Local equivalence of stabilizer states

Maarten Van den Nest, Jeroen Dehaene, Bart De Moor

Katholieke Universiteit Leuven, ESAT-SCD
Kasteelpark Arenberg 10, B-3001 Leuven, Belgium
E-mail: mvandenn@esat.kuleuven.ac.be

May 13, 2004

Abstract

In this paper we study local equivalence classes of stabilizer states. We discuss equivalence under stochastic local operations and classical communication (SLOCC), local unitary equivalence (LU) and local Clifford equivalence (LC). We show that two stabilizer states are SLOCC-equivalent if they are LU-equivalent. Focussing subsequently on LU-equivalence, we discuss LU-invariants. Furthermore, we give a graphical description of the action of LC-operations on graph states and present an efficient algorithm which recognizes whether two given stabilizer states are LC-equivalent.

1 Introduction

Stabilizer states have been studied extensively and play an important role in numerous applications in quantum information theory and quantum computing. A stabilizer state is a multiqubit pure state which is the unique simultaneous eigenvector of a complete set of commuting observables in the Pauli group, where the latter consists of all tensor products of Pauli matrices and the identity (with an additional phase factor). Graph states are special cases of stabilizer states, for which the defining set of commuting Pauli operators can be constructed on the basis of a mathematical graph. As stabilizer states can be described in a relatively transparent way, while they maintain a sufficiently rich structure, they have been employed in various fields of quantum information theory and quantum computing: in the theory of quantum error-correcting codes, the stabilizer formalism is used to construct so-called stabilizer codes which protect quantum systems from decoherence effects [1]; graph states have been used in multipartite purification schemes [2] and a measurement-based computational model has been designed which uses a particular graph state, namely the cluster state, as a universal resource for quantum computation - the one-way quantum computer [3]. Graph states have also been considered in the context of multi-particle entanglement: in [4] the entanglement in graph states was quantified and characterized in terms of the Schmidt measure.

As all of the above applications of stabilizer states use in some way the entanglement present in these states, it is sensible to investigate in more detail what the entanglement properties of stabilizer states are. It is the aim of this paper to address this question. The main objective of our investigation is a characterization of local equivalence classes of stabilizer states. Here *local* equivalence is a common denominator for SLOCC or local unitary (LU) operations. In the following, we review our recent results on this subject collected in refs. [5, 6, 7]. Most proofs are omitted and the reader is referred to these references for more details. This article is organized as follows: in section 2, we recall the basics about stabilizer states, local Clifford operations and their respective representations in terms of algebra over GF(2). We then consider equivalence of stabilizer states under SLOCC in section 3 and show that two stabilizer states are SLOCC-equivalent if and only if they are equivalent under LU. This result reduces our investigation of local equivalence to LU-equivalence. We proceed in section 4 with LU-equivalence: first, we present a complete family of invariants which separate the orbits of stabilizer states under LU. Secondly, we turn to the subgroup of the local unitary group consisting of local Clifford (LC) operations and study equivalence of stabilizer states under this important subgroup. We characterize the action of local Clifford operations on graph states in terms of a single graph transformation rule and, finally, we present an algorithm of polynomial complexity which recognizes whether two given graph states are LC-equivalent.

2 Preliminaries

2.1 Stabilizer states

The Pauli group $\mathcal{G}_n$ on n qubits consists of all 4×4^n n-fold tensor products of the form $\alpha\, v_1 \otimes v_2 \otimes \ldots \otimes v_n$, where $\alpha \in \{\pm 1, \pm i\}$ is an overall phase factor and the 2×2-matrices v_i $(i = 1, \ldots, n)$ 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 state $|\psi\rangle$ is defined as a simultaneous eigenvector with eigenvalue 1 of n commuting and independent [1] Pauli group elements M_i. The n eigenvalue equations $M_i|\psi\rangle = |\psi\rangle$ define the state $|\psi\rangle$ completely (up to an arbitrary phase). The set $\mathcal{S} := \{M \in \mathcal{G}_n | M|\psi\rangle = |\psi\rangle\}$ is called the stabilizer of the state $|\psi\rangle$. It is a group of 2^n commuting Pauli operators, all of which have

[1] This means that no product of the form $M_1^{x_1} \ldots M_n^{x_n}$, where $x_i \in \{0, 1\}$, yields the identity except when all x_i are equal to zero.

a real overall phase ± 1 and the n operators M_i are called generators of $\mathcal{S}$, as each $M \in \mathcal{S}$ can be written as $M = M_1^{x_1} \dots M_n^{x_n}$, for some $x_i \in \{0, 1\}$. The graph states [3, 2] constitute an important subclass of the stabilizer states. A (simple) graph [8] is a pair $G = (V, E)$ of sets, where V is a finite subset of $\mathbb{N}$ and the elements of E are 2-element subsets of V. The elements of V are called the vertices of the graph G and the elements of E are its edges. Usually, a graph is pictured by drawing a (labelled) dot for each vertex and joining two dots i and j by a line if the corresponding pair of vertices $\{i, j\} \in E$. For a graph with $|V| = n$ vertices, the adjacency matrix θ is the symmetric binary $n \times n$-matrix where $\theta_{ij} = 1$ if $\{i, j\} \in E$ and $\theta_{ij} = 0$ otherwise. Note that a simple graph has no loops and therefore $\theta_{ii} = 0$ for every $i = 1, \dots, n$. Now, given an n-vertex graph G with adjacency matrix θ 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 then the stabilizer state associated with the operators K_j.

We now briefly discuss the binary representation of the stabilizer formalism (for literature on this subject, see e.g. [1, 9]). Employing the mapping

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

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, an n-qubit stabilizer state corresponds to an n-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 $2n \times n$ matrix S, which is referred to as a generator matrix of the binary stabilizer subspace. This generator matrix satisfies $S^T P S = 0$ from the symplectic self-orthogonality property. The entire binary stabilizer subspace $\mathcal{C}_S$ is the column space of S, i.e., it is equal to

$$\mathcal{C}_S := \{Sx \mid x \in \mathbb{F}_2^n\}\,. \tag{2}$$

Note that the binary stabilizer space of a graph state $|G\rangle$, for a graph G with adjacency matrix θ, is generated by

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

2.2 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 (LC) 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 $2n \times 2n$ 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. 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 states $|\psi\rangle$, $|\psi'\rangle$ with generator matrices S, S', respectively, are LC-equivalent if and only if there exists $Q \in C_n^l$ such that

$$\mathcal{C}_{QS} = \mathcal{C}_{S'}. \tag{3}$$

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

3 SLOCC equivalence

In this section. we consider the equivalence of stabilizer states under stochastic local operations and classical communication (SLOCC). Remember that two

n-qubit states $|\psi\rangle$ and $|\psi'\rangle$ are SLOCC-equivalent if and only if there exists an operator $A \in GL(2,\mathbb{C})^{\otimes n}$ such that $A|\psi\rangle = |\psi'\rangle$. We recall the following theorem, proven by Verstraete et al.:

Theorem 1 [10] *Any $d_1 \times d_2 \times \ldots \times d_n$ multipartite state can be brought into a normal form by determinant one SLOCC operations. If the initial state has full rank 1-party reduced density operators then the 1-party density operators of its normal form are all maximally mixed, i.e. they are proportional to the identity. Moreover, the normal form is unique up to local unitary operators.*

The proof of theorem 1 is in fact a numerical algorithm which iteratively constructs the normal form of a given initial state. Furthermore, it follows immediately from the details of the algorithm that an initial state which already has maximally mixed 1-party operators, is in normal form. Therefore, two states are SLOCC-equivalent if and only if they have LU-equivalent normal forms and, what is more, two states with maximally mixed 1-party subsystems are SLOCC-equivalent if and only if they are LU-equivalent. Application of this last argument to stabilizer states yields the following theorem:

Theorem 2 *Two stabilizer states are SLOCC-equivalent if and only if they are LU-equivalent.*

Proof: It is sufficient to prove the theorem for fully entangled states, i.e. states which cannot cannot be written as a tensor product $|\xi\rangle|\phi\rangle$ in any way. Let $|\psi\rangle$ be such a fully entangled n-qubit stabilizer state with stabilizer $\mathcal{S}$. It follows from the identity

$$|\psi\rangle\langle\psi| = \frac{1}{2^n}\sum_{M\in\mathcal{S}} M$$

that the 1-qubit reduced density operators ρ_i of $|\psi\rangle$ are either proportional to the identity σ_0 or to an operator of the form $\sigma_0 \pm \sigma_u$, where $u \in \{x, y, z\}$. As $|\psi\rangle$ is fully entangled, the latter case cannot occur, since $\rho_i \sim \sigma_0 \pm \sigma_u$ is then a pure state and $|\psi\rangle$ can be written as a tensor product $\rho_i \otimes \text{Tr}_i\ |\psi\rangle\langle\psi|$, which is impossible. Thus, all the 1-qubit density operators of $|\psi\rangle$ are maximally mixed and the result follows from the discussion below theorem 1. □

4 Local unitary equivalence

The result in theorem 2 shows that we can restrict our attention to LU equivalence of stabilizer states. We investigate this matter in this section. First we introduce a family of LU-invariant functions which separate the orbits of stabilizer states. Secondly, we consider local Clifford equivalence of stabilizer states as an important special case of LU equivalence.

4.1 Invariants

Let $\Psi = |\psi\rangle\langle\psi|$ be a stabilizer state. A local *invariant* is a complex function $F(\Psi)$ which remains invariant under the action of all local unitary transformations, i.e.,

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

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 state. To obtain such a minimal complete set, it is well known [11] that it is sufficient to consider functions F which are polynomials in the entries of Ψ. 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 [12] 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. [13] achieve this goal, using earlier work of Rains [14]. These authors obtain a basis of homogeneous invariants of degree r in two main steps: first *binary trees* on r nodes are considered and to every tree B a permutation $\pi(B) \in S_r$ is associated, where S_r is the symmetric group of order r. Then one constructs LU-invariants of degree r in a one-to-one correspondence with n-tuples of permutations obtained in this way. However, the study of local invariants in ref. [13] is general in the sense that it regards arbitrary n-qubit density operators ρ. Closer inspection of these basic invariants when dealing with stabilizer states is certainly appropriate, given the very specific structure of these states. In ref. [6] we investigate the family of LU-invariants of Grassl et al. for the class of those density operators which are the projection operators describing stabilizer codes, a class of which the stabilizer states form a subset. We obtain a complete translation of the invariants of Grassl et al. into the binary stabilizer framework. In this section we repeat (an adapted version of) this result for the case of stabilizer states.

First we recall the construction of basic LU-invariants presented in ref. [13]: 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

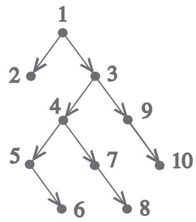

Figure 1: Binary tree on 10 nodes with maximal right paths $(1,3,9,10)$, (2), $(4,7,8)$ and $(5,6)$.

is given in Fig. 1. Denoting by $\mathcal{R}(B)$ the set of all maximal right paths of B, a permutation $\pi(B)$ is associated with the binary tree B. It 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. The set of all permutations obtained in this way is denoted by $\mathcal{P}_r$.

Next, let $\Pi = (\mu, \nu, \xi, \ldots)$ be an n-tuple of permutations $\mu, \nu, \xi, \ldots \in \mathcal{P}_r$. The $2^{nr} \times 2^{nr}$ matrix T_Π is defined as the permutation matrix which acts on $(\mathbb{C}^{2^n})^{\otimes r}$ by permuting 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

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

One obtains an LU-invariant $I_{r,\Pi}$ of degree r as follows:

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

where ρ is an arbitrary n-qubit density operator. One then has the following result:

Theorem 3 [13] *Fix $r \in \mathbb{N}_0$. Then the functions $\{I_{r,\Pi}\}_\Pi$, where Π range over all possible n-tuples of permutations in $\mathcal{P}_r$, form a basis of the linear space of homogeneous LU-invariants of degree r.*

In ref. [6] we obtain a complete translation of the invariants $I_{r,\Pi}$ into the binary stabilizer representation:

Definition 1 *Let B be a binary tree on r nodes with $t := |\mathcal{R}(B)|$ maximal right paths $p_1, \ldots, p_t$, which we suppose to be ordered in such a way that $st(p_1) < st(p_2) < \ldots < st(p_t)$. The columns $(R_B)_j$ of the $r \times t$ binary matrix R_B are defined by:*

$$(R_B)_j = \sum_{i \in p_j} e_i, \tag{4}$$

for every $j \in \{1, \ldots, t\}$, where e_i is the ith canonical base vector in $\mathbb{F}_2^r$.

Theorem 4 [6] *Let $\Psi = |\psi\rangle\langle\psi|$ be a stabilizer state on n qubits with generator matrix S. Let S_i^T $(i = 1, \ldots, n)$ be the $2 \times n$ submatrix of S obtained by selecting the ith and the $(n+i)$th row of S. Fix $r \in \mathbb{N}_0$, let $B_1, \ldots, B_n$ be n binary trees on r nodes and let $\Pi \in \mathcal{P}_r^n$ be the associated n-tuple of permutations. Then*

$$log_2\ I_{r,\Pi}(\Psi) \sim dim_{\mathbb{F}_2}\ ker \begin{bmatrix} R_{B_1}^T \otimes S_1^T \\ R_{B_2}^T \otimes S_2^T \\ \cdots \\ R_{B_n}^T \otimes S_n^T \end{bmatrix} \tag{5}$$

where $\sim$ denotes equality up to an additive constant independent of Ψ.

Theorem 4 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 state 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 stabilizer state [5]. However, the simple form of the result (5) 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 (5) can be computed efficiently via a calculation of the rank over $\mathbb{F}_2$ of the matrix

$$\begin{bmatrix} R_{B_1}^T \otimes S_1^T \\ R_{B_2}^T \otimes S_2^T \\ \cdots \\ R_{B_n}^T \otimes S_n^T \end{bmatrix}. \tag{6}$$

The invariants $I_{r,\Pi}(\Psi)$ can be presented in an alternative way as follows:

Theorem 5 [6] *Let S be a generator matrix of a stabilizer state and let the subblocks S_i^T be defined as in theorem 4. Fix $r \in \mathbb{N}_0$ and let $B_1, \ldots, B_n$ be n binary trees on r vertices. Let $\mathcal{R} = \mathcal{R}(B_1) \cup \ldots \cup \mathcal{R}(B_n)$ 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 (6) is equal to the dimension of the space*

$$\begin{aligned} \{(y^{(1)}, \ldots, y^{(r)}) \in\ &\mathcal{C}_S \times \ldots \times\ \mathcal{C}_S | \\ &supp\ (\sum_{j \in p} y^{(j)}) \subseteq \omega_p,\ for\ every\ p \in \mathcal{R}\} \end{aligned} \tag{7}$$

Here, the support supp(v) of any $v \in \mathbb{F}_2^{2n}$ is the subset of those $i \in \{1, \ldots, n\}$ such that $(v_i, v_{n+i}) \neq (0, 0)$.

This is clearly a more insightful presentation of the invariants $I_{r,\Pi}$ than (5), as (10) relates invariants to dimensions of subspaces of $\mathcal{C}_S \times \ldots \times \mathcal{C}_S$. In order to see the link between theorems 4 and 5, let us consider 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 (4), namely

$$\left[\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right] \quad \text{and} \quad [1\ 1]^T, \tag{8}$$

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

$$R_{B_i}^T \otimes S_i^T = \left[\begin{array}{cc} S_i^T & 0 \\ 0 & S_i^T \end{array}\right]$$

otherwise. Therefore, the null space of the matrix (6) consists of all vectors $(x, x') \in \mathbb{F}_2^{2k}$ such that

$$\begin{array}{ll} S_i(x + x') = 0 & \text{for every } i \in \omega \\ S_j x = S_j x' = 0 & \text{for every } j \in \omega^c, \end{array} \tag{9}$$

where ω^c is the complement of ω in $\{1, \ldots, n\}$. Note that (9) implies that $Sx = Sx'$ and therefore $x = x'$, since S has full rank. Thus, the solutions of (9) 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. Thus, the supports of the y's lie within the set ω and we have shown that

$$\log_2 I_{2,\Pi} \sim \dim \{y \in \mathcal{C}_S |\ \text{supp}(y) \subseteq \omega\}, \tag{10}$$

which corresponds to the result in theorem 5.

4.2 Local Clifford equivalence

We now focus our attention to Local Clifford operations. This subgroup of the local unitary group is of particular interest in the context of the stabilizer formalism, as the closed framework of stabilizer states plus (local) Clifford operations can be described entirely within the binary picture (see section II). First, we recall the well known result that any stabilizer state is LC-equivalent to a graph state, which reduces the study of LC-equivalence of stabilizer states to that of graph states. In the second paragraph, we translate the action of LC-operations on graphs states into transformations of their corresponding graphs and show that essentially one basic graph transformation rule suffices to generate the entire orbit of any graph state under LC. Finally, using this graphical description, we present a polynomial time algorithm which recognizes whether two given graph states are LC-equivalent.

4.2.1 Reduction to graph states

It is well known that any stabilizer state is LC-equivalent to some - generally non-unique - graph state [15]. Therefore, we can restrict our attention to the subclass of graph states when studying the local equivalence of stabilizer states. Note that in general the image of a graph state under a local Clifford operation

$$Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in C_n^l$$

need not again yield another graph state, as this transformation maps

$$\begin{bmatrix} \theta \\ I \end{bmatrix} \to Q \begin{bmatrix} \theta \\ I \end{bmatrix} = \begin{bmatrix} A\theta + B \\ C\theta + D \end{bmatrix}. \tag{11}$$

The image in (11) is the generator matrix of a graph state if and only if (a) the matrix $C\theta + D$ is nonsingular and (b) the matrix $\theta' := (A\theta + B)(C\theta + D)^{-1}$ has zeros on the diagonal. Then

$$Q \begin{bmatrix} \theta \\ I \end{bmatrix} (C\theta + D)^{-1} = \begin{bmatrix} \theta' \\ I \end{bmatrix} =: S'$$

is the generator matrix for a graph state with adjacency matrix θ'. Note that we need not impose the constraint that θ' be symmetric, since this is automatically the case, as S' is the image of a stabilizer generator matrix under an operation in C_n^l and therefore

$$\begin{bmatrix} \theta'^T & I \end{bmatrix} P \begin{bmatrix} \theta' \\ I \end{bmatrix} = 0,$$

which is equivalent to $\theta'^T = \theta'$. These considerations lead us to introduce, for each $Q \in C_n^l$, a domain of definition dom(Q), which is the set consisting of all θ which satisfy the conditions (a) and (b). Seen as a transformation of the space of all graph state adjacency matrices, Q then maps $\theta \in \mathrm{dom}(Q)$ to

$$Q(\theta) := (A\theta + B)(C\theta + D)^{-1}. \tag{12}$$

In this setting, it is of course a natural question to ask how the operations (12) affect the topology of the graph associated with θ. This issue is tackled in the next section.

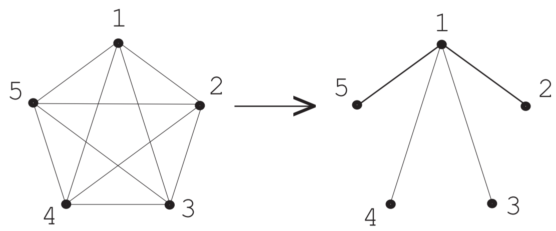

Figure 2: Application of the local graph complementation g_1 to the complete graph on 5 vertices.

4.2.2 Local graph complementation

In this section, we show how the operations (12) can be translated in terms of graph transformation rules. First, we need some additional terminology: let $G = (V, E)$ be a simple graph. Two vertices i and j of a graph $G = (V, E)$ are called adjacent vertices, or neighbors, if $\{i, j\} \in E$. The neighborhood $N(i) \subseteq V$ of a vertex i is the set of all neighbors of i. A graph $G' = (V', E')$ which satisfies $V' \subseteq V$ and $E' \subseteq E$ is a subgraph of G and one writes $G' \subseteq G$. For a subset $A \subseteq V$ of vertices, the induced subgraph $G[A] \subseteq G$ is the graph with vertex set A and edge set $\{\{i, j\} \in E | i, j \in A\}$. If G has an adjacency matrix θ, its complement G^c is the graph with adjacency matrix $\theta + \mathbb{I}$, where $\mathbb{I}$ is the $n \times n$-matrix which has all ones, except for the diagonal entries which are zero. We can now define the following graph transformation:

Definition 2 *Let $G = (V, E)$ be a simple graph. The local complement $g_i(G)$ of G at a vertex $i \in V$ is the simple graph on the same vertex set which is obtained by replacing the subgraph of G induced by the neighborhood of i by its complement. The adjacency matrix $g_i(\theta)$ of $g_i(G)$ is equal to*

$$g_i(\theta) = \theta + \theta_i \theta_i^T + \Lambda, \tag{13}$$

where θ_i is the ith column of θ and Λ is a diagonal matrix such as to yield zeros on the diagonal of $g_i(\theta)$. Addition in (13) is to be performed modulo two.

Example: Consider the 5-vertex graph G whith adjacency matrix $\theta_{ij} = 1$ for all $i \neq j$ and $\theta_{ii} = 0$ for all i (i.e. the complete graph), which is the defining graph for the GHZ state. The application of the elementary local Clifford operation g_1 to this graph is shown in Fig. 2.

We show in ref. [5] that local graph complementations g_i can be realized by performing local Clifford operations on the associated graph state:

Theorem 6 [5] *Let G be a simple graph on n vertices with adjacency matrix θ. Then*

$$g_i(\theta) = Q_i(\theta),$$

where

$$Q_i := \begin{bmatrix} I & diag(\theta_i) \\ \Lambda_i & I \end{bmatrix} \in C_n^l.$$

Here $\mathrm{diag}(\theta_i)$ *is the diagonal matrix which has* θ_{ij} *on the* j*th diagonal entry, for* $j = 1, \ldots, n$*, and* Λ_i *is the matrix which has a 1 on the* i*th diagonal entry and zeros elsewhere.*

Proof: The result can be shown straightforwardly by calculating $Q_i(\theta) = (\theta + \mathrm{diag}(\theta_i))(\Lambda_i\theta + I)^{-1}$ and noting that the matrix $\Lambda_i\theta + I$ is its own inverse for any θ. $\square$

What is more, a subsequent application of local complementations suffices to generate the entire orbit of any graph state under LC. Indeed, one has:

Theorem 7 [5] *Let* G *and* G' *be two simple graphs on the same vertex set with adjacency matrices* θ *and* θ'*, respectively. Then there exists an operation* $Q \in C_n^l$ *such that* $Q(\theta) = \theta'$ *if and only if there exists a finite sequence of local complementations* $g_{i_1}, g_{i_2}, \ldots, g_{i_N}$ *such that* $g_{i_1} g_{i_2} \ldots g_{i_N}(G) = G'$.

This result completely translates the problem of recognizing local Clifford equivalence of graph states in terms of graphs and graph transformations. Note that essentially one basic graph transformation rule suffices to generate the entire orbit of any graph state under LC.

As it turns out, local graph complementation is well known in graph theory (see e.g. [16] and references within). What is more, in ref. [17] a polynomial time algorithm is derived which detects whether two given graphs are related by a sequence of local complementations. This yields for our purposes an efficient algorithm which recognizes LC-equivalence of graph states. We repeat this algorithm in the next paragraph.

4.2.3 Algorithm

Suppose that two particular graph states $|G\rangle$, $|G'\rangle$ with adjacency matrices θ, θ', respectively, and generator matrices

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

respectively, are given and that one wishes to decide wether these states are LC-equivalent. Recall that $|G\rangle$ and $|G'\rangle$ are LC-equivalent if and only if there exists $Q \in C_n^l$ such that $\mathcal{C}_{QS} = \mathcal{C}_{S'}$. This occurs if and only if there exists an invertible $n \times n$ matrix R over $\mathbb{F}_2$ such that

$$QSR = S'. \tag{14}$$

If θ and θ' are fixed, (14) is a matrix equation in the unknowns Q and R. Note that we can get rid of the unknown R, as (14) is equivalent to

$$S^T Q^T P S' = 0. \tag{15}$$

Indeed, (15) expresses that $u^T P v = 0$ for every $u \in \mathcal{C}_{QS}$ and $v \in \mathcal{C}_{S'}$, which implies that $\mathcal{C}_{QS}$ and $\mathcal{C}_{S'}$ are each other's symplectic orthogonal complement. These spaces must therefore be equal, as any n-dimensional binary stabilizer space is its own symplectic dual, and (14) is obtained. More explicitly, (15) is the system of n^2 linear equations

$$\left(\sum_{i=1}^{n} \theta_{ij}\theta'_{ik}c_i\right) + \theta_{jk}a_k + \theta'_{jk}d_j + \delta_{jk}b_j = 0, \tag{16}$$

for all $j,\ k = 1,\ldots,n$, where the $4n$ unknowns a_i, b_i, c_i, d_i must satisfy the quadratic constraints

$$a_i d_i + b_i c_i = 1. \tag{17}$$

The set $\mathcal{V}$ of solutions to the linear equations (16), with disregard of the constraints, is a linear subspace of $\mathbb{F}_2^{4n}$. A basis $B = \{b_1, \ldots, b_d\}$ of $\mathcal{V}$ can be calculated efficiently in $\mathcal{O}(n^4)$ time by standard Gauss elimination over $\mathbb{F}_2$. Then we can search the space $\mathcal{V}$ for a vector which satisfies the constraints (17). As (16) is for large n a highly overdetermined system of equations, the space $\mathcal{V}$ is typically low-dimensional. Therefore, in the majority of cases this method gives a quick response. Nevertheless, in general one cannot exclude that the dimension of $\mathcal{V}$ is of order $\mathcal{O}(n)$ and therefore the overall complexity of this approach is nonpolynomial. However, it was shown in [17] that it is sufficient to enumerate a specified subset $\mathcal{V}' \subseteq \mathcal{V}$ with $|\mathcal{V}'| = \mathcal{O}(n^2)$ in order to find a solution which satisfies the constraints, if such a solution exists. Indeed, the following lemma holds:

Lemma 1 [17] *If dim($\mathcal{V}$) > 4, then the system (16)-(17) of linear equations plus constraints has a solution if and only if the set*

$$\mathcal{V}' := \{b + b' \mid b, b' \in B\} \subseteq \mathcal{V}$$

contains a vector which satisfies the constraints.

The proof of lemma 1 is involved and makes extensive use of local graph complementation. The reader is referred to ref. [17] for more details. Lemma 1 shows that, if a solution to (16)-(17) exists, this solution can be found by enumerating either all $|\mathcal{V}| \leq 16$ elements of $\mathcal{V}$ if $\dim(\mathcal{V}) \leq 4$ or the $\mathcal{O}(n^2)$ elements of $\mathcal{V}'$ if $\dim(\mathcal{V}) > 4$ and checking these vectors against the constraints (17). Hence, a polynomial time algorithm to check the solvability of (16)-(17) is obtained. The overall complexity of the algorithm is $\mathcal{O}(n^4)$. Note that, whenever LC-equivalence occurs, this algorithm provides an explicit local unitary operator in the Clifford group which maps the one state to the other, as a solution $(a_1, b_1, c_1, d_1,\ \ldots,\ a_n, b_n, c_n, d_n)$ to (16)-(17) immediately yields an operator $Q \in C_n^l$. Moreover, the present result immediately yields an efficient algorithm to recognize LC-equivalence of *all* stabilizer states (and not just the subclass of graph states). Indeed, if a particular stabilizer state is given then an LC-equivalent graph state can be found in polynomial time, as the typical existing algorithms used to produce this graph state essentially use pivoting methods, which can be implemented efficiently.

5 Conclusion

In this paper, we have performed an investigation of local equivalence classes of stabilizer states. We showed that two stabilizer states are equivalent under SLOCC if and only only if they are equivalent under LU. This reduces the present study to an investigation of LU equivalence classes. We proceeded by considering a complete, though infinite, family of LU-invariants, as constructed in [13], and we presented a complete translation of these invariants into the binary framework in which stabilizer states are usually described. In this context, an important open question remains to be answered: although the existence of a finite complete subset of this family of invariants is guaranteed, one has not yet been able to pinpoint it (neither in the case of arbitrary states nor in the special case of stabilizer states). Continuing our investigation of LU-equivalence, we focussed our attention to local Clifford operations, as this group is of particular interest both in theoretical investigations as for practical applications. We presented a translation of the action of local Clifford operations on graph states, showing that two graph states are LC-equivalent if and only if their associated graphs are related by a sequence of so-called local complementations. This result completely describes the LC-equivalence class of a graph state in terms of its graph. Finally, this result is the heart of an efficient algorithm which recognizes whether two given stabilizer states are LC-equivalent. We note that as well in this context there is a fundamental open question: it is not clear whether or not it is in fact a restriction at all to consider only LC operations in the problem of recognizing LU-equivalence of stabilizer states; in other words, the following question is naturally raised: are every two LU-equivalent stabilizer states also LC-equivalent?

Acknowledgments

This research is supported by: Research Council KUL: GOA-Mefisto 666, several PhD/postdoc & 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), research communities (ICCoS, ANMMM); AWI: Bil. Int. Collaboration Hungary/Poland; IWT: PhD Grants, Soft4s (softsensors); Belgian Federal Government: DWTC (IUAP IV-02 (1996-2001) and IUAP V-22 (2002-2006), PODO-II (CP/40: TMS and Sustainability); EU: CAGE; ERNSI; Eureka 2063-IMPACT; Eureka 2419-FliTE; Contract Research/agreements: Data4s, Electrabel, Elia, LMS, IPCOS, VIB; Quprodis and Quiprocone.

References

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

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

[3] 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.

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

[5] 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.

[6] M. Van den Nest, J. Dehaene, and B. De Moor. Local invariants of stabilizer codes. quant-ph/0404106.

[7] M. Van den Nest, J. Dehaene, and B. De Moor. An efficient algorithm to recognize local clifford equivalence of graph states. quant-ph/0405023.

[8] R Diestel. *Graph theory.* Springer, Heidelberg, 2000.

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

[10] F. Verstraete, J. Dehaene, and B. De Moor. Normal forms and entanglement measures for multipartite quantum states. *Phys. Rev. A*, 68(012103), 2003.

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

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

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

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

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

[16] A. Bouchet. Recognizing locally equivalent graphs. *Discrete Math.*, 114:75–86, 1993.

[17] A. Bouchet. An efficient algorithm to recognize locally equivalent graphs. *Combinatorica*, 11(4):315 –329, 1991.