Graphical description of the action of local Clifford transformations on graph states

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

(Dated: November 25, 2003)

We translate the action of local Clifford operations on graph states into transformations on their associated graphs - i.e. we provide transformation rules, stated in purely graph theoretical terms, which completely characterize the evolution of graph states under local Clifford operations. As we will show, there is essentially one basic rule, successive application of which generates the orbit of any graph state under local unitary operations within the Clifford group.

PACS numbers: 03.67.-a

I. INTRODUCTION

Stabilizer states and, more particularly, graph states, and (local) unitary operations in the Clifford group have been studied extensively and play an important role in numerous applications in quantum information theory and quantum computing. A stabilizer state is a multi-qubit pure state which is the unique simultaneous eigenvector of a complete set of commuting observables in the Pauli group, the latter consisting 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. The Clifford group consists of all unitary operators which map the Pauli group to itself under conjugation. As the closed framework of stabilizer theory plus the Clifford group turns out to have a relatively simple mathematical description while maintaining a sufficiently rich structure, it has 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]; (a quotient group of) the Clifford group has been used to construct performant mixed-state entanglement distillation protocols [4]; most recently, graph states were considered in the context of multiparticle entanglement: in [5] the entanglement in graph states was quantified and characterized in terms of the Schmidt measure.

The goal of this paper is to translate the action of local Clifford operations on graph states into transformations on their associated graphs - that is, to derive transformation rules, stated in purely graph theoretical terms, which completely characterize the evolution of graph states under local Clifford operations. The main reason for this research is to provide a tool for studying the local unitary (LU) equivalence classes of stabilizer states or, equivalently, of graph states [**?**] - since the quantification of multi-partite pure-state entanglement is far from being understood and a treatise of the subject in its whole is extremely complex, it is appropriate to restrict oneself to a more easily manageable yet nevertheless interesting subclass of physical states, as are the stabilizer states. The ultimate goal of this research is to characterize the LU-equivalence classes of stabilizer states, by finding suitable representatives within each equivalence class and/or constructing a complete and minimal set of local invariants which separate the stabilizer state orbits under the action of local unitaries. We believe that the result in this paper is a first significant step in this direction.

In section IV, we will show that the orbit of any graph state under local unitary operations within the Clifford group is generated by repeated application of essentially one basic graph transformation rule. The main tool for proving this result will be the representation of the stabilizer formalism and the (local) Clifford group in terms of linear algebra over $GF(2)$, where n-qubit stabilizer states are represented as n-dimensional linear subspaces of $\mathbb{Z}_2^{2n}$ which are self-orthogonal with respect to a symplectic inner product [1, 6] and where Clifford operations are the symplectic transformations of $\mathbb{Z}_2^{2n}$ [4, 7].

This paper is organized as follows: in section II, we start by recalling the notions of stabilizer states, graph states and the (local) Clifford group and the translation of these concepts into the binary framework. In section III, we then show (constructively) that each stabilizer state is equivalent to a graph state under local Clifford operations, thereby rederiving a result of Schlingemann [8]. Continuing within the class of graph states, in section IV we introduce our elementary graph theoretical rules which correspond to local Clifford operations and prove that these operations generate the orbit of any graph state under local Clifford operations.

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

II. PRELIMINARIES

A. Stabilizer states, graph states and the (local) Clifford group

Let $\mathcal{G}_n$ denote the Pauli group on n qubits, consisting of all $4 \cdot 4^n$ n-fold tensor products of the form $\alpha\, v_1 \otimes v_2 \otimes \cdots \otimes v_n$, 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

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

The Clifford group $\mathcal{C}_n$ is the normalizer of $\mathcal{G}_n$ in $U(2^n)$, i.e. it is the group of unitary operators U satisfying $U\mathcal{G}_nU^\dagger = \mathcal{G}_n$. We shall be concerned with the local Clifford group $\mathcal{C}_n^l$, which is the subgroup of $\mathcal{C}_n$ consisting of all n-fold tensor products of elements in $\mathcal{C}_1$.

An n-qubit stabilizer state $|\psi\rangle$ is defined as a simultaneous eigenvector with eigenvalue 1 of n commuting and independent [?] 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 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 $M = M_1^{x_1} \ldots M_n^{x_n}$, for some $x_i \in \{0, 1\}$. The so-called graph states [2, 3] constitute an important subclass of the stabilizer states. A graph [9] 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 correspondig 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 there is a one-to-one correspondence between a graph and its adjacency matrix. 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 $|\psi_{\mu_1\mu_2\ldots\mu_n}(G)\rangle$, where $\mu_i \in \{0, 1\}$, is then the stabilizer state defined by the equations

$$(-1)^{\mu_j} K_j\ |\psi_{\mu_1\mu_2\ldots\mu_n}(G)\rangle = |\psi_{\mu_1\mu_2\ldots\mu_n}(G)\rangle.$$

Since one can easily show that the 2^n eigenstates $|\psi_{\mu_1\mu_2\ldots\mu_n}(G)\rangle$ are equal up to local unitaries in the Clifford group, it suffices for our purposes to choose one of them as a representative of all graph states associated with G. Following the literature [5], we denote this representative by $|G\rangle := |\psi_{00\ldots0}(G)\rangle$. Furthermore, if the adjacency matrices of two graphs G and G' differ only in their diagonal elements, the states $|G\rangle$ and $|G'\rangle$ are equal up to a local Clifford operation, which allows for an a-priori reduction of the set of graphs which needs to be considered in the problem of local unitary equivalence. The most natural choice is to consider the class $\Theta \subseteq \mathbb{Z}_2^{n\times n}$ of adjacency matrices which have zeros on the diagonal. These correspond to so-called simple graphs, which have no edges of the form $\{i, i\}$ or, equivalently, none of the points is connected to itself with a line. From this point on, we will only consider graph states which are associated with simple graphs.

B. The binary picture

It is well-known [1, 6, 10] that the stabilizer formalism can be translated into a binary framework, which essentially exploits the homomorphism between $\mathcal{G}_1, \cdot$ and $\mathbb{Z}_2^2, +$ which maps $\sigma_0 = \sigma_{00} \mapsto 00$, $\sigma_x = \sigma_{01} \mapsto 01$, $\sigma_z = \sigma_{10} \mapsto 10$ and $\sigma_y = \sigma_{11} \mapsto 11$. In $\mathbb{Z}_2^2$ addition is to be performed modulo 2. The generalization to n qubits is defined by $\sigma_{u_1v_1} \otimes \cdots \otimes \sigma_{u_nv_n} = \sigma_{(u_1\ldots u_n|v_1\ldots v_n)} \mapsto (u_1 \ldots u_n|v_1 \ldots v_n) \in \mathbb{Z}_2^{2n}$, where $u_i, v_i \in \{0, 1\}$. Thus, an n-fold tensor product of Pauli matrices is represented as a $2n$-dimensional binary vector. Note that with this encoding one loses the information about the overall phases of Pauli operators. For now, we will altogether disregard these phases and we will come back to this issue later in this paper.

In the binary language, two Pauli operators σ_a and σ_b, where $a, b \in \mathbb{Z}_2^{2n}$, commute iff $a^TPb = 0$, where the $2n \times 2n$-matrix $P = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$ defines a symplectic inner product on the space $\mathbb{Z}_2^{2n}$. The stabilizer of a stabilizer state then corresponds to an n-dimensional linear subspace of $\mathbb{Z}_2^{2n}$ which is its own orthogonal complement with respect to this symplectic inner product. 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 satisfies $S^TPS = 0$ from the symplectic self-orthogonality property. The entire stabilizer subspace consists of all linear combinations of the columns of S, i.e. of all elements Sx, where $x \in \mathbb{Z}_2^n$. The matrix S, which is referred to as a generator matrix for the stabilizer, is of course non-unique. A change of generators amounts to multiplying S to the right with an invertible $n \times n$-matrix, which performs a basis change in the binary subspace. Note that a graph state which corresponds to a graph with adjacency matrix θ, has a generator matrix $S = \begin{bmatrix} \theta \\ I \end{bmatrix}$. Finally, it can be shown [4, 7] that, as we disregard overall phases, Clifford operations are just the symplectic transformations of $\mathbb{Z}_2^{2n}$, which preserve the symplectic inner product, i.e. they are the $2n \times 2n$-matrices Q which satisfy $Q^T P Q = P$. As local Clifford operations act on each qubit separately, they have the additional block structure $Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$, where the $n \times n$-blocks A, B, C, D are diagonal. In this case, the symplectic property of Q is equivalent to stating that each submatrix $\begin{bmatrix} A_{ii} & B_{ii} \\ C_{ii} & D_{ii} \end{bmatrix}$, which acts on the ith qubit, is invertible. The group of all such Q will be denoted by C^l.

Thus, in the binary stabilizer framework, two stabilizer states $|\psi\rangle$ and $|\psi'\rangle$ with generator matrices S and S' are equivalent under the local Clifford group iff [**?**] there is a $Q \in C^l$ and an invertible $R \in \mathbb{Z}_2^{n\times n}$ such that

$$QSR = S'. \tag{1}$$

Note that the physical operation which transforms $|\psi\rangle$ into $|\psi'\rangle$ is entirely determined by Q; the right matrix multiplication with R is just a basis change within the stabilizer of the target state.

III. REDUCTION TO GRAPH STATES

In this section we show that, under the transformations $S \to QSR$, each stabilizer generator matrix S can be brought into a (nonunique) standard form which corresponds to the generator matrix of a graph state.

Theorem 1: *Each stabilizer state is equivalent to a graph state under local Clifford operations.*

Proof: Consider an arbitrary stabilizer with generator matrix $S = \begin{bmatrix} Z \\ X \end{bmatrix}$. The result is obtained by proving the existence of a local Clifford operation $Q \in C^l$ such that $QS = \begin{bmatrix} Z' \\ X' \end{bmatrix}$ has an invertible lower block X'. Then

$$S' := QSX'^{-1} = \begin{bmatrix} Z'X'^{-1} \\ I \end{bmatrix},$$

where $Z'X'^{-1}$ is symmetric from the property $S'^T P S' = 0$; furthermore, the diagonal entries of $Z'X'^{-1}$ can be put to zero by additionally applying the operation $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ to the appropriate qubits, since this operation flips the ith diagonal entry of $Z'X'^{-1}$ when applied on the ith qubit. Eventually we end up with a graph state generator matrix of the desired standard form.

We now construct a local Clifford operation Q that yields an invertible lower block X'. We start by performing a basis change in the original stabilizer in order to bring S in the form

$$S \to \begin{bmatrix} R_z & S_z \\ R_x & 0 \end{bmatrix},$$

such that R_x is a full rank $n \times k$-matrix, where $k = \operatorname{rank} X$; the blocks R_z, S_z have dimensions $n \times k$, resp. $n \times (n-k)$. The symplectic self-orthogonality of the stabilizer implies that $S_z^T R_x = 0$. Furthermore, since S_z has full rank, it follows that the column space of S_z and the column space of R_x are each other's orthogonal complement.

Now, as R_x has rank k, it has an invertible $k \times k$-submatrix. Without loss of generality, we assume that the matrix consisting of the first k rows of R_x is invertible, i.e. $R_x = \begin{bmatrix} R_x^1 \\ R_x^2 \end{bmatrix}$, where the upper $k \times k$-block R_x^1 is invertible and R_x^2 has dimensions $(n-k) \times k$. Partitioning S_z similarly in a $k \times (n-k)$-block S_z^1 and a $(n-k) \times (n-k)$-block S_z^2 , i.e. $S_z = \begin{bmatrix} S_z^1 \\ S_z^2 \end{bmatrix}$, the property $S_z^T R_x = 0$ then implies that S_z^2 is also invertible: for, suppose that there exist $x \in \mathbb{Z}_2^{n-k}$ such that $(S_z^2)^T x = 0$; then the n-dimensional vector $v := (0, \ldots, 0, x)$ satisfies $S_z^T v = 0$ and therefore $v = R_x y$ for some $y \in \mathbb{Z}_2^k$. This last equation reads

$$\begin{bmatrix} 0 \\ x \end{bmatrix} = \begin{bmatrix} R_x^1 \\ R_x^2 \end{bmatrix} y = \begin{bmatrix} R_x^1 y \\ R_x^2 y \end{bmatrix}.$$

Since R_x^1 is by construction invertible, $R_x^1 y = 0$ implies that $y = 0$, yielding $x = R_x^2 y = 0$. This proves the invertibility of S_z^2.

In a final step, we perform a Hadamard transformation $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ on the qubits $k+1, \ldots, n$. It is now easy to verify that this operation indeed yields an invertible lower $n \times n$-block in the new generator matrix, thereby proving the result. □

This proposition is a special case of a result by Schlingemann [8], who showed, in a more general context of d-level systems rather then qubits, that each stabilizer code is equivalent to a graph code.

Remark: *overall phases* - Theorem 1 implies that our disregard of the overall phases of the stabilizer elements is justified. Indeed, this result states that each stabilizer state is equivalent to some graph state $|\psi_{\mu_1\mu_2\ldots\mu_n}(G)\rangle$, for some μ_i. As such a state is equivalent to the state $|G\rangle$, there is no need to keep track of the phases.

Theorem 1 shows that we can restrict our attention to 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 $Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ need not again yield another graph state, as this transformation maps

$$\begin{bmatrix} \theta \\ I \end{bmatrix} \to Q \begin{bmatrix} \theta \\ I \end{bmatrix} = \begin{bmatrix} A\theta + B \\ C\theta + D \end{bmatrix} \qquad (2)$$

for $\theta \in \Theta$. The image in (2) 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 zero diagonal. Then

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

is the generator matrix for a graph state with adjacency matrix $\theta' \in \Theta$. Note that we need not impose the constraint that θ' be symmetric, since this is automatically the case, as $\begin{bmatrix} \theta' \\ I \end{bmatrix}$ is the image of a stabilizer generator matrix under a Clifford operation, and thus

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

These considerations lead us to introduce, for each $Q \in C^l$, a domain of definition dom(Q), which is the set consisting of all $\theta \in \Theta$ which satisfy the conditions (a) and (b). Seen as a transformation of the space Θ of all graph state adjacency matrices, Q then maps $\theta \in \text{dom}(Q)$ to

$$Q(\theta) := (A\theta + B)(C\theta + D)^{-1}. \qquad (3)$$

In this setting, it is of course a natural question to ask how the operations (3) affect the topology of the graph associated with θ. We tackle this problem in the next section.

To conclude this section we state and prove a lemma which we will need later on in the paper.

Lemma 1: *Let $\theta \in \Theta$ and C, D be diagonal matrices s.t. $C\theta + D$ is invertible. Then there exists a unique $Q := \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in C^l$, where A, B are diagonal matrices, such that $\theta \in$ dom(Q).*

Proof: Note that, since $C\theta + D$ is invertible, we only need to look for a Q s.t. $Q(\theta)$ has zero diagonal in order for θ to be in the domain of Q. First we will prove the uniqueness of A and B: suppose there exist two pairs of diagonal matrices A, B and A', B' s.t.

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

and $\theta \in$ dom(Q), $\theta \in$ dom(Q'). Denoting $\theta_z := A\theta + B$, $\theta_z' := A'\theta + B'$ and $\theta_x := C\theta + D$, we have $Q(\theta) = \theta_z \theta_x^{-1}$ and $Q'(\theta) = \theta_z' \theta_x^{-1}$. Now, denoting by $z_i^T, \bar{z}_i^T, x_i^T$ the rows of resp. $\theta_z, \theta_z', \theta_x$, the crucial observation is that either $\bar{z}_i^T = z_i^T$ or $\bar{z}_i^T = z_i^T + x_i^T$ for all $i = 1, \ldots, n$, which is a direct consequence of the fact that Q, Q' have the same lower blocks C, D. Now, if the latter of the two possibilities is the case for some i_0, the i_0th diagonal entries of $Q(\theta)$ and $Q'(\theta)$ must be different, since $Q'(\theta)_{i_0 i_0} = \bar{z}_{i_0}^T (\theta_x^{-1})_{i_0} = z_{i_0}^T (\theta_x^{-1})_{i_0} + x_{i_0}^T (\theta_x^{-1})_{i_0} = Q(\theta)_{i_0 i_0} + 1$, with $(\theta_x^{-1})_{i_0}$ the i_0th column of θ_x^{-1}. As both $Q(\theta)$ and $Q'(\theta)$ have zero diagonal, this yields a contradiction and we have proven the uniqueness of A and B. To prove existence, note that for every i, there are exactly two couples (a_i, b_i) s.t. $\begin{bmatrix} a_i & b_i \\ C_{ii} & D_{ii} \end{bmatrix}$ is invertible. It follows from the above argument that we can always tune (a_i, b_i) such that $(A\theta + B)(C\theta + D)^{-1}$ has zero diagonal, where we take $A_{ii} = a_i$ and $B_{ii} = b_i$ for $i = 1, \ldots, n$. Since each 2×2-matrix $\begin{bmatrix} A_{ii} & B_{ii} \\ C_{ii} & D_{ii} \end{bmatrix}$ is invertible, the matrix $Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ is an element of C^l, which proves the result. $\square$

IV. LOCAL CLIFFORD OPERATIONS AS GRAPH TRANSFORMATIONS

In this section, we investigate how the transformations (3) can be translated as graph transformations. First we need some graph theoretical notions: 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 neigbors 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.

Definition 1: For each $i = 1, \ldots, n$, the graph transformation g_i sends an n-vertex graph G to the graph $g_i(G)$, which is obtained by replacing the subgraph $G[N(i)]$, i.e. the induced subgraph of the neigborhood of the ith vertex of G, by its complement. In terms of adjacency matrices, g_i maps $\theta \in \Theta$ to

$$g_i(\theta) = \theta + \theta \Lambda_i \theta + \Lambda,$$

where Λ_i has a 1 on the ith diagonal entry and zeros elsewhere and Λ is a diagonal matrix such as to yield zeros on the diagonal of $g_i(\theta)$.

The transformations g_i are obviously their own inverses. Note that in general different g_i and g_j do not commute; however, if $\theta \in \Theta$ has $\theta_{ij} = 0$, it holds that $g_i g_j(\theta) = g_j g_i(\theta)$, as one can easily verify.

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.

FIG. 1: Application of the graph operation g_1 to the GHZ graph.

1.

The operations g_i can indeed be realized as local Clifford operations (3). This is stated in theorem 2 and was found independently by Hein *et al.* [5].

Theorem 2: *Let g_i be defined as before and $\theta \in \Theta$. Then*

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

where

$$Q_i = \begin{bmatrix} I & diag(\theta_i) \\ \Lambda_i & I \end{bmatrix} \in C^l,$$

where $diag(\theta_i)$ is the diagonal matrix which has θ_{ij} on the jth diagonal entry, for $j = 1, \dots, n$.

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

The remainder of this section is dedicated to proving that the operations g_i in fact generate the entire orbit of a graph state under local Clifford operations, that is to say, two graph states $|G\rangle, |G'\rangle$ are equivalent under the local Clifford group iff there exists a finite sequence $g_{i_1}, \dots, g_{i_N}$ such that $g_{i_N} \dots g_{i_1}(G) = G'$. This result completely translates the action of local Clifford operations on graph states into a corresponding action on their graphs. In order to prove the result, we need the following lemma.

Lemma 2: *Define the matrix class $\mathbb{T} \subseteq \mathbb{Z}_2^{n\times n}$ by*

$$\mathbb{T} = \quad \{C\theta + D|\ \theta \in \Theta \text{ and } C, D \text{ are diagonal and } C\theta + D \text{ is invertible}\}$$

and consider an element $R \in \mathbb{T}$. Choose θ, C, D such that $R = C\theta + D$. Define the transformation f_i of $\mathbb{T}$ by $f_i(X) = X(\Lambda_i X + X_{ii}\Lambda_i + I)$, for $X \in \mathbb{T}$, and denote $f_{jk}(\cdot) := f_j f_k f_j(\cdot)$. Then (i) there exists a finite sequence of f_i's and f_{jk}'s such that

$$f_{j_M k_M} \dots f_{j_1 k_1} f_{i_N} \dots f_{i_1}(R) = I, \qquad (4)$$

where all the indices in the sequence are different; (ii) there exists a unique $Q_0 = \begin{bmatrix} A_0 & B_0 \\ C & D \end{bmatrix} \in C^l$, such that $\theta \in \ dom(Q_0)$ and

$$g_{j_M k_M} \dots g_{j_1 k_1} g_{i_N} \dots g_{i_1}(\theta) = Q_0(\theta),$$

where $g_{jk}(\cdot) := g_j g_k g_j(\cdot)$.

Proof: First, straightforward calculation shows that f_i maps the class of matrices of the form $C\theta + D$ to itself. Furthermore, for each $X \in \mathbb{T}$ the matrix $\Lambda_i X + X_{ii}\Lambda_i + I$ is invertible, which implies that f_i maps invertible matrices to invertible matrices. Therefore each f_i is indeed a transformation of $\mathbb{T}$. Now, statement (i) is proven by applying the algorithm below, where the idea is to successively make each ith row of R equal to the ith canonical basis vector $e_i^T = [0 \dots 0\ 1\ 0 \dots 0]$, by applying the correct f_j's in each step. The image of R throughout the consecutive steps will be denoted by the same symbol $\bar{R} = (r_{ij})$. Now, the algorithm consists of repeatedly performing one of the two following sequences of operations on $\bar{R}$:

Case 1: If $\bar{R}$ has a diagonal entry $r_{i_0 i_0} = 1$ (and the i_0th row of $\bar{R}$ is not yet equal to the basis vector $e_{i_0}^T$), apply f_{i_0}. It is easy to verify that, in this situation, f_{i_0} transforms the i_0th row of $\bar{R}$ into the basis vector $e_{i_0}^T$.

Case 2: If the conditions for case 1 are not fulfilled, apply the following sequence of three operations: firstly, fix a j_0 such that $r_{j_0 j_0} = 0$ and apply f_{j_0}. It can easily be seen that then $\text{diag}(\bar{R}) \to \text{diag}(\bar{R}) + \bar{R}_{j_0}$, where $\bar{R}_{j_0}$ is the j_0th column of $\bar{R}$ and $\text{diag}(\bar{R})$ is the diagonal of $\bar{R}$. Since $\bar{R}$ is invertible, $\bar{R}_{j_0}$ has some nonzero element, say on the k_0th position $r_{k_0 j_0} = 1$. Therefore, the application of f_{j_0} has put a 1 on the k_0th diagonal entry of the resulting $\bar{R}$. Now we apply f_{k_0}, turning the k_0th row into $e_{k_0}^T$ as in case 1. Furthermore, this second operation has put $r_{j_0 k_0}$ on the j_0th diagonal entry and, from the symmetry of $\bar{R}$, it holds that $r_{j_0 k_0} = r_{k_0 j_0} = 1$. Therefore, by again applying f_{j_0}, we obtain an $e_{j_0}^T$ on the j_0th row of the resulting $\bar{R}$. Finally, we note that after performing this sequence of operations, we end up with an $\bar{R}$ which will again satisfy the conditions for case 2.

Repetition of these elementary steps will eventually yield the identity matrix, which concludes the proof of statement (i).

Statement (ii) is proven by induction on the length of the sequence of f_i's and f_{jk}'s. As it turns out, the easiest way to do this is to consider the f_i's and f_{jk}'s as two different types of elementary blocks in the sequence (4). The proof will therefore consist of two parts A and B, part A dealing with the f_i's and part B with the f_{jk}'s.

Part A: in the basis step of the induction we have $f_i(R) = I$, where $R \in \mathbb{T}$. Any such R satisfies $R =$

$\Lambda_i R + R_{ii}\Lambda_i + I$ and therefore must be of the form

$$R = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ x_1 & & x_{i-1} & 1 & x_{i+1} & & x_n \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix} \leftarrow i$$

for some x_j. Then any θ, C, D which satisfy $R = C\theta + D$ must satisfy $\theta_{ij} = x_j$ and $D = I$; moreover, if $C_{jj} = 1$ for $j \neq i$ then the jth row of θ must be equal to zero and if $C_{ii} = 0$ the ith row of θ must be to zero. It is now easy to see that $g_i(\theta) = Q(\theta)$, with $Q = \begin{bmatrix} \cdot & \cdot \\ C & D \end{bmatrix}$.

In the induction step, we suppose that the statement holds for all sequences $f_{i_1}, \ldots, f_{i_N}$ of fixed length N and prove that this implies that the statement is true for sequences of length $N+1$. We start from the given that

$$f_{i_N} \ldots f_{i_1} f_i(R) = I$$

for some $f_i, f_{i_1}, \ldots, f_{i_N}$ and $R \in \mathbb{T}$ and we choose θ, C, D such that $C\theta + D = R$. Note that it follows from case 1 in the algorithm in part (i) of the lemma that we may take $C_{ii} = 1 = D_{ii}$, as a single f_i (as opposed to an f_{ij}) is only applied when $R_{ii} = 1$. Furthermore, we will denote by ω the set of all $j \in \{1, \ldots, n\}$ such that $C_{jj} = 1$. As R is invertible, this implies that $D_{kk} = 1$ for $k \in \omega^c$. Now, denoting $R' := f_i(R)$, we have $f_{i_N} \ldots f_{i_1}(R') = I$, which allows us to use the result for length N: for any θ', C', D' that satisfy $C'\theta' + D' = R'$ there exists a $Q' \in C^l$ which has C', D' as its lower blocks such that $\theta' \in \operatorname{dom}(Q')$ and

$$g_{i_N} \ldots g_{i_1}(\theta') = Q'(\theta'). \tag{5}$$

We make the following choices for θ', C', D':

$$\begin{aligned} \theta' &= g_i(\theta) \\ C' &= C + \Lambda_i \\ D' &= D + \operatorname{diag}(\theta_i)_\omega \end{aligned}$$

where $\operatorname{diag}(\theta_i)_\omega$ is the diagonal matrix which has θ_{ij} on the jth diagonal entry if $j \in \omega$ and zeros elsewhere. This choice for θ', C', D' indeed yields $C'\theta' + D' = R'$; we will however omit the calculation since it is straightforward. Now, using the definition of θ' and Theorem 2, equation (5) becomes

$$g_{i_N} \ldots g_{i_1} g_i(\theta) = (Q'Q_i)(\theta). \tag{6}$$

It is now again straightforward to show that $Q := Q'Q_i$ has C and D as its lower blocks. Uniqueness follows from lemma 1. This proves the induction step, thereby concluding the proof of part A.

Part B: The proof of this part is analogous to part A, though a bit more involved. The basis step now reads $f_{jk}(R) = I$. Now case 2 in the algorithm in part (i) of the lemma implies that $R_{jj} = 0 = R_{kk}$ and $R_{jk} = 1$, as only if this is the case, f_{jk} is applied in the algorithm. For simplicity, but without losing generality, we take $i = 1, j = 2$. Then R must be of the form

$$R = \left[\begin{array}{cc|c} 0 & 1 & \theta_1^T \\ 1 & 0 & \theta_2^T \\ \hline 0 & 0 & I \end{array}\right],$$

where the θ_i are $(n-2)$-dimensional column vectors. Choosing θ, C, D s.t. $R = C\theta + D$, the matrix θ must satisfy

$$\theta = \left[\begin{array}{cc|c} 0 & 1 & \theta_1^T \\ 1 & 0 & \theta_2^T \\ \hline \theta_1 & \theta_2 & \phi \end{array}\right],$$

where ϕ is a symmetric $(n-2) \times (n-2)$-matrix with zero diagonal; furthermore $D_{11} = 0 = D_{22}$, $D_{jj} = 1$, $C_{11} = 1 = C_{22}$ and if $C_{j+2,j+2} = 1$ then $\theta_{1j} = \theta_{2j} = \phi_{kj} = 0$, for $j, k = 1, \ldots, n-2$. We will give the proof for $C_{j+2,j+2} = 0$, the other cases are similar. Thus, we have to show that there exists a $Q_0 \in C^l$ with lower blocks C, D s.t. $g_{12}(\theta) = Q_0(\theta)$. To prove this, we use theorem 2, yielding

$$Q_0 = \begin{bmatrix} \cdot & \cdot \\ \Lambda_1 & I \end{bmatrix} \begin{bmatrix} I & \operatorname{diag}(g_1(\theta)_2) \\ \Lambda_2 & I \end{bmatrix} \begin{bmatrix} I & \operatorname{diag}(\theta_1) \\ \Lambda_1 & I \end{bmatrix},$$

where $g_1(\theta)_2 = (1, 0, \theta_{13}+\theta_{23}, \ldots, \theta_{1n}+\theta_{2n})$ is the second column of $g_1(\theta)$. A simple calculation reveals that

$$Q_0 = \begin{bmatrix} \cdot & \cdot \\ \Lambda_1 + \Lambda_2 & I + \Lambda_1 + \Lambda_2 \end{bmatrix} = \begin{bmatrix} \cdot & \cdot \\ C & D \end{bmatrix},$$

which proves the basis of the induction.

In the induction step, we again follow an analogous reasoning to part A: we suppose that the statement is true for sequences $f_{j_1k_1}, \ldots, f_{j_Nk_N}$ of length N and prove that this implies the statement for length $N+1$. Our starting point is now

$$f_{j_Nk_N} \ldots f_{j_1k_1} f_{jk}(R) = I$$

for some $f_{jk}, f_{j_1k_1}, \ldots, f_{j_Nk_N}$ and $R \in \mathbb{T}$. Note that again we have $R_{jj} = 0 = R_{kk}$ and $R_{jk} = 1$ as in the basis step. As from this point on the strategy is identical as in part A and all calculations are straightforward, we will only give a sketch: first we denote $R' = f_{jk}(R)$; for θ, C, D

s.t. $R = C\theta + D$, we define

$$\begin{aligned} \theta' &= g_{jk}(\theta) \\ C' &= C + \Lambda_j + \Lambda_k \\ D' &= D + \Lambda_j + \Lambda_k \end{aligned}$$

It then straightforward to show that $R' = C'\theta' + D'$. The induction yields a $Q' \in C^l$ with lower blocks C', D' such that

$$g_{j_N k_N} \cdots g_{j_1 k_1}(\theta') = Q'(\theta').$$

Using theorem 2, we calculate Q_{jk} s.t. $g_{jk}(\theta) = Q_{jk}(\theta)$. Then

$$g_{j_N k_N} \cdots g_{j_1 k_1} g_{jk}(\theta) = (Q' Q_{jk})(\theta)$$

and a last calculation shows that $Q_0 := Q' Q_{jk}$ has lower blocks C and D. Uniqueness again follows from lemma 1. This proves part B of the lemma. □

The main result of this paper is now an immediate corollary of lemmas 1 and 2:

Theorem 3: *Let $\theta \in \Theta$. Then the operations $g_1, \ldots, g_n$ generate the orbit of θ under the action (3) of the local Clifford group C^l.*

Proof: Let $Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in C^l$ such that $\theta \in \text{dom}(Q)$. Now, as $C\theta + D$ is an invertible element of $\mathbb{T}$, lemma 2(ii) can be applied, yielding a unique $Q_0 = \begin{bmatrix} A_0 & B_0 \\ C & D \end{bmatrix} \in C^l$ and sequence of g_i's and g_{jk}'s such that $\theta \in \text{dom}(Q_0)$ and

$$g_{j_M k_M} \cdots g_{j_1 k_1} g_{i_N} \cdots g_{i_1}(\theta) = Q_0(\theta),$$

As Q and Q_0 have the same lower blocks C and D and θ is in both of their domains, it follows from lemma 1 that $Q_0 = Q$ and the result follows. □

V. DISCUSSION

The result in Theorem 3 of course facilitates generating the equivalence class of a given graph state under local Clifford operations, as one only needs to successively apply the rule to an initial graph. Note that the lemma 2 implies that one only needs to consider sequences $g_{j_M k_M} \cdots g_{j_1 k_1} g_{i_N} \cdots g_{i_1}$ of limited length. Furthermore, the translation of the operations (3) into sequences of elementary graph operations gets rid of annoying technical domain questions. It is important to notice that we have *not* proven that each $Q \in C^l$ corresponds directly to a sequence of g_i's, since, in theorem 3, the decomposition into g_i's depends both on Q as well as θ.

In a final note, we wish to point out that testing whether two stabilizer states with generator matrices S, S' are equivalent under the local Clifford group is an easily implementable algorithm when one uses the binary framework. Indeed, one has equivalence iff there exists a $Q \in C^l$ s.t.

$$S^T Q^T P S' = 0, \tag{7}$$

as this expression states that the stabilizer subspaces generated by the matrices S' and QS are orthogonal to each other with respect to the symplectic inner product. Since any stabilizer subspace is its own symplectic orthogonal complement, the spaces generated by S' and QS must be equal, which implies the existence of an invertible R s.t. $S' = QSR$. Equation (7) is a system of n^2 linear equations in the $4n$ entries of $Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$, with n additional quadratic constraints $A_{ii}D_{ii} + B_{ii}C_{ii} = 1$ which state that $Q \in C^l$; these equations can be solved numerically by first solving the linear equations and disregarding the constraints and then searching the solution space for a Q which satisfies the constraints. Although we cannot exclude that the worst case number of operations is exponential in the number of qubits, in the majority of cases this algorithm gives a quick response, as for large n the system of equations is highly overdetermined and therefore generically has a small space of solutions. Note that, when equivalence occurs, the algorithm provides an explicit Q wich performs the transformation.

VI. CONCLUSION

In this paper, we have translated the action of local unitary operations within the Clifford group on graph states into transformations of their associated graphs. We have shown that there is essentially one elementary graph transformation rule, successive application of which generates the orbit of any graph state under the action of local Clifford operations. This result is a first step towards characterizing the LU-equivalence classes of stabilizer states.

Acknowledgments

M. Van den Nest thanks H. Briegel for inviting him to the Ludwig-Maximilians-Universität in Munich for collaboration and acknowledges interesting discussions with M. Hein and H. Briegel. 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; M. Van den Nest acknowlegdes support by the European Science Foundation (ESF).

[1] D. Gottesman, Ph.D. thesis, Caltech (1997), quant-ph/9705052.
[2] W. Dür, H. Aschauer, and H. Briegel, quant-ph/0303087.
[3] R. Raussendorf, D. Browne, and H. Briegel, quant-ph/0301052.
[4] J. Dehaene, M. Van den Nest, and B. De Moor, Phys. Rev. A **67** (2003).
[5] M. Hein, J. Eisert, and H. Briegel, quant-ph/0307130.
[6] A. Calderbank, E. Rains, P. Shor, and N. Sloane, Phys. Rev. Letters pp. 405–408 (1997).
[7] J. Dehaene and B. De Moor, quant-ph/0304125.
[8] D. Schlingemann, quant-ph/0111080.
[9] R. Diestel, *Graph theory* (Springer, Heidelberg, 2000).
[10] I. Chuang and M. Nielsen, *Quantum computation and quantum information* (Cambridge University press, 2000).
[] We will show in section III that each stabilizer state is equivalent to a graph state under the local Clifford group.
[] This means that no product of the form $M_1^{x_1}\dots M_n^{x_n}$, where $x_i \in \{0,1\}$, yields the identity except when all x_i are equal to zero.
[] Here we have used the fact that $|\psi\rangle$ and $|\psi'\rangle$ are equivalent under the local Clifford group iff they have equivalent stablizers $\mathcal{S}$, $\mathcal{S}'$, i.e. iff there exists a local Clifford operation U s.t. $U\mathcal{S}U^\dagger = \mathcal{S}'$.