All types of local equivalence of stabilizer states coincide

Maarten Van den Nest,[a] David Gross,[b,c] Jeroen Dehaene,[a] Bart De Moor[a]
[a] *ESAT-SCD, Katholieke Universiteit Leuven, B-3001 Leuven, Belgium*
[b] *Blackett Laboratory, Imperial College London, London SW7 2BW, UK*
[c] *Institute of Physics, University of Potsdam, D-14469 Potsdam, Germany*
(Dated: December 5, 2005)

Stabilizer states are highly entangled multi-party quantum states that are of interest in several important applications in quantum information theory, such as quantum error-correction and measurement-based quantum computation. We prove that two stabilizer states are related by a local unitary (LU) operation if and only if they are related by a local Clifford (LC) operation, thereby proving a conjecture that has been around for several years. Together with a previous result, this shows that the notions of SLOCC, LU and LC equivalence of stabilizer states coincide.

I. INTRODUCTION

Stabilizer states are special instances of pure states of multi-qubit quantum systems that are of interest in a number of domains in quantum information theory and quantum computation. Stabilizer states are defined in terms of the stabilizer formalism, which is a general framework originally designed in the 1990s to construct broad classes of quantum error-correcting codes – the *stabilizer codes* [1]. Next to their role in quantum error–correction, in recent years stabilizer states have been considered in a number of interesting applications, where the measurement–based model of quantum computation known as the *one–way quantum computer* is certainly among the most prominent [2, 3].

In a more exact definition, a stabilizer state is a pure n-qubit quantum state which is the simultaneous fixed point of a maximal set of commuting Pauli operators, where the latter are $n-$fold tensor products of the Pauli matrices and the identity (with an additional overall phase factor). It is well known that (many) stabilizer states have a high degree of genuine multi-party entanglement, and that this entanglement is one of the key ingredients responsible for the success with which stabilizer states are used in their applications, and therefore a detailed study of the entanglement properties of stabilizer states is called for. In the recent past a number of authors have studied this topic with considerable success [4–10], and also the present authors have investigated this subject [11–15].

When considering the nonlocal properties of stabilizer states, a natural subject is a study of the action of local unitary (LU) operations on stabilizer states and a classification of stabilizer states under LU equivalence; here, two stabilizer states are called LU equivalent if they are related by an LU transformation. In this context of local equivalence, an important role is played by the local Clifford (LC) operations, which are defined to be those LU operations mapping the set of stabilizer states to itself. Because of the close connection between stabilizer states and local Clifford operations, the action of these operations on stabilizer states can be described efficiently and in a transparent manner, allowing for a thorough understanding of this restricted problem. What is more, in this context the natural question is raised whether this restriction of local equivalence to LC operations is in fact a restriction at all. For several years it remained unclear whether there exist examples of LU equivalent stabilizer states that cannot be related by an LC operation; this is the content of the 28th open problem in quantum information theory on R. Werner's webpage, where the above problem was posted by D. Schlingemann [16]. Recently, the present authors obtained a partial result in this context [14], although a complete resolution of the issue was not achieved. In the present paper we resolve this problem to its full extent, as the following result will be proven.

Theorem 1 *Two stabilizer states are LU equivalent if and only if they are LC equivalent.*

This result has several interesting implications. First, it was shown in earlier work [15] of the present authors that every two SLOCC equivalent stabilizer states are also LU equivalent, where SLOCC is short for *stochastic local operations and classical communication*. Together with the present result, this shows that the three notions of SLOCC, LU and LC equivalence coincide for stabilizer states, and therefore there is in fact only one common notion of local equivalence. Second, in Ref. [12] we have presented an algorithm to recognize whether two stabilizer states are LC equivalent. This algorithm is efficient in that it has polynomial time complexity in the number of qubits. With the present result, this algorithm can be used to test any of the three local equivalences. A third implication is situated in the context of graph states. It is well known that every stabilizer state is LC equivalent to some graph state, such that in the study of local equivalence and multi–partite entanglement of stabilizer states it is sufficient to consider only graph states. In Ref. [11] we studied the effect of LC operations on graph states on the underlying graphs, and showed that the action of LC operations on graph states can be translated in terms of a single graph transformation rule called *local complementation*. The present result shows that this local complementation rule in fact embodies to a full extent the action of all local operations on graph states.

This paper is organized as follows. In section II we state the basic definitions concerning the stabilizer formalism, LU and LC equivalence. In section III we give a short outline of the proof of theorem 1, which consists of two main parts; these two parts are presented in sections IV and V, respectively.

II. BASIC DEFINITIONS

In this section we fix some notations and state some basic definitions.

The $2^n \times 2^n$ identity matrix is denoted by I_n, for every $n \in \mathbb{N}_0$. The n-qubit Hilbert space is denoted by $\mathcal{H}_n \cong \mathbb{C}^{2^n}$.

The Pauli group $\mathcal{G}_1$ on one qubit is the multiplicative subgroup of $U(2)$ generated by the Pauli matrices

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \; Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (1)$$

The Pauli group $\mathcal{G}_n$ on n qubits is the $n-$fold tensor product of $\mathcal{G}_1$ with itself. For an arbitrary operator $g \in \mathcal{G}_n$, we let $g_1, \ldots, g_n \in \{I, X, Y, Z\}$ denote the unique Pauli operators such that $g \sim g_1 \otimes \cdots \otimes g_n$ (where $\sim$ denotes equality up to a global phase factor). The *support* of g is the set

$$\mathrm{supp}(g) = \{i \in \{1, \ldots, n\} \mid g_i \neq I_1\}. \quad (2)$$

The element g is said to have *full support* if $\mathrm{supp}(g) = \{1, \ldots, n\}$.

A *stabilizer* $\mathcal{S}$ on n qubits is an Abelian subgroup of $\mathcal{G}_n$ that does not contain $-I$. The cardinality $|\mathcal{S}|$ of the stabilizer $\mathcal{S}$ is always a power of two not greater than 2^n. The *stabilizer code* associated to a stabilizer $\mathcal{S}$ is the subspace $V_{\mathcal{S}} \subseteq \mathcal{H}_n$ consisting of all simultaneous fixed points of the elements of $\mathcal{S}$, i.e.,

$$V_{\mathcal{S}} := \{|\psi\rangle \in \mathcal{H}_n \mid g|\psi\rangle = |\psi\rangle \text{ for every } g \in \mathcal{S}\}. \quad (3)$$

The dimension of $V_{\mathcal{S}}$ is equal to $2^n/|\mathcal{S}|$, which is a power of two. The stabilizer code $V_{\mathcal{S}}$ is identified with the operator

$$\rho := \frac{1}{2^n} \sum_{g \in \mathcal{S}} g, \quad (4)$$

which is, up to a multiplicative constant, equal to the orthogonal projector on the code $V_{\mathcal{S}}$. If $\mathcal{S}$ is a stabilizer with cardinality $|\mathcal{S}| = 2^n$, the code $V_{\mathcal{S}}$ is one-dimensional, or, equivalently, the associated projector ρ has rank one and is therefore of the form

$$\rho = |\psi\rangle\langle\psi| \quad (5)$$

for some $|\psi\rangle \in \mathcal{H}_n$. The class of states $|\psi\rangle$ that are obtained in this way is the set of *stabilizer states*. Thus, a stabilizer state on n qubits is any state $|\psi\rangle$ having the property that $g|\psi\rangle = |\psi\rangle$ for every element g in a maximal stabilizer $\mathcal{S}$, i.e., where $|\mathcal{S}| = 2^n$.

We now introduce the two notions of local equivalence of stabilizer codes (states) that we will study in the following. First, two stabilizer codes ρ and ρ' are called LU equivalent if there exists a local unitary operator $U \in U(2)^{\otimes n}$ such that $U\rho U^\dagger = \rho'$. Second, a 2×2 unitary operator U is called a *Clifford* operator on one qubit if $U\sigma U^\dagger \in \mathcal{G}_1$ for every Pauli matrix $\sigma \in \{X, Y, Z\}$. A *local Clifford* operator (LC operator) on n qubits is a local unitary operator $U = U_1 \otimes \cdots \otimes U_n$, where every tensor factor U_i is a Clifford operator. Two stabilizer codes are called LC equivalent if there exists an LC operator U relating the two codes under conjugation.

An important ingredient in the following will be a third kind of local operations, namely the *local semi-Clifford operations*, which are defined next. A 2×2 unitary operator U is called a *semi-Clifford* operator on one qubit if there exist a Pauli matrix $\sigma \in \{X, Y, Z\}$ such that $U\sigma U^\dagger \in \mathcal{G}_1$. Thus, a semi-Clifford operator is defined to send *at least one* of the Pauli matrices to another Pauli matrix under conjugation (up to a global phase factor). It is clear that every Clifford operator is also a semi-Clifford. We then define a *local semi-Clifford* operator on n qubits to be a local unitary operator $U = U_1 \otimes \cdots \otimes U_n$, where every tensor factor U_i is a semi-Clifford operator.

III. OUTLINE OF THE PROOF

The proof of theorem 1 consist in two main parts. In section IV we investigate the relevance of local semi-Clifford operations in the problem at hand. In particular, we will show that only local semi-Clifford operations can map a given stabilizer state to a second one; in other words, if $|\psi\rangle$ and $|\psi'\rangle$ are two LU equivalent stabilizer states and if U is an LU operator relating these two states, it is proved that U must be a local semi-Clifford operator [19]. In section V will will then use this result to show that, if U is a local semi-Clifford operator such that $U|\psi\rangle = |\psi'\rangle$, then U can be replaced by an LC operator V which also maps $|\psi\rangle$ to $|\psi'\rangle$. In the proof of this second part, an important role will be played by *diagonal* LU and LC operations.

IV. SEMI–CLIFFORD OPERATIONS

In this section we show that LU equivalence between two stabilizer states (codes) can only be realized by local semi-Clifford operations. First we need a number of definitions and preliminary results.

Let $m \in \mathbb{N}_0$. A $[2m, 2m-2, 2]$ stabilizer code is a code with stabilizer of the form

$$\mathcal{S} = \{I_{2m}, \; g, \; g, \; gg'\}, \quad (6)$$

where g, g' and gg' have full support. Every $[2m, 2m-2, 2]$ code is LU equivalent to the code $\rho^{[2m,2m-2,2]}$ equal

to

$$\frac{1}{4^m}(I_{2m} + X^{\otimes 2m} + (-1)^m Y^{\otimes 2m} + Z^{\otimes 2m}). \quad (7)$$

The operator $\rho^{[2,0,2]}$ has rank one, and is therefore a stabilizer state. More particularly, one has

$$\rho^{[2,0,2]} = |\psi_{\rm EPR}\rangle\langle\psi_{\rm EPR}|, \quad (8)$$

where

$$|\psi_{\rm EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (9)$$

is the EPR state. The following result was proven in Ref. [17] and will be an important part of our analysis.

Proposition 1 *[17] Let $m \in \mathbb{N}_0$, $m \geq 2$. Let ρ and ρ' be two $[2m, 2m-2, 2]$ stabilizer codes and let $U \in U(2)^{\otimes n}$ be an LU operator such that $U\rho U^\dagger = \rho'$. Then U is an LC operator.*

Let $\mathcal{S}$ be a stabilizer on n qubits. For every subgroup $\mathcal{T}$ of $\mathcal{S}$, the index of $\mathcal{T}$ in $\mathcal{S}$ is the number $[\mathcal{S} : \mathcal{T}] := |\mathcal{S}|/|\mathcal{T}|$. Note that $|\mathcal{S}|$ is a power of two, and therefore $|\mathcal{T}|$ and $[\mathcal{S} : \mathcal{T}]$ are also powers of two. For every $i = 1, \ldots, n$, define

$$\mathcal{S}\langle i\rangle \ := \ \{g \in \mathcal{S} \mid g_i = I_1\}. \quad (10)$$

Note that $\mathcal{S}\langle i\rangle$ is a subgroup of $\mathcal{S}$, for every $i = 1, \ldots, n$. We can then formulate the following lemmas.

Lemma 1 *Let $\mathcal{S}$ be a stabilizer on n qubits. Then*

$$[\mathcal{S} : \mathcal{S}\langle i\rangle] \in \{1, 2, 4\}, \quad (11)$$

for every $i = 1, \ldots, n$.

Proof: the proof is elementary. We start from the property that $\mathcal{S}$ can be partitioned into cosets of the subgroup $\mathcal{S}\langle i\rangle$:

$$\mathcal{S} = g^1\mathcal{S}\langle i\rangle \cup \cdots \cup g^N\mathcal{S}\langle i\rangle, \quad (12)$$

for some $g^1 = I_n, g^2, \ldots, g^N \in \mathcal{S}$, where $g^j\mathcal{S}\langle i\rangle \cap g^k\mathcal{S}\langle i\rangle = \emptyset$ for every $j, k = 1, \ldots, N$ with $j \neq k$. The number of cosets N is equal to $[\mathcal{S} : \mathcal{S}\langle i\rangle]$. Note that two elements $g, g' \in \mathcal{S}$ belong to different cosets of $\mathcal{S}\langle i\rangle$ if and only if $g_i \neq g'_i$, showing that there can be at most 4 cosets, as $g_i \in \{I_1, X, Y, Z\}$. Since $[\mathcal{S} : \mathcal{S}\langle i\rangle]$ is a power of two, the result follows. □

Lemma 2 *Let ρ and ρ' be LU equivalent stabilizer codes with stabilizers $\mathcal{S}$ and $\mathcal{S}'$, respectively. Let $U = U_1 \otimes \cdots \otimes U_n \in U(2)^{\otimes n}$ such that $U\rho U^\dagger = \rho'$. Then U_i is semi-Clifford for every $i \in \{1, \ldots, n\}$ such that $[\mathcal{S} : \mathcal{S}\langle i\rangle] = 2$.*

Proof: Let $i \in \{1, \ldots, n\}$ such that $[\mathcal{S} : \mathcal{S}\langle i\rangle] = 2$. Since ρ and ρ' are locally equivalent, we then also have $[\mathcal{S}' : \mathcal{S}'\langle i\rangle] = 2$; indeed, the numbers $|\mathcal{S}|$ and $|\mathcal{S}\langle i\rangle|$ are local invariants, such that $[\mathcal{S} : \mathcal{S}\langle i\rangle] = [\mathcal{S}' : \mathcal{S}'\langle i\rangle]$. Therefore, we can partition $\mathcal{S}$ and $\mathcal{S}'$ in cosets as follows:

$$\mathcal{S} = \mathcal{S}\langle i\rangle \cup g\mathcal{S}\langle i\rangle \quad \text{and} \quad \mathcal{S}' = \mathcal{S}'\langle i\rangle \cup g'\mathcal{S}'\langle i\rangle, \quad (13)$$

where $g \in \mathcal{S} \setminus \mathcal{S}\langle i\rangle$ and $g' \in \mathcal{S}' \setminus \mathcal{S}'\langle i\rangle$. Defining

$$\rho\langle i\rangle = \frac{1}{2^n}\sum_{h \in \mathcal{S}\langle i\rangle} h \quad \text{and} \quad \rho'\langle i\rangle = \frac{1}{2^n}\sum_{h' \in \mathcal{S}'\langle i\rangle} h', \quad (14)$$

it follows that

$$\rho = (I_n + g)\rho\langle i\rangle \quad \text{and} \quad \rho' = (I_n + g')\rho'\langle i\rangle \quad (15)$$

Using the identity $U\rho U^\dagger = \rho'$, and hence $U\rho\langle i\rangle U^\dagger = \rho'\langle i\rangle$, it follows that $\left(UgU^\dagger\right)\rho'\langle i\rangle = g'\rho'\langle i\rangle$. The r.h.s. of this equation is a sum of Pauli operators all having the same ith tensor factor, namely g'_i. Therefore, the l.h.s. must also have this property, and this can only occur if $U_i g_i U_i^\dagger \sim g'_i$. Since $g_i \neq I_1 \neq g'_i$, this shows that U_i is semi-Clifford. □

Lemma 3 *Let $\mathcal{S}$ be a stabilizer on n qubits and let Π be the smallest subgroup of $\mathcal{S}$ containing all subgroups $\mathcal{S}\langle i\rangle$, i.e.,*

$$\Pi = \left\{g^1 g^2 \ldots g^n |\ g^i \in \mathcal{S}\langle i\rangle,\ i = 1, \ldots, n\right\} \quad (16)$$

Then one of the following three cases occurs:

(i) $\Pi = \mathcal{S}$.

(ii) $[\mathcal{S} : \Pi] = 2$;

(iii) $[\mathcal{S} : \Pi] = 4$; *in this case, the associated code must be a $[2m, 2m-2, 2]$ code.*

Proof: Since Π is a subgroup of $\mathcal{S}$, $[\mathcal{S} : \Pi]$ is a power of two. Furthermore, each $\mathcal{S}\langle i\rangle$ is a subgroup of Π and therefore $[\mathcal{S} : \Pi] \leq [\mathcal{S} : \mathcal{S}\langle i\rangle] \leq 4$, for every $i = 1, \ldots, n$. This shows that

$$[\mathcal{S} : \Pi] \in \{1, 2, 4\}. \quad (17)$$

We investigate these possibilities case by case. First, if $[\mathcal{S} : \Pi] = 1$ then $\Pi = \mathcal{S}$ trivially, which proves (i).

We now prove (iii). If $[\mathcal{S} : \Pi] = 4$ then $\mathcal{S}$ can be partitioned in cosets as follows:

$$\mathcal{S} = \Pi \cup g\Pi \cup g'\Pi \cup gg'\Pi,$$

where $g, g' \in \mathcal{S} \setminus \Pi$ such that $gg' \in \mathcal{S} \setminus \Pi$. Note that the elements g, g' and gg' must have full support. Now, since $[\mathcal{S} : \Pi] = 4$ we must have $[\mathcal{S} : \mathcal{S}\langle i\rangle] = 4$ and therefore

$$\mathcal{S} = \mathcal{S}\langle i\rangle \cup g\mathcal{S}\langle i\rangle \cup g'\mathcal{S}\langle i\rangle \cup gg'\mathcal{S}\langle i\rangle,$$

for all $i = 1, \ldots, n$. We now claim that

$$\Pi \cap g\mathcal{S}\langle i\rangle = \Pi \cap g'\mathcal{S}\langle i\rangle = \Pi \cap gg'\mathcal{S}_i = \emptyset, \quad (18)$$

proving that $p \in \mathcal{S}\langle i\rangle$ for every $p \in \Pi$, and therefore $\Pi = \mathcal{S}\langle i\rangle$. As this equality holds for all $i = \{1, \ldots, n\}$, we obtain

$$\Pi = \mathcal{S}\langle 1\rangle = \cdots = \mathcal{S}\langle n\rangle = \{I\}, \tag{19}$$

such that

$$\mathcal{S} = \{I_n,\ g,\ g',\ gg'\}, \tag{20}$$

which proves case (iii). We now prove claim (18). First, suppose that $\Pi \cap g\mathcal{S}\langle i\rangle \neq \emptyset$, i.e., there exists $p \in \Pi$ and $h^i \in \mathcal{S}\langle i\rangle$ such that $p = gh^i$. But then

$$g = ph^i \in \Pi, \tag{21}$$

where we have used that $h^i \in \mathcal{S}\langle i\rangle \subseteq \Pi$. Thus, we obtain a contradiction, since $g \in \mathcal{S} \setminus \Pi$ by definition, and we have shown that $\Pi \cap g\mathcal{S}\langle i\rangle = \emptyset$. The rest of the claim is proven analogously. This completes the proof of the lemma. □

Before proving the main result of this section, we need one additional result. The *support* [20] of a stabilizer $\mathcal{S}$ is the set

$$\mathrm{supp}(\mathcal{S}) := \bigcup_{g\in\mathcal{S}} \mathrm{supp}(g). \tag{22}$$

Theorem 2 *Let ρ and ρ' be LU equivalent stabilizer codes with stabilizers $\mathcal{S}$ and $\mathcal{S}'$ on $n \geq 2$ qubits such that ρ cannot be written as a product of the form*

$$|\psi\rangle\langle\psi| \otimes \rho'', \tag{23}$$

where $|\psi\rangle$ is a 2–qubit stabilizer state LU equivalent to the EPR state and ρ'' is a stabilizer code on $n-2$ qubits. Let $U = U_1 \otimes \cdots \otimes U_n \in U(2)^{\otimes n}$ such that $U\rho U^\dagger = \rho'$. Then U_i is semi-Clifford for every $i \in supp(\mathcal{S})$.

Proof: We prove the result by induction on n. If $n = 2$, up to local equivalence plus permutations of the 2 qubits the following stabilizer codes ρ fulfilling the requirement of the theorem exist:

$$4\rho = \begin{cases} I_2 \\ I_2 + Z \otimes Z \\ I_2 + I_1 \otimes Z \\ I_2 + I_1 \otimes Z + Z \otimes I_1 + Z \otimes Z \end{cases} \tag{24}$$

It is straightforward to verify that the result holds for these codes.

In the induction step of the proof, fix $n \geq 3$ and suppose the result holds for all $n' < n$. Let ρ and ρ' be locally equivalent stabilizer codes on $n \geq 3$ qubits satisfying the requirement of the theorem, and let $U = U_1 \otimes \cdots \otimes U_n \in U(2)^{\otimes n}$ such that $U\rho U^\dagger = \rho'$. It follows that

$$U[i]\ \mathrm{Tr}_i(\rho) U[i]^\dagger = \ \mathrm{Tr}_i(\rho') \tag{25}$$

for every $i = 1, \ldots, n$, where we have denoted

$$U[i] = \ U_1 \otimes \cdots \otimes U_{i-1} \otimes U_{i+1} \otimes \cdots \otimes U_n. \tag{26}$$

Note that $\mathrm{Tr}_i(\rho)$ and $\mathrm{Tr}_i(\rho')$ are stabilizer codes on $n-1$ qubits, and that $\mathrm{Tr}_i(\rho)$ cannot be written as a product (23). We can therefore apply the induction hypotheses to every pair $\mathrm{Tr}_i(\rho)$ and $\mathrm{Tr}_i(\rho')$, where $i = 1, \ldots, n$. This proves that U_i is semi-Clifford for every j in the set

$$\bigcup_{i=1}^{n} \mathrm{supp}\ \mathcal{S}\langle i\rangle. \tag{27}$$

Now, if the set (27) is equal to $\mathrm{supp}(\mathcal{S})$ then we are done. If this is not the case, then there exist $j \in \mathrm{supp}(\mathcal{S})$ such that $j \notin \mathrm{supp}(\mathcal{S}\langle i\rangle)$ for every $i = 1, \ldots, n$, and hence $j \notin \mathrm{supp}(\Pi)$, where Π is defined as in lemma 3. This last property implies that $\Pi \neq \mathcal{S}$, and therefore case (ii) or case (iii) in lemma 3 must apply.

If case (ii) holds, the stabilizer $\mathcal{S}$ can be written as a partition

$$\mathcal{S} = \Pi \cup g\Pi, \tag{28}$$

where $g \in \mathcal{S}\setminus\Pi$, and therefore g has full support. Expression (28) together with the property that $j \notin \mathrm{supp}\ (\Pi)$ imply that $h_j \in \{I_1, g_j\}$ for every $h \in \mathcal{S}$, and thus $[\mathcal{S} : \mathcal{S}\langle j\rangle] = 2$. Lemma 2 then shows that U_j must be a semi-Clifford operation.

If case (iii) holds, then ρ and ρ' must be $[2m, 2m-2, 2]$ codes with $m \neq 1$, and proposition 1 then implies that U is a local Clifford operation, which is a fortiori local semi-Clifford. This proves the result. □

Corollary 1 *Let $|\psi\rangle$ and $|\psi'\rangle$ be fully entangled, LU equivalent stabilizer states on $n \geq 3$ qubits, and let $U \in U(2)^{\otimes n}$ be an LU operator such that $U|\psi\rangle = |\psi'\rangle$. Then U is a local semi-Clifford operator.*

Proof: letting $\mathcal{S}$ be the stabilizer of $|\psi\rangle$, it is clear that $\mathcal{S}$ has full support. Moreover, $|\psi\rangle$ is a fully entangled state on $n \geq 3$ qubits and therefore satisfies the requirements of theorem 2. The result follows immediately. □

From this point on, we will only consider fully entangled stabilizer states on $n \geq 3$ qubits. Note that the restriction to fully entangled states does not entail a loss of generality.

V. DIAGONAL LU AND LC OPERATIONS

In this section we use the result obtained in section IV to obtain the proof of our main result, theorem 1. Let $|\psi\rangle$ and $|\psi'\rangle$ be stabilizer states on n qubits and let $U = U_1 \otimes \cdots \otimes U_n$ be an LU operator such that $U|\psi\rangle = |\psi'\rangle$. According to corollary 1, there exist Pauli matrices $\sigma_i \in \{X, Y, Z\}$ such that $U_i\sigma_i U_i^\dagger \in \mathcal{G}_1$ for every $i = 1, \ldots, n$. It is then easy to verify that there exist LC operators

$$V = V_1 \otimes \cdots \otimes V_n, \quad V' = V_1' \otimes \cdots \otimes V_n' \tag{29}$$

such that

$$V_i' U_i V_i^\dagger Z (V_i' U_i V_i^\dagger)^\dagger = Z \tag{30}$$

for every $i = 1, \ldots, n$. Defining

$$\begin{aligned} D_i &:= V_i' U_i V_i^\dagger \quad (i = 1, \ldots, n), \\ D &:= D_1 \otimes \cdots \otimes D_n, \\ |\phi\rangle &:= V|\psi\rangle \\ |\phi'\rangle &:= V'|\psi\rangle, \end{aligned} \tag{31}$$

it follows that $D|\phi\rangle = |\phi'\rangle$. Note that (30) is equivalent to $[D_i, Z] = 0$ and therefore every D_i is a diagonal unitary matrix. The operator D will be called a DLU operator (on n qubits), short for *diagonal local unitary*. We now make the following claim.

Theorem 3 *Let $|\phi\rangle$ and $|\phi'\rangle$ be stabilizer states on n qubits and suppose there exists a DLU operation D on n qubits such that $D|\phi\rangle = |\phi'\rangle$. Then there exists a diagonal local Clifford (DLC) operation C on n qubits such that $C|\phi\rangle = |\phi'\rangle$.*

Note that a proof of the above theorem will immediately yield a proof of theorem 1. Indeed, using the notations (31) the identity $C|\phi\rangle = |\phi'\rangle$ implies that

$$V'^\dagger C V|\psi\rangle = |\psi'\rangle, \tag{32}$$

where $V'^\dagger C V$ is an LC operation since it is a product of LC operators. This shows that two LU equivalent stabilizer states $|\psi\rangle$ and $|\psi'\rangle$ are always LC equivalent.

In the remainder of this section we give a proof of theorem 3. To do so, let $|\phi\rangle$ and $|\phi'\rangle$ be arbitrary stabilizer states on n qubits and suppose there exists a DLU operation D on n qubits such that $D|\phi\rangle = |\phi'\rangle$. Let $\{|x\rangle\}_{x \in \mathbb{F}_2^n}$ be the computational basis of the $n-$qubit Hilbert space $\mathcal{H}_n$. Writing

$$\begin{aligned} D_x &:= \langle x|D|x\rangle, \\ \phi_x &:= \langle x|\phi\rangle \\ \phi_x' &:= \langle x|\phi'\rangle \end{aligned} \tag{33}$$

for every $x \in \mathbb{F}_2^n$, the identity $D|\phi\rangle = |\phi'\rangle$ is equivalent to

$$D_x \phi_x = \phi_x', \tag{34}$$

for every $x \in \mathbb{F}_2^n$. This identity is equivalent to

$$D_x = (\phi_x)^{-1} \phi_x' \tag{35}$$

for every $x \in \mathbb{F}_2^n$ such that $\phi_x \neq 0$. In other words, we obtain constraints on the diagonal elements D_x of D on those locations on the diagonal where the corresponding component ϕ_x of the state $|\phi\rangle$ is nonzero. Note that the equations in (34) involving those $x \in \mathbb{F}_2^n$ where $\phi_x = 0$ do not impose any constraints on D_x (they merely show that $\phi_x = 0$ if and only $\phi_x' = 0$). In the following we perform a detailed analysis of equation (35). This analysis will consist of three main parts A, B and C.

[A] First, since $|\phi\rangle$ and $|\phi'\rangle$ are stabilizer states, the coefficients ϕ_x and ϕ_x' have a very specific structure. Of central importance in this context is a result in Ref. [18] showing an intimate connection between these coefficients and quadratic forms over $\mathbb{F}_2$. This will yield a description of the r.h.s. of (35) in terms of such quadratic functions.

[B] Second, having obtained this result, we note that equation (35) states that the coefficients $(\phi_x)^{-1}\phi_x'$ are obtained as diagonal elements of a *local* diagonal operator, which places severe restrictions on the quadratic functions describing these coefficients. We will obtain a characterization of the possible quadratic forms in this respect.

[C] Finally, using this characterization we will constructively show that there exists a DLC operator C^{final} such that

$$C_x^{\text{final}} = (\phi_x)^{-1}\phi_x' = D_x \tag{36}$$

for every $x \in \mathbb{F}_2^n$ such that $\phi_x \neq 0$. Note that this will complete the proof of theorem 3, since the first equality in (36) is equivalent to $C^{\text{final}}|\phi\rangle = |\phi'\rangle$.

In the next three paragraphs we will consecutively deal with parts A, B and C. To maintain an overview of the different steps in our arguments, the proofs of propositions and lemmas will be postponed to the last paragraph of section V.

Part A

In this section we consider the connection between stabilizer states and quadratic functions over $\mathbb{F}_2$. First we introduce some definitions. Let $m \in \mathbb{N}_0$. A function $q : \mathbb{F}_2^m \to \mathbb{F}_2$ is called a quadratic form if there exist coefficients $\theta_{ij} \in \mathbb{F}_2$ $(i, j = 1, \ldots, m,\ i < j)$ and a vector $\lambda \in \mathbb{F}_2^m$ such that

$$q(x) = \sum_{i<j} \theta_{ij} x_i x_j + \lambda^T x \tag{37}$$

for every $x = (x_1, \ldots, x_m) \in \mathbb{F}_2^m$. The first term in the r.h.s. of (37) is called the quadratic part of q and the second term is called its linear part. Letting θ be the $k \times k$ symmetric matrix with zero diagonal (in short: *ZDS matrix*) such that the ijth entry of θ is equal to θ_{ij}, for every $i < j$, expression (37) can be written more compactly as

$$q(x) = x^T \mathcal{L}(\theta) x + a^T x, \tag{38}$$

where $\mathcal{L}(\theta)$ denotes the strictly lower triangular part of θ, i.e., $\mathcal{L}(\theta)$ is the $m \times m$ matrix satisfying $\mathcal{L}(\theta)_{ij} = \theta_{ij}$ for every $i < j$ and $\mathcal{L}(\theta)_{ij} = 0$ otherwise.

We also need some definitions regarding subspaces over $\mathbb{F}_2$ and their cosets. Let S be a $k-$dimensional subspace of $\mathbb{F}_2^n$. A generator matrix of S is an $n \times k$ matrix R, the

columns of which form a basis of S. If R is a generator matrix of S, an arbitrary element $y \in S$ can be written as $y = Rs$ for some $s \in \mathbb{F}_2^k$. Letting $t \in \mathbb{F}_2^n$ be an arbitrary vector, the coset of S determined by t is the set

$$S + t := \{y + t \mid y \in S\} = \{Rs + t \mid s \in \mathbb{F}_2^k\} \quad (39)$$

We can now state the connection between quadratic forms and stabilizer states by recalling the following result in Ref. [18].

Theorem 4 *[18] Let $|\phi\rangle$ be a stabilizer state on n qubits. Then there exist*

(i) a linear subspace S of $\mathbb{F}_2^n$,

(ii) a quadratic form $q : \mathbb{F}_2^k \to \mathbb{F}_2$, where k is the dimension of S, and

(iii) vectors $t \in \mathbb{F}_2^n$ and $d \in \mathbb{F}_2^k$ and a complex phase factor γ,

such that

$$(2^{k/2}\gamma)\phi_x = \begin{cases} i^{d^T s}(-1)^{q(s)} & \text{for every } x = Rs + t \\ 0 & \text{otherwise,} \end{cases} \quad (40)$$

where R is a generator matrix of S, and where the algebra in the exponent of the complex number i is to be performed over $\mathbb{F}_2$ (i.e., modulo 2).

Qualitatively, this result states that, first, the nonzero components ϕ_x can only be equal to ± 1 or $\pm i$ (up to the overall normalization); second, the distribution of the ± 1's and $\pm i$'s is governed by quadratic and linear forms; third, the nonzero components ϕ_x are organized in such a way that the corresponding vectors x lie in a coset of a linear subspace S of $\mathbb{F}_2^n$.

Now, let $|\phi\rangle$ and $|\phi'\rangle$ be arbitrary stabilizer states on n qubits and suppose there exists a DLU operation D on n qubits such that $D|\phi\rangle = |\phi'\rangle$. Define S, k, q, t and d for the state $|\phi\rangle$ as in theorem 4 and define S', k', q', t' and d' analogously for the state $|\phi'\rangle$. First, note that $k = k'$, $S = S'$ an $t = t'$ since $\phi_x = 0$ if and only $\phi'_x = 0$. Moreover, using the notations (33), we find that (35) is equivalent to

$$\begin{aligned} D_x &\sim i^{d'^T s}(-i)^{d^T s}(-1)^{q(s)+q'(s)} \\ &= i^{(d+d')^T s}(-1)^{q(s)+q'(s)+s^T d' d^T s + d^T s}, \end{aligned} \quad (41)$$

for every $x = Rs + t$, where $s \in \mathbb{F}_2^k$, where the symbol $\sim$ denotes equality up to a complex phase factor independent of x, and where in the second equality we have used that

$$i^a i^b = i^{a+b}(-1)^{ab} \quad (42)$$

for every $a, b \in \mathbb{F}_2$; as pointed out before, calculations in the exponent of i are always performed over $\mathbb{F}_2$. Thus, we have obtained a description of D_x in terms of quadratic forms for all x lying in the coset $S + t$. In particular, for every $x = Rs + t \in S + t$, the coefficient D_x has the form

$$D_x \sim i^{a^T s}(-1)^{f(s)}, \quad (43)$$

for some quadratic form f and some vector $a \in \mathbb{F}_2^k$. Note that, as remarked before, we have obtained no information whatsoever about the coefficients D_x where $x \notin S+t$.

Part B

Having obtained the general form (43) of D_x for $x \in S + t$, next we investigate which constraints are imposed on the quadratic form f using the information that D is a *local* diagonal matrix. It will turn out below that it suffices to perform this analysis for the special case where $a = 0$ and $t = 0$ in (43), i.e., the case were a genuine subspace S is considered rather than one of its cosets, and, furthermore, where only real coefficients $(-1)^{f(s)}$ occur in the r.h.s of (43). We will show below that the general case can be reduced to this special situation.

For the special case, the following result is obtained.

Proposition 2 *Let S be a $k-$dimensional subspace of $\mathbb{F}_2^n$ with generator matrix R, let f be a quadratic form on $\mathbb{F}_2^k$, and let D be a DLU operator on n qubits such that*

$$D_y = (-1)^{f(s)} \quad (44)$$

for every $y = Rs \in S$. Then there exists a vector $u \in S^\perp$ such that the ZDS matrix defining the quadratic part of f is equal to $R^T \hat{u} R$; here, $\hat{u}$ is the $n \times n$ diagonal matrix over $\mathbb{F}_2$ having the vector u on its diagonal.

Part C

Proposition 2 gives a complete characterization of the quadratic forms f that can appear in (44). Next we will use this characterization to show that for every DLU operator D satisfying (44) there exists a DLC operator C such that $D_y = C_y$ for every $y \in S$.

Proposition 3 *Let*

$$C := \begin{bmatrix} 1 & 0 \\ 0 & i^{u_1}(-1)^{v_1} \end{bmatrix} \otimes \cdots \otimes \begin{bmatrix} 1 & 0 \\ 0 & i^{u_n}(-1)^{v_n} \end{bmatrix} \quad (45)$$

be a DLC operator, where $u_i, v_i \in \mathbb{F}_2$, for every $i = 1, \ldots, n$, and let S be a $k-$dimensional subspace of $\mathbb{F}_2^n$ with generator matrix R, such that $u := (u_1, \ldots, u_n) \in S^\perp$. Then there exists a vector $w \in \mathbb{F}_2^k$ such that

$$C_y = (-1)^{s^T \mathcal{L}(R^T \hat{u} R)s + w^T s} \quad (46)$$

for every $y = Rs \in S$. Moreover, the set of vectors w that can be obtained by tuning u and v is the whole space $\mathbb{F}_2^k$.

We then immediately obtain the following result.

Corollary 2 *Let S be a $k-$dimensional subspace of $\mathbb{F}_2^n$ with generator matrix R, let f be a quadratic form on $\mathbb{F}_2^k$, and let D be a DLU operator on n qubits such that*

$$D_y = (-1)^{f(s)} \tag{47}$$

for every $y = Rs \in S$. Then there exists a DLC operator C such that $C_y = D_y$ for every $y \in S$.

Proof: this is an immediate corollary of propositions 2 and 3. □

The only fact that now remains to be proven is that, starting from the general situation (43), one can work one's way back to the special case we considered in proposition 2. The general situation is the following: let S be a $k-$dimensional subspace of $\mathbb{F}_2^n$ with generator matrix R, let f be a quadratic form on $\mathbb{F}_2^k$, and let $t \in \mathbb{F}_2^n$ and $a \in \mathbb{F}_2^k$. Let D be a DLU operator on n qubits such that

$$D_x \sim i^{a^T s}(-1)^{f(s)} \tag{48}$$

for every $x = Rs + t \in S + t$, where $s \in \mathbb{F}_2^k$. We also need an additional definition. Let $X^{[t]}$ be the Pauli operator on n qubits such that $X_i^{[t]} = X$ whenever $t_i = 1$ and $X_i^{[t]} = I_1$ otherwise. We can then state the following result.

Lemma 4 *With the definitions above, there exists a DLC operator $\tilde{C}$ and a quadratic form g on $\mathbb{F}_2^k$ such that, denoting $\tilde{D} := X^{[t]}\tilde{C}DX^{[t]}$, one has*

$$\tilde{D}_y = (-1)^{g(s)} \tag{49}$$

for every $y = Rs \in S$.

Note that $\tilde{D}$ is a DLU operator, since $\tilde{C}D$ is DLU and $X^{[t]}$ is a local permutation matrix (note that $X^{[t]}$ is also symmetric). Furthermore, since $\tilde{D}$ satisfies the requirements of corollary 2, it follows that there exists a DLC operator C such that $C_y = \tilde{D}_y$ for every $y \in S$. This implies that for every $y \in S$ we have

$$\begin{aligned} D_{y+t} &= \tilde{C}_{y+t}^{-1}(X^{[t]}\tilde{D}X^{[t]})_{y+t} = \tilde{C}_{y+t}^{-1}\tilde{D}_y \\ &= \tilde{C}_{y+t}^{-1}C_y \\ &= \tilde{C}_{y+t}^{-1}\left(X^{[t]}CX^{[t]}\right)_{y+t} \\ &= \left(\tilde{C}^{-1}X^{[t]}CX^{[t]}\right)_{y+t}. \end{aligned} \tag{50}$$

As $\tilde{C}^{-1}$ and $X^{[t]}CX^{[t]}$ are both DLC operators, also their product must be DLC. Thus, we have obtained a DLC operator

$$C^{\text{final}} := \tilde{C}^{-1}X^{[t]}CX^{[t]} \tag{51}$$

such that $C_x^{\text{final}} = D_x$ for every $x \in S + t$. It then follows from (35) that

$$C_x^{\text{final}} = (\phi_x)^{-1}\phi'_x \tag{52}$$

for every x such that $\phi_x \neq 0$, and w therefore have

$$C^{\text{final}}|\phi\rangle = |\phi'\rangle, \tag{53}$$

which completes the proof of theorem 3.

Proofs of propositions 2 and 3 and lemma 4

Proof of proposition 2: Let F be a quadratic form on $\mathbb{F}_2^n$ such that

$$F(y) = f(s) \tag{54}$$

for every $y = Rs \in S$. Note that $D_y = (-1)^{F(y)}$ for every $y \in S$. We let θ be the associated $n \times n$ ZDS matrix as in (38).

Writing D as

$$D = \alpha \begin{bmatrix} 1 & 0 \\ 0 & \alpha_1 \end{bmatrix} \otimes \cdots \otimes \begin{bmatrix} 1 & 0 \\ 0 & \alpha_n \end{bmatrix}, \tag{55}$$

where $\alpha, \alpha_1, \ldots, \alpha_n$ lie on the complex unit circle, we have

$$D_x = \alpha \prod_{i=1}^{n} \alpha_i^{x_i} \tag{56}$$

for every $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. This immediately shows that

$$\alpha = D_0 = (-1)^{F(0)} = 1. \tag{57}$$

Further, letting $y, y' \in S$, simple algebra shows that

$$D_{y+y'} = D_y D_{y'} \prod_{i=1}^{n} \beta_i^{y_i y'_i}, \tag{58}$$

where $\beta_i := (\bar{\alpha}_i)^2$, and therefore

$$(-1)^{F(y+y')+F(y)+F(y')} = \prod_{i=1}^{n} \beta_i^{y_i y'_i}. \tag{59}$$

In particular, this result shows that, for every $y, y' \in S$, the sum $F(y + y') + F(y) + F(y')$ can only depend on the Hadamard product $y \circ y' := (y_1 y'_1, \ldots, y_n y'_n)$ of the vectors y and y'. Therefore, there exists a function $G : \mathbb{F}_2^n \to \mathbb{F}_2$ (in one variable) such that

$$F(y + y') + F(y) + F(y') = G(y \circ y') \tag{60}$$

for every $y, y' \in S$. We now analyze the above equation. First, it is easy to verify that the l.h.s. of (60) is equal to $y^T\theta y'$. Writing $y = Rs$ and $y' = Rs'$ for some $s, s' \in \mathbb{F}_2^k$, it follows that

$$[\text{l.h.s. of (60)}] = y^T\theta y' = s^T(R^T\theta R)s'. \tag{61}$$

Second, we note that *every* function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is a polynomial function; therefore, we can write G as a sum $G = c + L + H$, where $c \in \mathbb{F}_2$ is a constant,

$$L : x \in \mathbb{F}_2^n \mapsto u^T x \tag{62}$$

is a linear function (for some $u \in \mathbb{F}_2^n$) and H is a polynomial function with terms of degree ≥ 2. We then find that (60) is equivalent to

$$s^T(R^T\theta R)s' = c + L(Rs \circ Rs') + H(Rs \circ Rs') \tag{63}$$

for every $s, s' \in \mathbb{F}_2^k$. Note that we immediately find that $c = 0$. Further, we note that the l.h.s. of (63) is bilinear in s and s', and therefore the r.h.s. of this equation must also have this property. However, $H(Rs \circ Rs')$ does not contain any bilinear terms in s and s', but only higher–order terms, and $H(Rs \circ Rs')$ must therefore be identical to zero. We can therefore conclude that

$$s^T(R^T\theta R)s' = L(Rs \circ Rs') = \sum_{i=1}^{n} u_i(Rs)_i(Rs')_i \tag{64}$$

(where we recall that u is defined in (62)). Some algebra then shows that the r.h.s. of this equation is equal to $s^T R^T \hat{u} R s'$, and therefore we obtain the identity

$$R^T\theta R = R^T\hat{u}R. \tag{65}$$

We also note that $R^T\theta R$ has zero diagonal, implying that also $R^T\hat{u}R$ must have this property; one can verify that this is equivalent to requiring that $u \in S^\perp$.

In a last step we recall that θ is the ZDS matrix associated to the quadratic form F, i.e.,

$$F(x) = x^T\mathcal{L}(\theta)x + F_{\text{lin}}(x), \tag{66}$$

for every $x \in \mathbb{F}_2^n$, where F_{lin} is the linear part of F. We also recall that F was defined as an extension of f to the entire space $\mathbb{F}_2^n$. Using (54) we find that

$$f(s) = F(Rs) = s^T R^T\mathcal{L}(\theta)Rs + F_{\text{lin}}(Rs) \tag{67}$$

for every $s \in \mathbb{F}_2^k$. Using lemma 5, which is proven below, we find that there exists a vector $\lambda \in \mathbb{F}_2^k$ such that

$$s^T R^T\mathcal{L}(\theta)Rs = s^T\mathcal{L}(R^T\theta R)s + \lambda^T s \tag{68}$$

for every $s \in \mathbb{F}_2^k$. This shows that the quadratic part of f is determined by the matrix $R^T\theta R$. But (65) shows that $R^T\theta R = R^T\hat{u}R$, and the desired result is obtained. □

Lemma 5 *Let θ be an $n \times n$ ZDS matrix over $\mathbb{F}_2$ and let R be an $n \times k$ matrix over $\mathbb{F}_2$, for some $n, k \in \mathbb{N}_0$. Then there exists a vector $\lambda \in \mathbb{F}_2^k$ such that*

$$s^T R^T\mathcal{L}(\theta)Rs = s^T\mathcal{L}(R^T\theta R)s + \lambda^T s \tag{69}$$

for every $s \in \mathbb{F}_2^k$.

Proof: Since θ is ZDS, we have $\theta = \mathcal{L}(\theta) + (\mathcal{L}(\theta))^T$ and thus

$$\begin{aligned} R^T\theta R &= R^T\mathcal{L}(\theta)R + R^T(\mathcal{L}(\theta))^T R \\ &= R^T\mathcal{L}(\theta)R + (R^T\mathcal{L}(\theta)R)^T \end{aligned} \tag{70}$$

Since $R^T\theta R$ is also ZDS [21], we also have

$$R^T\theta R = \mathcal{L}(R^T\theta R) + (\mathcal{L}(R^T\theta R))^T. \tag{71}$$

It follows from (70) and (71) that

$$X := R^T\mathcal{L}(\theta)R + \mathcal{L}(R^T\theta R) \tag{72}$$

is a symmetric matrix. Writing X as a sum $X := \Xi + \Lambda$, where Ξ is ZDS and Λ is diagonal, it follows that

$$\begin{aligned} s^T R^T\mathcal{L}(\theta)Rs + s^T\mathcal{L}(R^T\theta R)s &= s^T X s \\ &= s^T\Lambda s, \end{aligned} \tag{73}$$

for every $s \in \mathbb{F}_2^k$, where we have used that $s^T\Xi s = 0$ as Ξ is ZDS. Denoting $\lambda := (\Lambda_{11}, \ldots, \Lambda_{kk})$, we have

$$s^T\Lambda s = \lambda^T s, \tag{74}$$

and it follows that

$$s^T R^T\mathcal{L}(\theta)Rs + s^T\mathcal{L}(R^T\theta R)s = \lambda^T s, \tag{75}$$

for every $s \in \mathbb{F}_2^k$. This ends the proof. □

Proof of proposition 3: For every $x \in \mathbb{F}_2^n$, we have

$$C_x = i^{u_1 x_1} \ldots i^{u_n x_n}(-1)^{v^T x}. \tag{76}$$

Using (42), simple algebra shows that (76) is equal to

$$i^{u^T x}(-1)^{x^T\mathcal{L}(uu^T)x + v^T x}. \tag{77}$$

Letting $y = Rs \in S$ and recalling that $u \in S^\perp$, it follows that

$$C_y = (-1)^{s^T R^T\mathcal{L}(uu^T)Rs + v^T Rs}. \tag{78}$$

Now we note that $\mathcal{L}(uu^T) = \mathcal{L}(uu^T + \hat{u})$ and the symmetric matrix $uu^T + \hat{u}$ has zero diagonal, such that lemma 5 can be applied to this matrix; this shows that there exists a vector $\lambda \in \mathbb{F}_2^k$ such that

$$\begin{aligned} s^T R^T\mathcal{L}(uu^T)R^T s &= s^T R^T\mathcal{L}(uu^T + \hat{u})R^T s \\ &= s^T\mathcal{L}(R^T(uu^T + \hat{u})R)s + \lambda^T s, \end{aligned} \tag{79}$$

for every $s \in \mathbb{F}_2^k$, where in the second equality we have used lemma 5. Moreover, since $u \in S^\perp$ we have $R^T u = 0$, and we obtain

$$s^T R^T\mathcal{L}(uu^T)R^T s = s^T\mathcal{L}(R^T\hat{u}R)s + \lambda^T s. \tag{80}$$

Using this result in (78) shows that

$$C_y = (-1)^{s^T\mathcal{L}(R^T\hat{u}R)s + w^T s}, \tag{81}$$

where the vector w is equal to

$$w = R^T v + \lambda. \tag{82}$$

Since R has full rank and λ is only a function of u (and not of v), it follows that the set of vectors $R^T v + \lambda$ that can be obtained by tuning u and v is the whole space $\mathbb{F}_2^k$. This ends the proof. □

Proof of lemma 4: Since the map

$$f_a : x = Rs + t \in S + t \mapsto f_a(x) := a^T s \tag{83}$$

is an affine map defined on the coset $S+t$, there exists an affine map F_a defined on the whole space $\mathbb{F}_2^n$ such that f_a is the restriction of F_a to $S + t$. In other words, there exists a vector $\tilde{a} = (\tilde{a}_1, \ldots, \tilde{a}_n) \in \mathbb{F}_2^n$ and a constant $c \in \mathbb{F}_2$ such that

$$a^T s = \tilde{a}^T x + c, \tag{84}$$

for every $x = Rs + t \in S + t$. A successive application of the rule (42) then shows that

$$i^{a^T s} = i^{\tilde{a}^T x + c} = \gamma\ i^{\tilde{a}_1 x_1} \ldots i^{\tilde{a}_n x_n} (-1)^{h(s)}, \tag{85}$$

where h is some quadratic form on $\mathbb{F}_2^k$ and γ is a complex phase factor independent of s. We now define the DLC operator

$$\tilde{C} := \bar{\gamma} \begin{bmatrix} 1 & 0 \\ 0 & (-i)^{\tilde{a}_1} \end{bmatrix} \otimes \cdots \otimes \begin{bmatrix} 1 & 0 \\ 0 & (-i)^{\tilde{a}_n} \end{bmatrix}. \tag{86}$$

We then have

$$\tilde{C}_x = \bar{\gamma} (-i)^{\tilde{a}_1 x_1} \ldots (-i)^{\tilde{a}_n x_n} \tag{87}$$

for every $x = Rs + t \in S + t$. This property, together with the given (48), shows that

$$\tilde{C}_x D_x = (-1)^{f(s)+h(s)} \tag{88}$$

for every $x = Rs + t$. Note that $g := f + h$ is again a quadratic form. We now define

$$\tilde{D} := X^{[t]} \tilde{C} D X^{[t]} \tag{89}$$

and calculate $\tilde{D}_y$ for every $y = Rs \in S$:

$$\begin{aligned} \tilde{D}_y &= \langle y | X^{[t]} \tilde{C} D X^{[t]} | y \rangle \\ &= \langle y + t | \tilde{C} D | y + t \rangle \\ &= \tilde{C}_{y+t} D_{y+t} = (-1)^{g(s)}. \end{aligned} \tag{90}$$

This proves the desired result. □

Acknowledgments

MVDN thanks F. Verstraete and R. Raussendorf for interesting discussions, and Prof. J. Preskill for inviting him to visit the Institute for Quantum Information at the California Institute of Technology. MVDN thanks E. Hostens for a thorough reading of the manuscript. Research of MVDN, JD and BDM supported by: Research Council KUL: GOA AMBioRICS, CoE EF/05/006 Optimization in Engineering, several PhD/postdoc and fellow grants; Flemish Government: FWO: PhD/postdoc grants, projects, 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 (new quantum algorithms), G.0499.04 (Statistics), G.0211.05 (Nonlinear), G.0226.06 (cooperative systems and optimization), G.0321.06 (Tensors), G.0553.06 (VitamineD), research communities (ICCoS, ANMMM, MLDM); IWT: PhD Grants,GBOU (McKnow), Eureka-Flite2 Belgian Federal Science Policy Office: IUAP P5/22 ('Dynamical Systems and Control: Computation, Identification and Modelling', 2002-2006) ; PODO-II (CP/40: TMS and Sustainability); EU: FP5-Quprodis; ERNSI; Contract Research/agreements: ISMC/IPCOS, Data4s, TML, Elia, LMS, Mastercard

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

[2] 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.

[3] R. Raussendorf, J. Harrington, and K. Goyal. A fault-tolerant one-way quantum computer. quant-ph/0510135, 2005.

[4] M. Hein, J. Eisert, and H.J. Briegel. Multi-party entanglement in graph states. *Phys. Rev. A*, 69:062311, 2004. quant-ph/0307130.

[5] O. Guehne, G. Toth, P. Hyllus, and H.J. Briegel. Bell inequalities for graph states. quant-ph/0410059, 2004.

[6] M. Hein, W. Dür, and H.J. Briegel. Entanglement properties of multipartite entangled states under the influence of decoherence. quant-ph/0408165.

[7] W. Dür and H.J. Briegel. Stability of macroscopic entanglement under decoherence. *Phys. Rev. Lett.*, 92(18):180403, 2004.

[8] D. Fattal, T. Cubitt, Y. Yamamoto, S. Bravyi, and I. Chuang. Entanglement in the stabilizer formalism.

quant-ph/0406168, 2004.

[9] S. Bravyi, D. Fattal, and D. Gottesman. GHZ extraction yield for multipartite stabilizer states. quant-ph/0504208, 2005.

[10] G. Toth, O. Guehne, and H. Briegel. Two-setting Bell inequalities for graph states. quant-ph/0510007, 2005.

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

[12] M. Van den Nest, J. Dehaene, and B. De Moor. Efficient algorithm to recognize local Clifford equivalence of graph states. *Phys. Rev. A*, 70:034302, 2004. quant-ph/0405023.

[13] M. Van den Nest, J. Dehaene, and B. De Moor. Finite set of invariants to characterize local Clifford equivalence of stabilizer states. *Phys. Rev. A*, 72:014307, 2005. quant-ph/0410165.

[14] M. Van den Nest, J. Dehaene, and B. De moor. Local unitary versus local Clifford equivalence of stabilizer states. *Phys. Rev. A*, 71:062323, 2005. quant-ph/0411115.

[15] M. Van den Nest, J. Dehaene, and B. De Moor. Local equivalence of stabilizer states. In *Proceedings of the 16th international symposium on mathematical theory of networks and systems (MTNS)*. K.U. Leuven, Belgium, 2004.

[16] Open problems in quantum information theory. http://www.imaph.tu-bs.de/qi/problems/.

[17] E. Rains. Quantum codes of minimum distance two. *IEEE Trans. Inform. Theory*, 45(1):266–271, 1999. quant-ph/9704043.

[18] 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.

[19] In fact, we show that this result is true for arbitrary stabilizer codes.

[20] This definition is introduced for technical reasons. If the support of a stabilizer on n qubits is strictly contained within the set $\{1, \ldots, n\}$, then the associated code can be written as the product of a code on fewer qubits and the identity matrix. Therefore, for any reasonable application it makes no sense to consider stabilizers not having full support. This definition is however introduced here to facilitate the induction argument made in the proof of theorem 2.

[21] Let R_i be the ith column of R; then $(R^T\theta R)_{ii}$ is equal to $R_i^T\theta R_i$; now, as θ is ZDS one has $x^T\theta x = 0$ for every $x \in \mathbb{F}_2^n$, and therefore $(R^T\theta R)_{ii} = 0$ for every i. This shows that $R^T\theta R$ is ZDS