},k_{\xi(1)}\ldots;\ i_{\mu(2)},j_{\nu(2)},k_{\xi(2)}\ldots;\ \ldots;\ i_{\mu(r)},j_{\nu(r)},k_{\xi(r)}\ldots}.$$

If Π ranges over all elements in $\mathcal{S}_r^n$, the matrices T_Π linearly generate the algebra defined by (6). Therefore, one obtains a generating set of basic invariants $I_{r,\Pi}$ of degree r, where

$$I_{r,\Pi}(\rho) := \mathrm{Tr}\ (T_\Pi \cdot \rho^{\otimes r}). \tag{7}$$

However, linear dependencies within the set of matrices T_Π do exist and therefore the resulting set of invariants is not minimal. In ref. [6] Grassl et al. improved the above result, as the authors presented a method which is able to pinpoint within the set $\{I_{r,\Pi}\}_\Pi$ a linearly independent subset for every r. Their approach was to consider *binary trees* and to associate with every binary tree B on r nodes a permutation $\pi(B) \in \mathcal{S}_r$. Enumeration of all possible n-tuples of permutations obtained in this way then yields a linearly independent subset of basic invariants. We now repeat the details of this construction.

A (labelled, ordered and connected) binary tree B on r vertices is a special instance of a simple, oriented and connected graph, i.e. it consists of a set of vertices or nodes $V = \{1, \ldots, r\}$ which can be connected by arrows according to a number of prescriptions. If there is an arrow from a node $f \in V$ to a node $s \in V$ then f is called the father of s and, conversely, s is a son of f. In a binary tree, all nodes but one have exactly one father. The one node without father is called the root of the tree. Furthermore, every node has at most two sons (called left and right son, respectively). The labelling of the r nodes is obtained by traversing the tree in the order root - left subtree - right subtree. A *maximal right path* p in a binary tree B is an ordered tuple of nodes $p = (v_0, v_1, \ldots, v_s)$ such that v_0 is not the right son of any node of B, v_i is the right son of v_{i-1} for $i = 1, \ldots, s$ and v_s has no right son. An example of a labelled binary tree is given in Fig. 1.

Denoting by $\mathcal{R}(B)$ the set of all maximal right paths of B, the permutation $\pi(B)$ associated with the binary tree B is defined by the product of cycles

$$\pi(B) = \prod_{(v_0,v_1,\ldots,v_s)\ \in\ \mathcal{R}(B)} (v_0 v_1 \ldots v_s).$$

Note that $\pi(B) \in \mathcal{S}_r$ whenever B has exactly r nodes and that there is a one-to-one correspondence between B and $\pi(B)$. The set of all permutations obtained in this way is denoted by $\mathcal{P}_r$. According to the result in [6], the invariants $\{I_{r,\Pi}\}$, where $\Pi = (\pi_1, \ldots, \pi_r) \in \mathcal{P}_r^n$ ranges over all n-tuples of permutations in $\mathcal{P}_r$, forms a vector space basis of the homogeneous invariants of degree r.

To conclude this section, we state some definitions regarding binary trees, which will be used below. Let B be a binary tree on r nodes. The *start* $\mathrm{st}(p)$ of a path $p = (v_0, v_1, \ldots, v_s) \in \mathcal{R}(B)$ is the element v_0 and the *finish* $\mathrm{fin}(p)$ is the element v_s. The *length* of p is the number $s + 1$. By an expression of the form "$i \in p$" is meant that the node i belongs to the set $\{v_0, v_1, \ldots, v_s\}$ (note that, due to the canonical labelling of the nodes, there is a one-to-one correspondence between p and the set $\{v_0, v_1, \ldots, v_s\}$). For every node i, the path $p(i) \in \mathcal{R}(B)$ is the unique maximal right path such that $i \in p(i)$.

Let B have $t := |\mathcal{R}(B)|$ maximal right paths $p_1, \ldots, p_t$, which we suppose to be ordered in such a way that $\mathrm{st}(p_1) < \mathrm{st}(p_2) < \cdots < \mathrm{st}(p_t)$. The columns $(R_B)_j$ of the matrix $R_B \in M_{r\times t}(\mathbb{F}_2)$ are defined by:

$$(R_B)_j = \sum_{i \in p_j} e_i, \tag{8}$$

for every $j \in \{1, \ldots, t\}$, where e_i is the ith canonical base vector in $\mathbb{F}_2^r$. The columns $(D_B)_j$ of the matrix $D_B \in M_r(\mathbb{F}_2)$ are defined by:

$$(D_B)_j = \sum_{i \in p(j),\ i \leq j} e_i, \tag{9}$$

for every $j \in \{1, \ldots, r\}$. Finally, the linear space V_B consists of all $x \in \mathbb{F}_2^r$ such that $\sum_{i\in p} x_i = 0$ for every $p \in \mathcal{R}(B)$ (i.e., V_B is the null space of the matrix R_B^T).

V. MAIN RESULT AND DISCUSSION

We are now in a position to state the central result of this paper.

Theorem 1 *Let $\rho_{\mathcal{S}}$ be a stabilizer code of length n and dimension k with generator matrix S. Let S_i^T $(i = 1, \ldots, n)$ be the $2 \times k$ submatrix of S obtained by selecting the ith and the $(n+i)$th row of S. Fix $r \in \mathbb{N}_0$, let $B_1, B_2, \ldots, B_n$ be n binary trees on r nodes and let $\Pi \in \mathcal{P}_r^n$ be the associated n-tuple of permutations. Then*

$$log_2\ I_{r,\Pi}(\rho_{\mathcal{S}}) \sim dim_{\mathbb{F}_2}\ ker \begin{bmatrix} R_{B_1}^T \otimes S_1^T \\ R_{B_2}^T \otimes S_2^T \\ \ldots \\ R_{B_n}^T \otimes S_n^T \end{bmatrix}, \tag{10}$$

where $\sim$ denotes equality up to an additive constant independent of $\rho_{\mathcal{S}}$.

Theorem 1 shows how the information contained in the invariants $I_{r,\Pi}$ can be recuperated within the binary representation of the stabilizer formalism. The fact that *a* translation into the binary framework is possible is of course not unexpected, as a stabilizer code is, up to information about the overall phases of its stabilizer elements, defined by its generator matrix. Moreover, these phases do not play a role in determining the (local) equivalence class of a code [9]. However, the simple form of the result (10) is remarkable: an invariant $I_{r,\Pi}$ is in a one-to-one correspondence with the dimension of a binary linear space which depends only on the generator matrix S - and this in a very transparant way. Additionally, it is interesting to notice the explicit way in which the n-tuple of binary trees appear in the result: every matrix R_{B_i}, corresponding to the ith binary tree, is coupled via a tensor product to the matrix S_i, which is the subblock of S containing the information about the ith qubit. Finally, we note that the r.h.s. of (10) can be computed efficiently via a calculation of the rank over $\mathbb{F}_2$ of the matrix

$$\begin{bmatrix} R_{B_1}^T \otimes S_1^T \\ R_{B_2}^T \otimes S_2^T \\ \cdots \\ R_{B_n}^T \otimes S_n^T \end{bmatrix}. \tag{11}$$

Before proving theorem 1 in section VI, we investigate the invariants (10) in more detail. We start with the invariants of smallest nontrivial degree, i.e. $r = 2$. There are exactly two binary trees on 2 vertices, as node 2 can either be the right or the left son of node 1. Equivalently, there are two possible matrices R_B according to definition (8), namely

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad [1\ 1]^T, \tag{12}$$

where the identity matrix corresponds to the tree where 2 is the left son of 1. Now, consider an n-tuple $(B_1, \ldots, B_n)$ of binary trees and the corresponding n-tuple of permutations $\Pi \in \mathcal{P}_2^n$. Let $\omega \subseteq \{1, \ldots, n\}$ denote the set of all i such that $R_{B_i} = [1\ 1]^T$ - note that every n-tuple of binary trees on 2 nodes corresponds uniquely to such a set ω. Using the notation S_i as in theorem 1, this implies that

$$R_{B_i}^T \otimes S_i^T = [S_i^T\ \ S_i^T]$$

whenever $i \in \omega$ and

$$R_{B_i}^T \otimes S_i^T = \begin{bmatrix} S_i^T & 0 \\ 0 & S_i^T \end{bmatrix}$$

otherwise. Therefore, the null space of the matrix (11) consists of all vectors $(x, x') \in \mathbb{F}_2^{2k}$ such that

$$\begin{aligned} S_i(x + x') = 0 &\quad \text{for every } i \in \omega \\ S_j x = S_j x' = 0 &\quad \text{for every } j \in \omega^c, \end{aligned} \tag{13}$$

where ω^c is the complement of ω in $\{1, \ldots, n\}$. Note that (13) implies that $Sx = Sx'$ and therefore $x = x'$, since S has full rank. Thus, the solutions of (13) are in a one-to-one correspondence with the linear subspace of $\mathbb{F}_2^k$ of those x satisfying $S_j x = 0$ for every $j \in \omega^c$. The linear mapping $\phi_S : \mathbb{F}_2^k \to \mathbb{F}_2^{2n}$ defined by the matrix S maps the space of such x's to the space of vectors $y = Sx$ which satisfy $y_j = y_{n+j} = 0$ for every $j \in \omega^c$. As S has full rank, the mapping ϕ_S is injective and the spaces of the x's and the y's have equal dimension. Recalling that the *support* $\text{supp}(v)$ of any $v \in \mathbb{F}_2^{2n}$ is the subset of those $i \in \{1, \ldots, n\}$ such that $(v_i, v_{n+i}) \neq (0, 0)$, we can state that the supports of the y's lie within the set ω. Thus, we have shown that

$$\log_2 I_{2,\Pi} \sim \dim \{y \in \mathcal{C}_S |\ \text{supp}(y) \subseteq \omega\}. \tag{14}$$

This is clearly a more insightful presentation of the invariants $I_{2,\Pi}$ than (10), as (14) relates invariants to the dimensions of the subspaces $\mathcal{C}_S^\omega$ of the code space $\mathcal{C}_S$. Moreover, a similar argument as above can be made to obtain an analogous presentation of the invariants of higher degree:

Theorem 2 *Let S be a $2n \times k$ generator matrix of a stabilizer code and let the subblocks S_i^T be defined as in theorem 1. Fix $r \in \mathbb{N}_0$ and let $B_1, \ldots, B_n$ be n binary trees on r vertices. Let $\mathcal{R} = \mathcal{R}(B_1) \cup \cdots \cup \mathcal{R}(B_n)$ denote the set of all maximal right paths of these trees. For every $p \in \mathcal{R}$, let ω_p denote the subset of all $i \in \{1, \ldots, n\}$ such that $p \notin \mathcal{R}(B_i)$. Then the dimension of the kernel of the matrix (11) is equal to the dimension of the space*

$$\begin{aligned} \{(y^{(1)}, \ldots, y^{(r)}) \in\ & \mathcal{C}_S \times \cdots \times\ \mathcal{C}_S | \\ & supp\ (\sum_{j \in p} y^{(j)}) \subseteq \omega_p,\ \ for\ every\ p \in \mathcal{R}\}. \end{aligned} \tag{15}$$

The proof of theorem 2 is omitted, as it is a straightforward generalization of the considerations made above for the invariants of degree 2. A number of properties of the invariants immediately follow from theorem 2: e.g., consider an invariant I_{r+1,Π_0} such that its n binary trees B_i have got a common maximal right path p_0 of exactly one element i_0, i.e. $p_0 = (i_0) \in \mathcal{R}(B_1) \cap \cdots \cap \mathcal{R}(B_n)$. Considering (15) for this invariant, it follows that $\omega_{p_0} = \emptyset$. Consequently, $\text{supp}(y^{(i_0)}) \subseteq \emptyset$ and therefore $y^{(i_0)} = 0$ for every $y^{(i_0)}$ in (15). Thus, the invariant I_{r+1,Π_0} is equal to an invariant of degree r corresponding to binary trees $\bar{B}_i$ which are obtained by deleting the node i_0 from the original trees B_i. Reversing the above argument shows that any invariant of degree r can be written as an invariant of degree $r + 1$, thereby showing that

$$\{I_{r,\Pi}\}_\Pi \subset \{I_{r+1,\Pi'}\}_{\Pi'}$$

for every r, where Π (Π') ranges over all elements in $\mathcal{P}_r^n$ ($\mathcal{P}_{r+1}^n$). Moreover, this argument can be generalized to show that an invariant corresponding to a tuple of binary trees which have some subtree in common, can be written as the product of invariants of lower degree.

VI. PROOF OF THEOREM 1

The proof of theorem 1 is given in two main parts. We show in subsection A that it is sufficient to prove the theorem for graph states. The proof of theorem 1 for graph states is subsequently given in subsection B. For the remainder of this section, we fix r and consider an n-tuple $\Pi = (\pi_1, \ldots, \pi_n)$ of permutations $\pi_i \in \mathcal{P}_r$ and n binary trees B_i on r vertices corresponding to the permutations π_i. We denote $\mathcal{B} := (B_1, \ldots, B_n)$.

A. Reduction to graph states

Suppose that theorem 1 holds for all graph states. Let $\rho_{\mathcal{S}}$ be a stabilizer code of length n and dimension k with generator matrix S. For large enough $m > n$, there exists a stabilizer state $|\psi\rangle$ on m qubits such that $\rho_{\mathcal{S}}$ can be obtained from $|\psi\rangle$ by tracing out the qubits $n+1, \ldots, m$, i.e.

$$\rho_{\mathcal{S}} = |\psi\rangle\langle\psi|^{\{1,\ldots,n\}}$$

using the notation of section 3. Furthermore, $|\psi\rangle$ is equivalent to some graph state $|G\rangle$ under the local Clifford group. Denoting $\omega = \{1, \ldots, n\}$, it follows that $\rho_{\mathcal{S}}$ is locally equivalent to ρ_G^{ω}. Letting S' be the generator matrix of $|G\rangle$, this last fact translates into the binary picture as

$$\mathcal{C}_{QS} = \mathcal{C}_{S'}^{\omega} \tag{16}$$

for some $Q \in C_n^l$. Now, let $\Pi' \in \mathcal{P}_r^m$ be the m-tuple of permutations which is obtained by appending to Π $m-n$ times the identity permutation (which belongs to $\mathcal{P}_r$) and let $\mathcal{B}' = (B_1, \ldots, B_n, B_0, \ldots, B_0)$ be the associated m-tuple of binary trees; here B_0 is the binary tree with r maximal right paths (i), corresponding to the identity permutation. The crucial observation is now

$$I_{r,\Pi}(\rho_{\mathcal{S}}) = I_{r,\Pi'}(\psi).$$

This identity can easily be verified by using the definition of $I_{r,\Pi'}$. Moreover, $I_{r,\Pi'}(\psi) = I_{r,\Pi'}(\rho_G)$ since the states $|\psi\rangle$ and $|G\rangle$ are locally equivalent. We can now apply theorem 1 and find

$$\begin{aligned} \log_2 I_{r,\Pi}(\rho_{\mathcal{S}}) &= \log_2 I_{r,\Pi'}(\rho_G) \\ &\sim \dim_{\mathbb{F}_2} \ker \begin{bmatrix} R_{B_1}^T \otimes S_1'^T \\ \cdots \\ R_{B_n}^T \otimes S_n'^T \\ R_{B_0}^T \otimes S_{n+1}'^T \\ \cdots \\ R_{B_0}^T \otimes S_m'^T \end{bmatrix} \end{aligned} \tag{17}$$

Applying theorem 2 to the generator matrix S' and the binary trees $\mathcal{B}'$, (17) is equal to the dimension of

$$\begin{aligned} \{(y^{(1)}, \ldots, y^{(r)}) \in \ &\mathcal{C}_{S'} \times \cdots \times \ \mathcal{C}_{S'} | \\ &\text{supp } (\sum_{j \in p} y^{(j)}) \subseteq \omega_p, \text{ for every } p \in \mathcal{R}'\} \end{aligned} \tag{18}$$

where $\mathcal{R}' = \mathcal{R}(B_1) \cup \cdots \cup \mathcal{R}(B_n) \cup \mathcal{R}(B_0)$. As the last $m-n$ trees in the m-tuple $\mathcal{B}'$ are equal to B_0, every $y^{(j)}$ in (18) has $\text{supp}(y^{(j)}) \subseteq \omega$. Therefore, the dimension of (18) is equal to the dimension of

$$\begin{aligned} \{(x^{(1)}, \ldots, x^{(r)}) \in \ &\mathcal{C}_{S'}^{\omega} \times \cdots \times \ \mathcal{C}_{S'}^{\omega} | \\ &\text{supp } (\sum_{j \in p} x^{(j)}) \subseteq \omega_p, \text{ for every } p \in \mathcal{R}\} \end{aligned} \tag{19}$$

where now $\mathcal{R} = \mathcal{R}(B_1) \cup \cdots \cup \mathcal{R}(B_n)$. Finally, we recall the identity (16) and note that (19) remains invariant if $\mathcal{C}_{QS}$ is replaced by $\mathcal{C}_S$. A last application of theorem 2 yields

$$\log_2 I_{r,\Pi}(\rho_{\mathcal{S}}) \sim \dim_{\mathbb{F}_2} \ker \begin{bmatrix} R_{B_1}^T \otimes S_1^T \\ R_{B_2}^T \otimes S_2^T \\ \cdots \\ R_{B_n}^T \otimes S_n^T \end{bmatrix}, \tag{20}$$

which is the desired result.

B. Proof of theorem 1 for graph states

Fix a graph G on n vertices with adjacency matrix θ and the generator matrix

$$S = \begin{bmatrix} \theta \\ I \end{bmatrix},$$

which has $2 \times n$ subblocks S_i^T defined as in theorem 1 by

$$S_i^T = \begin{bmatrix} \theta_i^T \\ e_i^T \end{bmatrix}.$$

The proof of theorem 1 for the case where $\rho_{\mathcal{S}} = \rho_G$ is structured as follows: in lemma 3 we show that the invariant $I_{r,\Pi}(\rho_G)$ is equal to a sum of the form

$$\frac{1}{N} \sum_{X \in \mathcal{V}} (-1)^{\mathcal{Q}(X)}, \tag{21}$$

where N is a normalization factor independent of G, $\mathcal{V}$ is a linear subspace of $M_{n \times r}(\mathbb{F}_2)$ and $\mathcal{Q}$ is a quadratic form on $M_{n \times r}(\mathbb{F}_2)$. Preliminary material used to prove this result will be gathered in lemmas 1 and 2. In lemma 4, we subsequently show that the form $\mathcal{Q}$ is in fact identical zero on the space $\mathcal{V}$, which implies that the sum in (21) is (up to the normalization) equal to the cardinality of $\mathcal{V}$. Finally, this cardinality is related to the r.h.s of (10) and the proof of theorem 1 is completed.

It will be convenient to work with a real variant of the set of Pauli matrices (as in ref. [13]), defined by

$$\begin{aligned} \tau_{00} &= \sigma_{00}, \\ \tau_{01} &= \sigma_{01}, \\ \tau_{10} &= \sigma_{10}, \\ \tau_{11} &= i\sigma_{11} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \end{aligned} \tag{22}$$

which we will call the tau matrices. Analogous to the notation introduced in section 3, n-fold products of tau matrices are represented as

$$\tau_{u_1 v_1} \otimes \cdots \otimes \tau_{u_n v_n} = \tau_{(u,v)},$$

where $(u,v) = (u_1, \ldots, u_n, v_1, \ldots, v_n) \in \mathbb{F}_2^{2n}$. We now prove a useful parameterization of the projector ρ_G:

Lemma 1 *The projector ρ_G can be parameterized as follows:*

$$\rho_G = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{k_\theta(x)} \; \tau_{(\theta x, x)}, \tag{23}$$

where k_θ is the quadratic form over $\mathbb{F}_2$ associated with θ, i.e., $k_\theta(x) = \sum_{i<j} \theta_{ij} x_i x_j$.

Proof: the state $|G\rangle$ is defined by the n relations $\tau_{(\theta_j, e_j)}|G\rangle = |G\rangle$, where θ_j is the jth column of θ and e_j is the jth canonical basis vector of $\mathbb{F}_2^n$. The stabilizer of $|G\rangle$ consists of all products

$$M_x = \prod_{j=1}^n \tau_{(\theta_j, e_j)}{}^{x_j},$$

where $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. After a repeated application of the multiplication rule [13]

$$\tau_{(u,v)} \tau_{(u',v')} = (-1)^{v^T u'} \tau_{(u+u', v+v')},$$

where $u, u', v, v' \in \mathbb{F}_2^n$, we arrive at

$$M_x = (-1)^{k_\theta(x)} \; \tau_{(\theta x, x)}.$$

Since $\rho_G = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} M_x$, we obtain the result. $\square$

Lemma 1 will be used below to compute the invariant $I_{r,\Pi}(\rho_G)$. After plugging (23) in (7), we will be dealing with expressions of the form

$$\mathrm{Tr}\;(T_\Pi \; \tau_1 \otimes \tau_2 \otimes \cdots \otimes \tau_r), \tag{24}$$

where the τ_i's are themselves n-fold tensor products of the tau matrices, i.e. $\tau_i \in \mathcal{G}_n$ for every $i = 1, \ldots, r$. A closer look at these expressions beforehand is appropriate. To this end, let $X, Y, \ldots$ be any r operators in $M_2(\mathbb{C})^{\otimes n}$, i.e.,

$$\begin{aligned} X &= X_1 \otimes \cdots \otimes X_n, \\ Y &= Y_1 \otimes \cdots \otimes Y_n, \; \ldots, \end{aligned}$$

where $X_i, Y_i, \cdots \in M_2(\mathbb{C})$. Furthermore, for any $\pi \in \mathcal{P}_r$ we denote

$$A_{r,\pi}(U, V, \ldots) := \sum_{i_1, \ldots, i_r} U_{i_1 i_{\pi(1)}} \; V_{i_2 i_{\pi(2)}} \cdots,$$

where U, $V, \ldots$ are r arbitrary 2×2 matrices. Using the definition of T_Π, it is then easy to check that

$$\mathrm{Tr}\;(T_\Pi \; X \otimes Y \otimes \ldots) = \prod_{i=1}^n A_{r,\pi_i}(X_i, Y_i, \ldots). \tag{25}$$

It follows that (24) is a product of n factors of the form

$$A_{r,\pi}(\tau_{u_1 v_2}, \ldots, \tau_{u_r v_r}) =: A_{r,\pi}(u,v),$$

where $u = (u_1, \ldots, u_r)$ and $v = (v_1, \ldots, v_r) \in \mathbb{F}_2^r$. Expressions of this type are calculated in lemma 2:

Lemma 2 *Let $\pi \in \mathcal{P}_r$ be a permutation corresponding to a binary tree B and let $(u,v) \in \mathbb{F}_2^{2r}$. Let the matrix D_B and the space V_B be defined as in section 4. Then*

$$A_{r,\pi}(u,v) = \begin{cases} 2^{r - dim \; V_B} (-1)^{u^T D_B^T v} & \text{if } u, v \in V_B \\ 0 & \text{otherwise} \end{cases}$$

Proof: First, note that the entries of the 1-qubit operators τ_{ab} can be parameterized as

$$(\tau_{ab})_{x,y} = (-1)^{a(b+x)} \delta_{x+y,b},$$

where $a, b, x, y \in \mathbb{F}_2$. Using this formula in the definition of $A_{r,\pi}$, we obtain

$$A_{r,\pi}(u,v) = \sum_{x \in \mathbb{F}_2^r} (-1)^{u^T(v+x)} \delta_{x_1 + x_{\pi(1)}, v_1} \cdots \delta_{x_r + x_{\pi(r)}, v_r}.$$

Equivalently, the sum runs over all $x \in \mathbb{F}_2^r$ which lie in the affine subspace determined by the equations $x_i + x_{\pi(i)} = v_i$ for all $i = 1, \ldots, r$. However, this system of equations may not be consistent: indeed, one can easily show that a solution exists iff $v \in V_B$. Whenever this is the case, the solutions are given by $x = x_0 + x'$, where $x_0 = D_B^T v + v$ and x' satisfies $x'_i + x'_{\pi(i)} = 0$ for every $i = 1, \ldots, r$. Moreover, the space of all such x' is the orthogonal complement of V_B with respect to the standard inner product in $\mathbb{F}_2^r$ (or equivalently, the column space of R_B), as one can verify. Therefore, we have

$$A_{r,\pi}(u,v) = \begin{cases} \sum_{x' \in V_B^\perp} (-1)^{u^T(D_B^T v + x')} & \text{if } v \in V_B \\ 0 & \text{otherwise} \end{cases}$$

Furthermore, the sum $\sum_{x' \in V_B^\perp} (-1)^{u^T x'}$ is equal to $2^{r - \dim V_B}$ if $u \in V_B$ and zero otherwise. This proves the result. $\square$

We now proceed in calculating the invariant $I_{r,\Pi}(\rho_G)$. Using lemma 1 in (7), we find that $I_{r,\Pi}(\rho_G)$ is equal to the sum

$$\frac{1}{2^{nr}} \sum_{x^{(1)},\ \dots,\ x^{(r)}\ \in\ \mathbb{F}_2^n} \Big\{ (-1)^{\sum_{i=1}^r k_\theta(x^{(i)})} \times \\ \text{Tr}\ \big(T_\Pi\ \tau_{(\theta x^{(1)}, x^{(1)})} \otimes \dots \otimes \tau_{(\theta x^{(r)}, x^{(r)})} \big) \Big\} \tag{26}$$

First, denoting by $\mathcal{P}_{\text{lows}}(\theta)$ the strictly lower triangular part of θ and writing

$$X := [x^{(1)}| \dots |x^{(r)}] \in M_{n \times r}(\mathbb{F}_2),$$

we obtain the shorthand notation

$$\sum_{i=1}^r k_\theta(x^{(i)}) = \text{Tr}\ X^T \mathcal{P}_{\text{lows}}(\theta) X$$

Secondly, the trace in (26) splits into a product of n factors as in (25), each of which can be calculated by employing lemma 2. The calculation is straightforward. Defining for every $X \in M_{n \times r}(\mathbb{F}_2)$ the matrix $X_\mathcal{B} \in M_{n \times r}(\mathbb{F}_2)$ by

$$(X_\mathcal{B})_{ij} = \sum_{k=1}^r X_{ik}\,(D_{B_i})_{kj}\,,$$

one finds that (26) is equal (up to a normalization independent of G) to

$$\sum (-1)^{\ \text{Tr}\ X^T \mathcal{P}_{\text{lows}}(\theta) X +\ \text{Tr}\ X_\mathcal{B}^T \theta X}, \tag{27}$$

where the sum runs over all X such that

$$S_i^T \left(\sum_{j \in p} x^{(j)} \right) = 0 \tag{28}$$

for every $i \in \{1, \dots, n\}$ and $p \in \mathcal{R}(B_i)$. We will denote the space of all such X by $V_\mathcal{B}(G)$. We have proven:

Lemma 3 *The invariant $I_{r,\Pi}(\rho_G)$ can be written as*

$$I_{r,\Pi}(\rho_G) = \frac{1}{N} \sum_{X \in V_\mathcal{B}(G)} (-1)^{\ Tr\ X^T \mathcal{P}_{lows}(\theta) X +\ Tr\ X_\mathcal{B}^T \theta X}, \tag{29}$$

where N is a normalization factor independent of G and the definitions of $V_\mathcal{B}(G)$ and $X_\mathcal{B}$ are as above.

The last part of our argument consists of showing that the quadratic form $\mathcal{Q}(X) :=\ \text{Tr}\ X^T \mathcal{P}_{\text{lows}}(\theta) X +\ \text{Tr}\ X_\mathcal{B}^T\ \theta X$ is zero on the space $V_\mathcal{B}(G)$. Once this result is shown, the proof of theorem 1 is immediate: indeed, if $\mathcal{Q}(X) = 0$ for every $X \in V_\mathcal{B}(G)$ then $\log_2 I_{r,\Pi}(\rho_G) \sim \dim V_\mathcal{B}(G)$. Moreover, the matrices $X = [x^{(1)}| \dots |x^{(r)}] \in V_\mathcal{B}(G)$ can be reshaped as vectors $\tilde{X} = (x^{(1)}, \dots, x^{(r)}) \in \mathbb{F}_2^{nr}$ which are exactly the elements in the null space of the matrix

$$\begin{bmatrix} R_{B_1}^T \otimes S_1^T \\ R_{B_2}^T \otimes S_2^T \\ \dots \\ R_{B_n}^T \otimes S_n^T \end{bmatrix}. \tag{30}$$

Clearly, the spaces of the X's and the $\tilde{X}$'s have the same dimension and the proof of theorem 1 is thus completed. We now show that $\mathcal{Q} = 0$ on the space $V_\mathcal{B}(G)$:

Lemma 4 $\mathcal{Q}(X) = 0$ *for every* $X \in V_\mathcal{B}(G)$.

Proof: Let $X = [x^{(1)}| \dots |x^{(r)}]$ be an element of $V_\mathcal{B}(G)$. Recall that by definition (28) this entails that

$$\begin{bmatrix} \theta_i^T \\ e_i^T \end{bmatrix} \left(\sum_{j \in p} x^{(j)} \right) = 0 \tag{31}$$

for every $i \in \{1, \dots, n\}$ and $p \in \mathcal{R}(B_i)$. In particular,

$$\sum_{j \in p} x_i^{(j)} = 0 \tag{32}$$

for every $i \in \{1, \dots, n\}$ and for every $p \in \mathcal{R}(B_i)$, where $x^{(j)} = (x_1^{(j)}, \dots, x_n^{(j)})$. Consequently,

$$\sum_{j=1}^r x^{(j)} = 0. \tag{33}$$

Now, consider the first term of $\mathcal{Q}(X)$:

$$\begin{aligned} \mathcal{Q}_1 &:= \text{Tr}\ X^T \mathcal{P}_{\text{lows}}(\theta) X \\ &= \sum_{j=1}^r x^{(j)T} \mathcal{P}_{\text{lows}}(\theta)\ x^{(j)}. \end{aligned} \tag{34}$$

Substituting $x^{(r)} = \sum_{j=1}^{r-1} x^{(j)}$ (from (33)), an easy calculation shows that

$$\mathcal{Q}_1 = \sum_{j=1}^{r-1} \left(\sum_{k=1}^{j-1} x^{(k)} \right)^T \theta\ x^{(j)}.$$

Let $\omega_{ij} \subseteq \{1, \dots, n\}$ consist of all $k \in \{1, \dots, j-1\}$ which belong to a maximal right path p of B_i such that $\text{fin}(p) \geq j$. Then, denoting $y^{(j)} := \sum_{k=1}^{j-1} x^{(k)}$, (32) implies that $y_i^{(j)} = \sum_{k \in \omega_{ij}} x_i^{(k)}$.

The second term of $\mathcal{Q}(X)$ is

$$\begin{aligned} \mathcal{Q}_2 &:= \text{Tr}\ X_\mathcal{B}^T\ \theta X \\ &= \sum_{j=1}^r z^{(j)T} \theta\ x^{(j)}, \end{aligned} \tag{35}$$

where $z^{(j)}$ is the jth column of $X_{\mathcal{B}}$. Let η_{ij} consist of all $k \in \{1, \ldots, j-1\}$ which belong to the unique maximal right path of B_i which contains j. It then follows from the definition of $X_{\mathcal{B}}$ that $z_i^{(j)} = \sum_{k \in \eta_{ij} \cup \{j\}} x_i^{(k)}$. Note that $\eta_{ir} \cup \{r\} \in \mathcal{R}(B_i)$ and therefore $z_i^{(r)} = 0$ for every $i = 1, \ldots, n$ from (32). Thus, $z^{(r)} = 0$. Combining the above results, we obtain

$$\mathcal{Q}_1 + \mathcal{Q}_2 = \sum_{j=1}^{r-1} (y^{(j)} + z^{(j)})^T \theta\, x^{(j)}, \tag{36}$$

where

$$y_i^{(j)} + z_i^{(j)} = \left(\sum_{k \in \omega_{ij}} x_i^{(k)} \right) + \left(\sum_{k \in \eta_{ij}} x_i^{(k)} \right) + x_i^{(j)}. \tag{37}$$

In the sum (37), every $k \in \omega_{ij} \cap \eta_{ij}$ gives rise to a double appearance of the term $x_i^{(k)}$ and consequently all such terms vanish. As $\eta_{ij} \subseteq \omega_{ij}$, we obtain

$$y_i^{(j)} + z_i^{(j)} = \left(\sum_{k \in \omega_{ij} \setminus \eta_{ij}} x_i^{(k)} \right) + x_i^{(j)}. \tag{38}$$

When using (38) to calculate (36), the terms $x_i^{(j)}$ in (38) do not contribute to the sum, as they give rise to terms ${x^{(j)}}^T \theta\, x^{(j)}$ in (36), which are equal to zero since θ is symmetric. Thus, defining the vectors $u^{(j)}$ by

$$u_i^{(j)} := \left(\sum_{k \in \omega_{ij} \setminus \eta_{ij}} x_i^{(k)} \right),$$

(36) becomes

$$\mathcal{Q}(X) = \sum_{j=1}^{r-1} {u^{(j)}}^T \theta\, x^{(j)}. \tag{39}$$

Note that the set $\omega_{ij} \setminus \eta_{ij}$ consists of all $k \in \{1, \ldots, j-1\}$ which belong to some path $p \neq p(j)$ in $\mathcal{R}(B_i)$ such that $\text{fin}(p) \geq j$. We now show that whenever j and l belong to the same maximal right path of B_i, one has $\omega_{ij} \setminus \eta_{ij} = \omega_{il} \setminus \eta_{il}$ and consequently $u_i^{(j)} = u_i^{(l)}$. To see this, fix i and consider arbitrary nodes j and l which lie on the same maximal right path of B_i. Without loss of generality we can assume that $j < l$. Denoting by j' the right son of j, we prove that $\omega_{ij} \setminus \eta_{ij} = \omega_{ij'} \setminus \eta_{ij'}$: indeed, if $j' = j + 1$ then j does not have a left son (due to the canonical labelling of the nodes) and the assertion follows trivially; if on the other hand $j' > j + 1$ then j has a left subtree. However, the maximal right paths p in this subtree do not contribute to $\omega_{ij'} \setminus \eta_{ij'}$, as they all satisfy $\text{fin}(p) < j'$ (which is again due to the canonical labelling of the nodes). Therefore $\omega_{ij} \setminus \eta_{ij} = \omega_{ij'} \setminus \eta_{ij'}$ and iteration of this argument shows that $\omega_{ij} \setminus \eta_{ij} = \omega_{il} \setminus \eta_{il}$.

We will now use the above property of the $u^{(j)}$'s to show that $\mathcal{Q}(X) = 0$. Let us consider the first binary tree B_1 and suppose that $(1, 2, 3)$ is a maximal right path of this tree. This example is chosen for notational convenience, but the argument will work for any maximal right path in any tree. Thus, we have $u_1^{(1)} = u_1^{(2)} = u_1^{(3)} \equiv u$. Denoting $u^{(j)} = (u, v^{(j)})$ for $j = 1, 2, 3$, the relevant terms in (39) are

$$\begin{aligned}
&{u^{(1)}}^T \theta\, x^{(1)} + {u^{(2)}}^T \theta\, x^{(2)} + {u^{(3)}}^T \theta\, x^{(3)} \\
&= (u, v^{(1)})^T \theta\, x^{(1)} + (u, v^{(2)})^T \theta\, x^{(2)} + (u, v^{(3)})^T \theta\, x^{(3)} \\
&= (u,\ 0\ )^T \theta (x^{(1)} + x^{(2)} + x^{(3)}) \\
&\quad + (0, v^{(1)})^T \theta\, x^{(1)} + (0, v^{(2)})^T \theta\, x^{(2)} + (0, v^{(3)})^T \theta\, x^{(3)}
\end{aligned}$$

In the r.h.s. of the last equality, the first term is equal to

$$u\ \theta_1^T (x^{(1)} + x^{(2)} + x^{(3)}),$$

which is equal to zero from (31), since $(1, 2, 3)$ is a maximal right path of B_1. Applying this argument to all the maximal right paths of the trees in $\mathcal{B}$ shows that indeed $\mathcal{Q} = 0$ on the space $V_{\mathcal{B}}(G)$. This ends the proof. □

VII. CONCLUSION

In this paper, we have considered a complete family of local invariants of stabilizer codes and we have given a translation of these invariants into the binary representation of the stabilizer formalism. In particular, we have related invariants to dimensions of binary subspaces which depend only on the generator matrix of a code. The aim of this investigation is mainly to provide a tool to study the structure of equivalence classes of codes. We note that some important issues in the present matter remain to be settled: firstly, it is to date not clear how a finite complete set of invariants can be constructed, i.e., what the minimal degree r is such that the values of the invariants of degree smaller than r determine the local equivalence class of any stabilizer code. Secondly, there is the question whether it is sufficient to consider local Clifford operations in order to recognize local equivalence of stabilizer codes. In other words, are two stabilizer codes locally equivalent if and only if they are equivalent under the local Clifford group? We believe that the results in this paper are a significant step towards answering these questions.

Acknowledgments

MVDN thanks M. Hein, for interesting discussions concerning local equivalence of stabilizer states. Dr. Bart De Moor is a full professor at the Katholieke Universiteit Leuven, Belgium. Research supported by Research

Council KUL: GOA-Mefisto 666, GOA-Ambiorics, several PhD/postdoc and fellow grants; Flemish Government: - FWO: PhD/postdoc grants, 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: PhD Grants, 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; QUIPROCONE; QUPRODIS.

[1] D. Gottesman. *Stabilizer codes and quantum error correction.* PhD thesis, Caltech, 1997. quant-ph/9705052.

[2] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction via codes over gf(4). *IEEE transactions on information theory.* quant-ph/9608006.

[3] I. Chuang and M. Nielsen. *Quantum computation and quantum information.* Cambridge University press, 2000.

[4] A.L. Onishchik and E.B. Vinberg. *Lie groups and algebraic groups.* springer, Berlin, 1990.

[5] T.A. Springer. *Invariant theory*, volume 585 of *Lecture notes in mathematics.* Springer, Berlin, 1977.

[6] M. Grassl, M. Rötteler, and T. Beth. Computing local invariants of qubit systems. *Phys.Rev. A*, 58:1833–1839, 1998. quant-ph/9712040.

[7] E.M. Rains. Polynomial invariants of quantum codes. quant-ph/9704042.

[8] M. Hein, J. Eisert, and H.J. Briegel. Multi-party entanglement in graph states. quant-ph/0307130.

[9] M. Van den Nest, J. Dehaene, and B. De moor. Graphical description of the action of local clifford operations on graph states. *Phys. Rev. A*, 69:022316, 2004. quant-ph/0308151.

[10] R. Raussendorf, D.E. Browne, and H.J. Briegel. Measurement-based quantum computation with cluster states. *Phys. Rev. A*, 68:022312, 2003. quant-ph/0301052.

[11] W. Dür, H. Aschauer, and H.J. Briegel. Multiparticle entanglement purification for graph states. *Phys. Rev. Lett.*, 91:107903, 2003. quant-ph/0303087.

[12] D. Schlingemann. Stabilizer codes can be realized as graph codes. quant-ph/0111080.

[13] J. Dehaene and B. De Moor. The clifford group, stabilizer states, and linear and quadratic operations over gf(2). *Phys. Rev. A*, 68:042318, 2003. quant-ph/0304125.

[14] A simple graph G has no loops or multiple edges. Therefore, it can be described by a $n \times n$ symmetric matrix θ where θ_{ij} is equal to 1 whenever there is an edge between vertices i and j and zero otherwise. As G has no loops, $\theta_{ii} = 0$ for every $i = 1, \ldots, n$