C[subscript 3], semi-clifford and generalized semi-clifford operations

$\mathcal{C}_3$, Semi-Clifford and Generalized Semi-Clifford Operations

Salman Beigi* Peter W. Shor†

Abstract

Fault-tolerant quantum computation is a basic problem in quantum computation, and teleportation is one of the main techniques in this theory. Using teleportation on stabilizer codes, the most well-known quantum codes, Pauli gates and Clifford operators can be applied fault-tolerantly. Indeed, this technique can be generalized for an extended set of gates, the so called $\mathcal{C}_k$ hierarchy gates, introduced by Gottesman and Chuang (Nature, 402, 390-392). $\mathcal{C}_k$ gates are a generalization of Clifford operators, but our knowledge of these sets is not as rich as our knowledge of Clifford gates. Zeng et al. in (Phys. Rev. A 77, 042313) raise the question of the relation between $\mathcal{C}_k$ hierarchy and the set of semi-Clifford and generalized semi-Clifford operators. They conjecture that any $\mathcal{C}_k$ gate is a generalized semi-Clifford operator. In this paper, we prove this conjecture for $k = 3$. Using the techniques that we develop, we obtain more insight on how to characterize $\mathcal{C}_3$ gates. Indeed, the more we understand $\mathcal{C}_3$, the more intuition we have on $\mathcal{C}_k$, $k \geq 4$, and then we have a way of attacking the conjecture for larger k.

1 Introduction

The theory of fault-tolerant quantum computation is one of the main parts of the theory of quantum computation. In this theory we are introducing a quantum code, a universal set of gates, and then a method to apply these gates fault-tolerantly [1]. The most important quantum codes are quantum stabilizer codes, and teleportation is an idea to apply a universal set of quantum gates on these codes [2].

It is well-known that all Pauli gates as well as Clifford operators can be applied fault-tolerantly using teleportation. However, these are not the only gates with such a property. Indeed, a Clifford operator can be applied fault-tolerantly via teleportation because by conjugation it sends the Pauli group to itself. Generalizing this idea, we can define the so called $\mathcal{C}_k$ hierarchy operators.

Definition 1.1 *Let $\mathcal{P} = \mathcal{C}_1$ denote the Pauli group. For $k \geq 1$ define*

$$\mathcal{C}_{k+1} = \{U : \ U\mathcal{P}U^\dagger \subseteq \mathcal{C}_k\}. \tag{1}$$

Gottesman and Chuang in [2] introduce these sets and show that all $\mathcal{C}_k$ gates can be applied fault-tolerantly via teleportation. However, our knowledge of these operators is poor.

By definition, $\mathcal{C}_2$ is the Clifford group, and there is a rich theory for characterizing and representing these operators [3]. Also, by definition $\mathcal{C}_k \subseteq \mathcal{C}_{k+1}$. But for $k \geq 3$, $\mathcal{C}_k$ is no

*Institute for Quantum Information, California Institute of Technology, Pasadena, CA
†Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA

longer a group [4], and because of that, the problem of studying $\mathcal{C}_k$ hierarchy turns out to be a hard one. However, if we restrict ourselves to diagonal gates in $\mathcal{C}_k$, it is a group [4].

Let us think of the diagonal gates in another direction. If $U \in \mathcal{C}_k$ is diagonal, then U commutes with all σ_z operators, and then $U\mathcal{P}U^\dagger$ contains a maximal abelian subgroup of $\mathcal{P}$. Also, for such a U, it is not hard to see that Q_1UQ_2 is in $\mathcal{C}_k$ and satisfies the same property for all Clifford operators Q_1 and Q_2. This observation leads us to the following definition.

Definition 1.2 *A unitary operator U acting on n qubits is called semi-Clifford if $U\mathcal{P}U^\dagger$ contains a maximal abelian subgroup of $\mathcal{P}$. In other words, U, under conjugation, sends a maximal abelian subgroup of $\mathcal{P}$ to another maximal abelian subgroup of $\mathcal{P}$.*

Semi-Clifford operators are first defined in [5] for one qubit operators, and are generalized for n qubits in [4]. Also in [4], Zeng et al. raise the question of the relation between semi-Clifford operators and $\mathcal{C}_k$ hierarchy. They show that all $\mathcal{C}_k$ hierarchy gates are semi-Clifford if $n = 1, 2$ (n is the number of qubits). For $n = 3$ they prove the same property if $k = 3$, and propose the following conjecture for larger n.

Conjecture 1.1 [4] *All gates in $\mathcal{C}_3$ are semi-Clifford operations.*

Moreover, for $k \geq 4$ by giving an example they show that there are gates in $\mathcal{C}_k$ which are not semi-Clifford. But they realize that those gates are *generalized semi-Clifford*.

Definition 1.3 *A generalized semi-Clifford operator on n qubits is defined to send, by conjugation, the linear span of at least one maximal abelian subgroup of $\mathcal{P}$ to the linear span of another maximal abelian subgroup of $\mathcal{P}$.*

Clearly, any semi-Clifford operator is generalized semi-Clifford. But we can think of an abelian group of 2^n diagonal matrices which are all linearly independent and are different from σ_z gates; then, the span of this group is the same as the span of all σ_z operators in $\mathcal{P}$. Thus, semi-Clifford and generalized semi-Clifford operators are not the same.

Here is the second conjecture made in [4].

Conjecture 1.2 [4] *All gates in $\mathcal{C}_k$ are generalized semi-Clifford operations.*

The main result of this paper is that Conjecture 1.2 holds for $k = 3$.

Theorem 1.1 *Every gate in $\mathcal{C}_3$ is generalized semi-Clifford.*

1.1 Related works

Gottesman and Mochon (personal communication) have disproved Conjecture 1.1, i.e. they have found a gate in $\mathcal{C}_3$ which is not semi-Clifford. Here we briefly discuss their counterexample.

Consider seven qubits and call them $A_1, A_2, A_3, B_1, B_2, B_2$, and R. Let U be the multiplication of the three controlled-swap gates which act on (R, A_i, B_i), $i = 1, 2, 3$ (it swaps A_i and B_i if R is $|1\rangle$). Also, let V be the multiplication of four controlled-σ_z gates which act on (A_1, A_2, A_3), (A_1, B_2, B_3), (B_1, A_2, B_3), and (B_1, B_2, A_3). By computing the action of UV on Pauli matrices it can be seen that $UV \in \mathcal{C}_3$; however, VU is not in $\mathcal{C}_3$ since $(VU)\sigma_x(VU)^\dagger$, where σ_x acts on qubit R, does not belong to $\mathcal{C}_2$.

Now, we claim that UV is a $\mathcal{C}_3$ gate which is not semi-Clifford. Suppose UV is semi-Clifford; then, by Proposition 1 of [4] there are Clifford operations Q_1, Q_2 such that $D =$

Q_1UVQ_2 is diagonal. On the other hand, since UV is in $\mathcal{C}_3$, $D \in \mathcal{C}_3$, which means that $D\mathcal{P}D^\dagger \subseteq \mathcal{C}_2$. Note that, for any $\sigma \in \mathcal{P}$ and $Q \in \mathcal{C}_2$, $\bar{\sigma}$ and $\bar{Q}$ (the entry-wise complex conjugate of σ and Q) also belong to $\mathcal{P}$ and $\mathcal{C}_2$, respectively. Hence, $D\mathcal{P}D^\dagger \subseteq \mathcal{C}_2$ implies $\bar{D}\mathcal{P}D^T \subseteq \mathcal{C}_2$, or equivalently $\bar{D} = D^\dagger = Q_2^\dagger VUQ_1^\dagger \in \mathcal{C}_3$. Therefore, VU is in $\mathcal{C}_3$, which is a contradiction.

1.2 Structure of the paper

In Section 2, we fix some notations on Pauli operators and then review the characterization of Clifford operations from [3], which represents each Clifford gate by a C-matrix (a symplectic matrix) and an h-vector over the binary field.

In Section 3, we formulate our main idea for proving Theorem 1.1, which is to express the whole assumptions in terms of some relations on C-matrices and h-vectors.

In Section 4, we reduce the problem to a special case where C-matrices contain a block of zeros, which is easier to handle.

In Section 5, we are trying to obtain more information from the representation of Clifford operations based on C-matrices and h-vectors. Indeed, C and h characterize Clifford operators up to an overall phase. Thus, having C and h, we should be able to determine entries of a Clifford operator as a matrix, up to an overall phase. In Section 5, we explicitly find the matrix representation of Clifford operations in the special case introduced in Section 4. The generalization of these results are studies in Appendix A, in which each Clifford operator is expressed as a linear combination of Pauli matrices, and the coefficients of this expansion are computed.

In Section 6, we find a formula that given two Clifford operators Q and Q' represented by (C, h) and (C', h'), respectively, expresses whether $QQ' = Q'Q$ or $QQ' = -Q'Q$. Notice that this is a valid question since the representation of Clifford operations by C-matrices and h-vectors, is independent of an overall phase, and cannot distinguish $Q'Q$ and $-Q'Q$.

In Section 7, we put all pieces together and finish the proof of Theorem 1.1.

2 Preliminaries

2.1 Pauli operators

First of all let us fix some notations for Pauli matrices.

$$\sigma_{00} = \tau_{00} = \sigma_0 = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}, \qquad \sigma_{01} = \tau_{01} = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2}$$

$$\sigma_{10} = \tau_{10} = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad i\sigma_{11} = \tau_{11} = i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{3}$$

Pauli operators over n qubits are denoted by σ_a and τ_a, where $a = \begin{pmatrix} v \\ w \end{pmatrix}$ is in $\mathbf{Z}_2^{2n}$ and

$$\sigma_a = \sigma_{v_1 w_1} \otimes \cdots \otimes \sigma_{v_n w_n}, \tag{4}$$

$$\tau_a = \tau_{v_1 w_1} \otimes \cdots \otimes \tau_{v_n w_n}. \tag{5}$$

Also, we represent the phases $\pm 1, \pm i$ by $i^\delta(-1)^\epsilon$, where $\delta, \epsilon \in \mathbf{Z}_2$. Then, it is easy to see that the multiplication of two Pauli operators $\big(i^{\delta_1}(-1)^{\epsilon_1}\tau_{a_1}\big)\big(i^{\delta_2}(-1)^{\epsilon_2}\tau_{a_2}\big)$ is equal to $i^\delta(-1)^\epsilon\tau_a$, where

$$\delta = \delta_1 + \delta_2, \tag{6}$$

$$\epsilon = \epsilon_1 + \epsilon_2 + \delta_1\delta_2 + a_2^T J\, a_1, \tag{7}$$

$$a = a_1 + a_2, \tag{8}$$

in which T denotes the transposed matrix,

$$J = \begin{pmatrix} 0 & I_n \\ 0 & 0 \end{pmatrix}, \tag{9}$$

and I_n is the identity matrix of size n. As a result,

$$\tau_a \tau_b = (-1)^{b^T P a} \tau_b \tau_a, \tag{10}$$

where

$$P = J + J^T = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}. \tag{11}$$

2.2 Clifford operators

Assume that Q is a Clifford operator. By definition for each Pauli matrix τ_a, $Q\tau_a Q^\dagger$ is also a Pauli operator. According to Eq. (8) and

$$Q\tau_{a_1}\tau_{a_2}Q^\dagger = (Q\tau_{a_1}Q^\dagger)(Q\tau_{a_2}Q^\dagger) \tag{12}$$

to compute the image of Pauli operators under conjugation by Q, it is sufficient to know $Q\tau_{e_j}Q^\dagger$, $j = 1, \ldots, 2n$, where $\{e_1, \ldots, e_{2n}\}$ is the standard basis of $\mathbf{Z}_2^{2n}$ (all coordinates of e_j are 0 except the j-th which is 1). Hence, assume that $Q\tau_{e_j}Q^\dagger = i^{d_j}(-1)^{h_j}\tau_{c_j}$, where $d, h \in \mathbf{Z}_2^{2n}$, and $c_j \in \mathbf{Z}_2^{2n}$. Notice that τ_{e_j} and then $Q\tau_{e_j}Q^\dagger$ are hermitian, so d_j can be determined in terms of c_j; $d_j = c_j^T J\, c_j$. Thus, if we define a $2n \times 2n$ matrix C whose j-th column is equal to c_j, then

$$d = diag(C^T J\, C), \tag{13}$$

where $diag(M)$ denotes a vector whose j-th coordinate is the j-th entry on the diagonal of M.

Now, using the matrix C and Eq. (12) we can compute $Q(i^{\delta_1}(-1)^{\epsilon_1}\tau_{a_1})Q^\dagger$ in terms of C and h. In fact, $Q(i^{\delta_1}(-1)^{\epsilon_1}\tau_{a_1})Q^\dagger = i^{\delta_2}(-1)^{\epsilon_2}\tau_{a_2}$ where

$$\begin{aligned} a_2 &= Ca_1, && (14)\\ \delta_2 &= \delta_1 + d^T a_1, && (15)\\ \epsilon_2 &= \epsilon_1 + h^T a_1 + a_1^T lows(C^T J\, C + dd^T)a_1 + \delta_1 d^T a_1, && (16) \end{aligned}$$

in which $lows(M)$ denotes the strictly lower triangular part of matrix M.

In order to determine the conditions that C and h should satisfy, note that if τ_a and τ_b commute, then their image under conjugation by Q, commute as well. Therefore, by Eqs. (10) and (14), the map $a \to Ca$ should preserve the *symplectic inner product*, i.e. $a^T C^T P C b = a^T P b$, or equivalently

$$C^T P C = P. \tag{17}$$

Matrices C that satisfy Eq. (17) are called *symplectic*.

Dehaene and De Moor prove the following theorem in [3].

Theorem 2.1 [3] *For any symplectic matrix C (satisfying Eq. (17)) and any vector h over $\mathbf{Z}_2$, there is a unique (up to a phase) Clifford operator Q such that $Q(i^{\delta_1}(-1)^{\epsilon_1}\tau_{a_1})Q^\dagger = i^{\delta_2}(-1)^{\epsilon_2}\tau_{a_2}$ where a_2, δ_2 and ϵ_2 are given by Eqs. (14)-(16).*

According to this theorem any Clifford operator Q can be represented by a pair (C, h), where C is a symplectic matrix. Then, to get a full representation of Clifford operators as a group, it is sufficient to compute the inverse and product of these operators based on C-matrices and h-vectors.

Theorem 2.2 [3]

(a) *Given* (C_1, h_1) *and* (C_2, h_2) *defining two Clifford operators* Q_1 *and* Q_2*, respectively, the product* $Q_{12} = Q_2 Q_1$ *is represented by* (C_{12}, h_{12}) *such that*

$$\begin{aligned} C_{12} &= C_2 C_1, && (18)\\ h_{12} &= h_1 + C_1^T h_2 + diag(C_1^T lows(C_2^T J\, C_2 + d_2 d_2^T) C_1 + d_1 d_2^T C_1), && (19) \end{aligned}$$

where d_1 *and* d_2 *are defined in Eq. (13).*

(b) *Given* (C, h) *defining a Clifford operator* Q*, the inverse* $Q' = Q^{-1}$ *is represented by* (C', h') *such that*

$$\begin{aligned} C' &= C^{-1}, && (20)\\ h' &= C^{-T} h + diag(C^{-T} lows(C^T J\, C + dd^T) C^{-1} + d' d^T C^{-1}), && (21) \end{aligned}$$

where $M^{-T} = (M^{-1})^T$*, and* $d' = diag(C^{-T} J\, C^{-1})$*.*

Theorems 2.1 and 2.2 give a full representation of Clifford group. However, this representation is up to a phase, i.e. two Clifford operations that differ only on a global phase have the same C-matrix and h-vector.

As the last remark on this representation notice that each Pauli operator is a Clifford gate as well. So, we can represent it by a C-matrix and an h-vector. Also, by Eq. (10) every two Pauli matrices either commute or anti-commute. Therefore, the C-matrix for all Pauli operators is identity. More explicitly, the Pauli operator τ_a corresponds to $(C = I_{2n}, h = Pa)$.

3 Main ideas

In this section, we formulate our main idea for proving Theorem 1.1. Let U be a $\mathcal{C}_3$ gate on n qubits. Then, by definition $U\mathcal{P}U^\dagger$ is a subset of Clifford group, so if we define $Q_i = U\sigma_{e_i}U^\dagger$, $i = 1, \ldots, 2n$, then Q_i is a Clifford gate and

$$\begin{aligned} Q_i^2 &= I, && (22)\\ Q_i\, Q_j &= (-1)^{\delta_{i+n,j}}\, Q_j\, Q_i, && (23) \end{aligned}$$

where $\delta_{i+n,j}$ is the Kronecker delta function, and $i \le j$.

Conversely, let $Q_1, \ldots, Q_{2n}$ be Clifford operators that satisfy Eqs. (22) and (23). Then, $Q_1, \ldots, Q_n$ commute, and they have a common eigenvector $|\alpha\rangle$ with eigenvalues $+1$ or -1. Let $Q_i|\alpha\rangle = (-1)^{\lambda_i}|\alpha\rangle$, for $i = 1, \ldots, n$, where $\lambda_i \in \mathbf{Z}_2$. Define the linear operator U by

$$U|x_1 \ldots x_n\rangle = Q_{n+1}^{x_1+\lambda_1} \ldots Q_{2n}^{x_n+\lambda_n}|\alpha\rangle, \qquad (24)$$

for every standard basis vector $|x_1 \ldots x_n\rangle$, where $x_1, \ldots, x_n \in \mathbf{Z}_2$.

We claim that U is unitary and $Q_i = U\sigma_{e_i}U^\dagger$ for every i. Since all Q_i's are unitary, the vectors $U|x_1 \ldots x_n\rangle$ are normal. Also, if $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ are different, say at the first coordinate $(x_1 + y_1 = 1)$, then

$$\begin{aligned} \langle x_1 \ldots x_n|U^\dagger U|y_1 \ldots y_n\rangle &= \langle\alpha|Q_{n+1}^{x_1+y_1} \ldots Q_{2n}^{x_n+y_n}|\alpha\rangle\\ &= (-1)^{\lambda_1}\langle\alpha|Q_1 Q_{n+1}^{x_1+y_1} \ldots Q_{2n}^{x_n+y_n}|\alpha\rangle\\ &= -(-1)^{\lambda_1}\langle\alpha|Q_{n+1}^{x_1+y_1} \ldots Q_{2n}^{x_n+y_n} Q_1|\alpha\rangle\\ &= -\langle\alpha|Q_{n+1}^{x_1+y_1} \ldots Q_{2n}^{x_n+y_n}|\alpha\rangle\\ &= -\langle x_1 \ldots x_n|U^\dagger U|y_1 \ldots y_n\rangle. && (25) \end{aligned}$$

Thus, $\langle x_1 \dots x_n | U^\dagger U | y_1 \dots y_n \rangle = 0$ and U is unitary. $Q_i = U \sigma_{e_i} U^\dagger$ can be proved by showing that the action of $U^\dagger Q_i U$ on the basis vectors is equal to the action of σ_{e_i}.

This observation shows that any C_3 gate corresponds to a subgroup of the Clifford group which is isomorphism to the Pauli group, and vice versa. Also, it suggests to study subgroups of Clifford group, isomorphic to Pauli group, instead of $\mathcal{C}_3$ gates directly.

Theorem 3.1 *Theorem 1.1 is equivalent to the following:*

Let $\mathcal{G}$ be a subgroup of the Clifford group which is isomorphic to the Pauli group. Then there exist maximal abelian subgroups $\mathcal{H} \subset \mathcal{G}$ and $\mathcal{H}' \subset \mathcal{P}$ such that the linear span of $\mathcal{H}$ is equal to the linear span of $\mathcal{H}'$. □

To proceed through this idea, let the group $\mathcal{G}$ be generated by Clifford operations $Q_1, \dots, Q_{2n}$ that satisfy Eqs. (22) and (23). As a Clifford operator, let Q_i be represented by the pair (C_i, h_i), $i = 1, \dots, 2n$. Then according to Theorem 2.2, Eq. (22) implies

$$C_i^2 = I, \tag{26}$$

$$h_i + C_i^T h_i + diag(C_i^T lows(C_i^T J C_i + d_i d_i^T) C_i + d_i d_i^T C_i) = 0, \tag{27}$$

and Eq. (23) implies

$$C_i C_j = C_j C_i, \tag{28}$$

$$\begin{aligned} h_i + C_i^T h_j + diag(C_i^T lows(C_j^T J C_j + d_j d_j^T) C_i + d_i d_j^T C_i) \\ = h_j + C_j^T h_i + diag(C_j^T lows(C_i^T J C_i + d_i d_i^T) C_j + d_j d_i^T C_j), \end{aligned} \tag{29}$$

for every i, j.

Notice that representing a Clifford operator by a C-matrix and an h-vector is independent of a global phase. This is why here we do not see the sign of Eq. (23). Indeed, we need another equation, which we call *the sign formula*, to compute this sign and get a full representation of Eqs. (22) and (23).

Unlike Eqs. (26) and (28), Eqs. (27) and (29) are not easy to handle, so we need to somehow reduce these equations to simpler ones.

Let Q be an arbitrary Clifford operator represented by the pair (C, h). Define $Q_i' = Q Q_i Q^\dagger$; then, $Q_1', \dots, Q_{2n}'$ satisfy Eqs. (22) and (23) as well, so they generate a subgroup of the Clifford group isomorphic to the Pauli group. Also, since Q sends Pauli operators to Pauli operators under conjugation, proving the claim in Theorem 3.1 for the group generated by $\{Q_i' : i = 1, \dots, 2n\}$, implies the theorem for the group generated by $\{Q_i : i = 1, \dots, 2n\}$.

This argument shows that in Eqs. (26)-(29), we can replace the symplectic matrices $C_1, \dots, C_{2n}$ by $CC_1C^{-1}, \dots CC_{2n}C^{-1}$ for every symplectic matrix C. Here we use the fact that every symplectic matrix corresponds to the C-matrix of some Clifford operation Q (Theorem 2.1), and the formulas for the C-matrix of the inverse and multiplication of Clifford operators (Theorem 2.2).

4 Symplectic involutions

In the previous section we see that each of the symplectic matrices C_i is an involution ($C_i^2 = I$). Therefore, if C_i was a matrix in a field of characteristic different from 2, C_i was diagonalizable with $+1, -1$ on the diagonal. In fact, a stronger property holds; it is proved in [6] that for any commutative set of symplectic involutions over a field of characteristic $\neq 2$, there exists a symplectic matrix M such that MCM^{-1} is diagonal with $+1, -1$ diagonal entries, for every matrix C in the set.

Here, all the symplectic involutions are over $\mathbf{Z}_2$, and the above proposition does not hold anymore. However, following almost the same steps as in [6], an analogous result can be proved.

Theorem 4.1 *For every symplectic involution C of size $2n$ over $\mathbf{Z}_2$ there exists a symplectic matrix M such that*

$$MCM^{-1} = \begin{pmatrix} I & E \\ 0 & I \end{pmatrix}, \tag{30}$$

where E is a symmetric matrix ($E^T = E$).

Proof: Let us consider the block form of C

$$C = \begin{pmatrix} A & E \\ F & B \end{pmatrix}, \tag{31}$$

where A, B, E and F are $n \times n$ matrices. $C^2 = I$ and $C^T P C = P$. Then $PC = C^T P$, or equivalently PC is symmetric. In other words, $B = A^T$, and E and F are symmetric. Therefore,

$$C = \begin{pmatrix} A & E \\ F & A^T \end{pmatrix}. \tag{32}$$

Also, $C^2 = I$ gives AE and FA are symmetric and $A^2 + EF = I$.

Assume that $rank(E) = r$. Then there is an invertible matrix R such that

$$RER^T = \begin{pmatrix} e & 0 \\ 0 & 0 \end{pmatrix}, \tag{33}$$

where e is a full-rank matrix of size $r \times r$. Since E is symmetric, e is symmetric as well.

Now notice that

$$M_1 = \begin{pmatrix} R & 0 \\ 0 & R^{-T} \end{pmatrix} \tag{34}$$

is symplectic and the upper-right block of $M_1 C M_1^{-1}$ is equal to RER^T. So, we may assume that

$$E = \begin{pmatrix} e & 0 \\ 0 & 0 \end{pmatrix}. \tag{35}$$

Let

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \tag{36}$$

where the matrices a_1, a_2, a_3 and a_4 are of sizes $r \times r, r \times (n-r), (n-r) \times r$ and $(n-r) \times (n-r)$, respectively. AE is symmetric and e is invertible; then $a_3 = 0$ and $a_1 e$ is symmetric.

Now define

$$S = \begin{pmatrix} e^{-1}a_1 & e^{-1}a_2 \\ (e^{-1}a_2)^T & 0 \end{pmatrix}, \tag{37}$$

and

$$M_2 = \begin{pmatrix} I & 0 \\ S & I \end{pmatrix}. \tag{38}$$

Since S is symmetric, M_2 is symplectic. Also, the upper-left block of $M_2 C M_2^{-1}$ is equal to

$$\begin{pmatrix} 0 & 0 \\ 0 & a_4 \end{pmatrix}. \tag{39}$$

Hence, we can assume that a_1 and a_2 are zero as well. (Note that in $M_2 C M_2^{-1}$, E remains unchanged.)

Let

$$F = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix}. \tag{40}$$

using $A^2 + EF = I$ we get $a_4^2 = I$, $f_1 = e^{-1}$, $f_2 = 0$, and $f_3 = 0$ since F is symmetric. Then

$$C = \begin{pmatrix} 0 & 0 & e & 0 \\ 0 & a_4 & 0 & 0 \\ e^{-1} & 0 & 0 & 0 \\ 0 & f_4 & 0 & a_4^T \end{pmatrix}. \tag{41}$$

Now, observe that the map

$$\Phi(X, Y) = \begin{pmatrix} u_1 & 0 & u_2 & 0 \\ 0 & v_1 & 0 & v_2 \\ u_3 & 0 & u_4 & 0 \\ 0 & v_3 & 0 & v_4 \end{pmatrix}, \tag{42}$$

where

$$X = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix}, \qquad Y = \begin{pmatrix} v_1 & v_2 \\ v_3 & v_4 \end{pmatrix}, \tag{43}$$

preserves multiplication: $\Phi(X_1X_2, Y_1Y_2) = \Phi(X_1, Y_1)\Phi(X_2, Y_2)$. Hence, according to the above block form of C, it is sufficient to prove the theorem for the special cases

$$C = \begin{pmatrix} 0 & e \\ e^{-1} & 0 \end{pmatrix}, \qquad C = \begin{pmatrix} a & 0 \\ f & a^T \end{pmatrix}. \tag{44}$$

In the first case if we let

$$M = \begin{pmatrix} I & 0 \\ e^{-1} & I \end{pmatrix}, \tag{45}$$

then

$$MCM^{-1} = \begin{pmatrix} I & e \\ 0 & I \end{pmatrix}, \tag{46}$$

and the theorem holds.

In the second case, notice that

$$\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} C \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} = \begin{pmatrix} a^T & f \\ 0 & a \end{pmatrix}. \tag{47}$$

Then if $f \neq 0$, by the same steps as before, we can reduce C to smaller matrices and use induction. Thus, we may assume that $f = 0$, and

$$C = \begin{pmatrix} a^T & 0 \\ 0 & a \end{pmatrix}. \tag{48}$$

Since $C^2 = I$, $a^2 = I$. Hence, there exists an invertible matrix R on $\mathbf{Z}_2$ such that RaR^{-1} is in the Jordan normal form, and it is a block diagonal matrix, each of its blocks is either $I_1 = (1)$ or

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{49}$$

On the other hand,

$$M = \begin{pmatrix} R^{-T} & 0 \\ 0 & R \end{pmatrix} \tag{50}$$

is symplectic and

$$M\,C\,M^{-1} = \begin{pmatrix} R^{-T}a^TR^T & 0 \\ 0 & RaR^{-1} \end{pmatrix}. \tag{51}$$

Therefore, if we prove the theorem for the two cases $a = (1)$ and

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \tag{52}$$

we are done.

In the first case there is nothing to prove, and in the second case we have

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{53}$$

□

Recall that if the characteristic of the field is not 2 we can replace the matrix in Eq. (30) by a diagonal one. Also, a commutative set of symplectic involutions over such a field can be simultaneously transformed to a set of diagonal matrices under a symplectic change of basis [6]. Comparing to this result and based on Theorem 4.1, one may expect that on a field of characteristic 2, we can transform a commutative set of symplectic involutions to matrices of the form of Eq. (30). However, this is not the case; for a counterexample consider the following matrices:

$$C_1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad C_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}. \tag{54}$$

Both C_1 and C_2 are symplectic, $C_1^2 = C_2^2 = I$, and $C_1C_2 = C_2C_1$. If C_1 and C_2 could be transformed to the form of Eq. (30), then $(I + C_1)(I + C_2) = 0$, which does not hold.

Theorem 4.2 *Let $\mathcal{M}$ be a commutative set of symplectic involutions of size $2n \times 2n$ over $\mathbf{Z}_2$. Then there exists a symplectic matrix M such that for every $C \in \mathcal{M}$, MCM^{-1} is of the form*

$$MCM^{-1} = \begin{pmatrix} A & E \\ 0 & A^T \end{pmatrix}, \tag{55}$$

where A and E are $n \times n$ matrices.

Proof: We prove the theorem by induction on n. If $\mathcal{M}$ contains only the identity matrix, then there is nothing to prove. So, let $C \in \mathcal{M}$ be unequal to identity. According to Theorem 4.1, we may assume

$$C = \begin{pmatrix} I & E \\ 0 & I \end{pmatrix}. \tag{56}$$

Also, as in the proof of Theorem 4.1, we may assume

$$E = \begin{pmatrix} e & 0 \\ 0 & 0 \end{pmatrix}, \tag{57}$$

where e is a full-rank symmetric matrix of size $r \times r$.

Let $C' \in \mathcal{M}$ be different from C. If we consider the block form of C'

$$C' = \begin{pmatrix} A' & E' \\ F' & B' \end{pmatrix}, \tag{58}$$

then $B'^T = A'$, and E', F' are symmetric (because C' is symplectic and $C'^2 = I$.) Thus, we may assume

$$C' = \begin{pmatrix} a_1 & a_2 & e_1 & e_2 \\ a_3 & a_4 & e_2^T & e_4 \\ f_1 & f_2 & a_1^T & a_3^T \\ f_2^T & f_4 & a_2^T & a_4^T \end{pmatrix}. \tag{59}$$

Now, writing the constraint $CC' = C'C$, and using the fact that e is full-rank, we conclude that $a_3 = 0$, $f_1 = 0$ and $f_2 = 0$. Hence, every matrix in $\mathcal{M}$ is of the form

$$C' = \begin{pmatrix} a_1 & a_2 & e_1 & e_2 \\ 0 & a_4 & e_2^T & e_4 \\ 0 & 0 & a_1^T & 0 \\ 0 & f_4 & a_2^T & a_4^T \end{pmatrix}. \tag{60}$$

Therefore, if $r = n$, which covers the base case $n = 1$, we are done. So, assume that $n > r \geq 1$.

Suppose we map such a matrix C' to its sub-matrix

$$D' = \begin{pmatrix} a_4 & e_4 \\ f_4 & a_4^T \end{pmatrix}. \tag{61}$$

This map over matrices in the form of Eq. (60) preserves addition and multiplication. Therefore, all matrices D' are symplectic involutions and commute. Thus, by induction we may assume $f_4 = 0$, and we are done. □

The following corollary is a conclusion of the above theorem and the argument at the end of Section 3.

Corollary 4.1 *To prove the claim of Theorem 3.1, it is sufficient to consider the case that the group $\mathcal{G}$ is generated by Clifford operators $Q_1, \ldots, Q_{2n}$ which are represented by pairs $(C_1, h_1), \ldots, (C_{2n}, h_{2n})$ such that*

$$C_i = \begin{pmatrix} A_i & E_i \\ 0 & A_i^T \end{pmatrix}, \tag{62}$$

where $A_i^2 = I$, and E_i and $A_i E_i$ are symmetric. □

5 Clifford operators as linear transformations

In Section 2, we present the characterization of Clifford operators based on how they transform Pauli matrices under conjugation. In this section, we describe these operators as linear transformations.

In Appendix A, a Clifford operator Q, given by a C-matrix and an h-vector, is represented as a linear combination of Pauli matrices, and the coefficients of this expansion are extracted. These results are very general; however, according to Corollary 4.1 for the purpose of proving our main theorem, we may assume that the matrix C is in the form of Eq. (62). In the following, we show that in this special case, Q is a permutation times a diagonal matrix. This result is used in Section 6 in order to find a formula which indicates whether two Clifford operators commute or anti-commute ($QQ' = Q'Q$ or $QQ' = -Q'Q$).

Assume that Q is a Clifford gate, represented by the pair (C, h), where $Q^2 = I$ and

$$C = \begin{pmatrix} A & E \\ 0 & A^T \end{pmatrix}, \qquad h = \begin{pmatrix} f \\ g \end{pmatrix}. \tag{63}$$

In this special case we can find a simpler expression for Theorem 2.1. In fact,

$$C^T J C = \begin{pmatrix} 0 & 0 \\ 0 & AE \end{pmatrix}, \tag{64}$$

and

$$d = diag(C^T J C) = \begin{pmatrix} 0 \\ d_0 \end{pmatrix}, \tag{65}$$

where $d_0 = diag(AE)$. Thus,

$$Q\tau_a Q = (i)^{d_0^T a_2} (-1)^{h^T a + a_2^T lows(AE + d_0 d_0^T) a_2} \, \tau_{Ca}, \tag{66}$$

where

$$a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}. \tag{67}$$

Also, since $Q^2 = I$ by Eq. (27),

$$A^T f = f. \tag{68}$$

Let $\{\, |x\rangle : x \in \mathbf{Z}_2^n \}$ be the standard basis for the Hilbert space of n qubits. Then we have

$$\tau_a |x\rangle = (-1)^{a_1^T (x + a_2)} |x + a_2\rangle. \tag{69}$$

Let $a_2 = 0$. By Eq. (66)

$$\tau_a Q \, |x\rangle = Q \, (Q \tau_a Q) \, |x\rangle = Q (-1)^{f^T a_1} \tau_{Ca} \, |x\rangle,$$

and by Eq. (69)

$$\tau_a Q \, |x\rangle = (-1)^{f^T a_1} (-1)^{a_1^T A^T x} Q \, |x\rangle = (-1)^{a_1^T (f + A^T x)} Q \, |x\rangle. \tag{70}$$

As a result, $Q|x\rangle$ is the simultaneous eigenvector of all τ_a, where $a_2 = 0$, with eigenvalue $(-1)^{a_1^T (f + A^T x)}$. Therefore, there exists λ_x such that

$$Q \, |x\rangle = \lambda_x \, |f + A^T x\rangle. \tag{71}$$

This equation shows that the action of Q on standard basis vectors is the same as a permutation with some phases λ_x. So, if we could compute these phases, then we had a complete characterization of Q as a linear operator.

Let b be such that $b_1 = 0$. By Eq. (71),

$$\tau_b Q\,|0\rangle = \lambda_0 \tau_b |f\rangle = \lambda_0 |f + b_2\rangle. \tag{72}$$

Hence,

$$\lambda_0 Q\,|f + b_2\rangle = Q\tau_b Q\,|0\rangle. \tag{73}$$

Equivalently,

$$\begin{aligned}
\lambda_0\lambda_{f+b_2}|f + A^T(f + b_2)\rangle &= (i)^{d_0^T b_2}(-1)^{g^T b_2 + b_2^T lows(AE+d_0 d_0^T)b_2}\,\tau_{Cb}\,|0\rangle \\
&= (i)^{d_0^T b_2}(-1)^{g^T b_2 + b_2^T lows(AE+d_0 d_0^T)b_2}\,(-1)^{b_2^T AEb_2}\,|A^T b_2\rangle \\
&= (i)^{d_0^T b_2}(-1)^{d_0^T b_2 + g^T b_2 + b_2^T lows(AE+d_0 d_0^T)b_2}\,|A^T b_2\rangle,
\end{aligned} \tag{74}$$

where in the last equation we use $b_2^T AEb_2 = d_0^T b_2$. Therefore, by $A^T f = f$ we obtain

$$\lambda_0\lambda_{f+y} = (i)^{d_0^T y}(-1)^{d_0^T y + g^T y + y^T lows(AE+d_0 d_0^T)y}, \tag{75}$$

which determines entries of Q up to an overall sign.

Theorem 5.1 *Let Q be a Clifford operator, represented by C, h which are given by Eq. (63), and let $Q^2 = I$. Then, the action of Q on standard basis vectors is described by Eq. (71), where λ_x's are phases that can be computed by Eq. (75).* □

6 Sign formula

Recall that in Eqs. (26)-(29) we express equations $Q_i^2 = Q_j^2 = I$ and $Q_iQ_j = \pm Q_jQ_i$ for two Clifford operations Q_i and Q_j, in terms of their C-matrices and h-vectors. However, these formulas are independent of the plus or minus sign, so we need another formula, which we call the sign formula, to recognize two cases $Q_iQ_j = Q_jQ_i$ and $Q_iQ_j = -Q_jQ_i$.

Suppose $Q = Q_i$ and $Q' = Q_j$ are represented by ($C = C_i, h = h_i$) and ($C' = C_j, h' = h_j$), respectively, and satisfy Eqs. (26)-(29). Following Corollary 4.1, let us assume

$$C = \begin{pmatrix} A & E \\ 0 & A^T \end{pmatrix}, \qquad C' = \begin{pmatrix} A' & E' \\ 0 & A'^T \end{pmatrix}, \tag{76}$$

where $A^2 = A'^2 = I$. Also, let

$$h = \begin{pmatrix} f \\ g \end{pmatrix}, \qquad h' = \begin{pmatrix} f' \\ g' \end{pmatrix}. \tag{77}$$

Then by Eq. (29) we have $f + A^T f' = f' + A'^T f$, or equivalently

$$(I + A^T)f' = (I + A'^T)f. \tag{78}$$

According to Eq. (71)

$$Q'Q\,|0\rangle = Q'\lambda_0\,|f\rangle = \lambda_0\lambda'_f\,|f' + A'^T f\rangle. \tag{79}$$

Similarly, $QQ'|0\rangle = \lambda_{f'}\lambda'_0\,|f + A^T f'\rangle$. Therefore, we conclude that $Q'Q = -QQ'$ if and only if $\lambda_0\lambda'_f = -\lambda'_0\lambda_{f'}$, or equivalently

$$(\lambda_0^2)(\lambda'_0\lambda'_f) = -(\lambda_0'^2)(\lambda_0\lambda_{f'}). \tag{80}$$

Now note that using Eq. (75) we can explicitly compute all the terms in this equation. As a result, the sign in $Q'Q = \pm QQ'$ can be determined in terms of C, h, C', and h'. We do not express this formula here because of its complexity; however, it is clear from Eq. (80) that if $f = f' = 0$, then Q and Q' commute.

Lemma 6.1 *Suppose Q and Q' are represented by Eqs. (76) and (77), and satisfy $Q^2 = Q'^2 = I$ and $QQ' = \pm Q'Q$. Then, if $f = f' = 0$, $QQ' = Q'Q$.* □

7 Proof of Theorem 1.1

Using Theorem 3.1, let $\mathcal{G}$ be a subgroup of the Clifford group, isomorphic to the Pauli group. Suppose that $\mathcal{G}$ is generated by $Q_1, \ldots, Q_{2n}$ which are represented by pairs

$$(C_1, h_1), \ldots, (C_{2n}, h_{2n}), \tag{81}$$

respectively, and satisfy Eqs. (22) and (23), and then (26)-(29). By Corollary 4.1, we may assume that

$$C_i = \begin{pmatrix} A_i & E_i \\ 0 & A_i^T \end{pmatrix}, \qquad h_i = \begin{pmatrix} f_i \\ g_i \end{pmatrix}. \tag{82}$$

We prove that there exists a maximal abelian subgroup $\mathcal{H}$ of $\mathcal{G}$ such that all of matrices in $\mathcal{H}$ are diagonal. In that case, the linear span of $\mathcal{H}$ would be equal to the linear span of the group generated by all σ_z operators (which is a maximal abelian subgroup of the Pauli group), and we are done.

Define the map $T : \mathbf{Z}_2^{2n} \to \mathbf{Z}_2^n$ that sends $x = (x_1, \ldots, x_{2n})$ to the f-vector of the Clifford operator $Q_1^{x_1} \ldots Q_{2n}^{x_{2n}}$. (By f-vector we mean the upper part of its h-vector.) T is not linear but *almost linear*.

Lemma 7.1

(i) *$Ker\, T = T^{-1}(0)$ is a linear subspace of $\mathbf{Z}_2^{2n}$.*

(ii) *For any x and x', where $T(x) = T(x')$, $x + x' \in Ker\, T$.*

(iii) *If $y \in Ker\, T$, then $T(x + y) = T(x)$, for any x.*

(iv) *For every $y \in \mathbf{Z}_2^n$, $T^{-1}(y)$ is either empty or equal to $x + Ker\, T$, for some $x \in \mathbf{Z}_2^{2n}$.*

(v) $|Ker\, T|.|Im\, T| = 2^{2n}$

Proof: Define $\mathcal{Q}_x = Q_1^{x_1} \ldots Q_{2n}^{x_{2n}}$ and $\mathcal{A}_x = A_1^{x_1} \ldots A_{2n}^{x_{2n}}$.

(i) We should show that if the f-vectors of $\mathcal{Q}_x$ and $\mathcal{Q}_{x'}$ are both zero, then the f-vector of $\mathcal{Q}_{x+x'} = \pm \mathcal{Q}_x \mathcal{Q}_{x'}$ is also zero. By Theorem 2.2 the f-vector of $\mathcal{Q}_x \mathcal{Q}_{x'}$ is equal to $T(x) + \mathcal{A}_x^T T(x') = 0$.

(ii) Let $T(x) = T(x')$. Then, again by Theorem 2.2 and Eq. (68)

$$T(x + x') = T(x) + \mathcal{A}_x^T T(x') = T(x) + \mathcal{A}_x^T T(x) = 0. \tag{83}$$

Thus, $x + x'$ is in $Ker\, T$.

(iii) $T(x + y) = T(x) + \mathcal{A}_x^T T(y) = T(x)$.

(iv) and (v) are clear from (ii) and (iii). □

Lemma 7.2 *$dim\, Ker\, T = n$, and T is surjective.*

Proof: By the previous lemma, $|Ker\, T|.|Im\, T| = 2^{2n}$, so if we prove $dim\, Ker\, T = n$, then T would be surjective automatically.

$|Im\, T| \leq 2^n$, then $|Ker\, T| \geq 2^n$, or equivalently $\dim Ker\, T = r \geq n$.

Let $x, x' \in Ker\, T$, so by definition, the f-vector of $\mathcal{Q}_x$ and $\mathcal{Q}_{x'}$ are both zero. Thus, by Lemma 6.1, $\mathcal{Q}_x$ and $\mathcal{Q}_{x'}$ commute. Therefore, since by Lemma 7.1, $Ker\, T$ is a linear subspace, $\mathcal{H} = \{\pm \mathcal{Q}_x, \pm i \mathcal{Q}_x : x \in Ker T\}$ is an abelian subgroup of $\mathcal{G}$. On the other hand, every maximal abelian subgroup of the Pauli group is of size 4×2^n. (The factor 4 is duo to the phases ± 1 and $\pm i$.) Hence, $4 \times 2^r = |\{\pm \mathcal{Q}_x, \pm i \mathcal{Q}_x : x \in Ker T\}| \leq 4 \times 2^n$. As a result, $dim\, Ker\, T = r = n$. □

This lemma and its proof show that $\mathcal{H}$ is a maximal abelian subgroup of $\mathcal{G}$.

Lemma 7.3 *$\mathcal{A}_x = I$, for any $x \in Ker\, T$.*

Proof: By Eq. (78), if $x \in Ker\, T$, we have

$$(I + \mathcal{A}_x^T)T(y) = (I + \mathcal{A}_y^T)T(x) = 0, \tag{84}$$

for every y. On the other hand, by Lemma 7.2, T is surjective; thus, $(I + \mathcal{A}_x^T)y = 0$, for every vector y. Equivalently, $\mathcal{A}_x = I$. □

Now, we are ready to finish the proof. $\mathcal{H}$ is a maximal abelian group of $\mathcal{G}$ which is a group isomorphic to the Pauli group. Therefore, if we show that all elements of $\mathcal{H}$ are diagonal, the linear span of $\mathcal{H}$ is equal to the linear span of the maximal abelian subgroup of the Pauli group generated by σ_z gates, and then we are done.

Let $x \in Ker\, T$; we prove that $\mathcal{Q}_x$ is diagonal. Using Eq. (71), since the f-vector of $\mathcal{Q}_x$ is zero, and $\mathcal{A}_x = I$, $\mathcal{Q}_x|y\rangle = \lambda_y|y\rangle$, for some λ_y. This equality means that $\mathcal{Q}_x$ is diagonal in the standard basis. We are done.

8 Conclusion

In this paper we develop some techniques to characterize $\mathcal{C}_3$ gates based on the subgroups of the Clifford group isomorphic to the Pauli group. We prove that any such group, after conjugation by a Clifford operation, contains a maximal abelian subgroup, all of whose elements are diagonal. This result proves the conjecture that any $\mathcal{C}_3$ gate is a generalized semi-Clifford gate. Using Proposition 2 of [4], we conclude that any $\mathcal{C}_3$ gate is of the form $Q\Pi\Lambda Q'$, where Π is a permutation, Λ is diagonal, and Q, Q' are Clifford operations. To obtain a deeper understanding of $\mathcal{C}_3$ gates we should characterize all of these groups (subgroups of Clifford group isomorphic to Pauli group). Such a characterization leads us to a better understanding of $\mathcal{C}_3$, and then $\mathcal{C}_k$, $k \geq 4$.

Acknowledgements. Authors are thankful to Carlos Mochon, Daniel Gottesman, and Bei Zeng for providing the counterexample of Conjecture 1.1. They are also grateful to unknown referees for their comments which improved the presentation of the results.

Appendix A

This appendix contains some results regarding the coefficients of the linear expansion of a Clifford operator in terms of Pauli matrices.

Let Q be an arbitrary Clifford operation represented by the pair (C, h). Since Pauli operators consist a basis for the linear space of matrices, there are complex numbers r_a, $a \in \mathbf{Z}_2^{2n}$, such that

$$Q = \sum_a r_a \, (i^{a^T Ja} \, \tau_a). \tag{85}$$

Using Eqs. (14)-(16), for every $b \in \mathbf{Z}_2^{2n}$ we have

$$Q \, \tau_b \, Q^\dagger = (i)^{d^T b} (-1)^{h^T b + b^T lows(C^T JC + dd^T)b} \, \tau_{Cb}, \tag{86}$$

where d is defined by Eq. (13), and then

$$Q\tau_b = (i)^{d^T b} (-1)^{h^T b + b^T lows(C^T JC + dd^T)b} \, \tau_{Cb} Q. \tag{87}$$

Therefore, replacing Q by Eq. (85), we get

$$\sum_a r_a (i)^{a^T J\, a} (-1)^{b^T J\, a} \tau_{a+b} \\ = (i)^{d^T b} (-1)^{h^T b + b^T lows(C^T JC + dd^T) b} \sum_{a'} r_{a'} (i)^{a'^T J\, a'} (-1)^{a'^T J\, Cb} \tau_{a'+Cb}. \quad (88)$$

Equivalently, if $a' = a + b + Cb$, then

$$r_a\, (i)^{a^T J\, a} (-1)^{b^T J\, a} = r_{a'}\, (i)^{d^T b} (i)^{a'^T J\, a'} (-1)^{h^T b + b^T lows(C^T JC + dd^T) b} (-1)^{a'^T J\, Cb}. \quad (89)$$

Suppose b is an eigenvector of C with eigenvalue one ($Cb = b$). Then $a' = a$, and by the above equation if $r_a \neq 0$

$$(-1)^{b^T J\, a} = (i)^{d^T b} (-1)^{h^T b + b^T lows(C^T JC + dd^T) b} (-1)^{a^T J\, b}. \quad (90)$$

Thus, $d^T b$ must be zero.

To see this fact more explicitly, consider the block form of C

$$C = \begin{pmatrix} A & E \\ F & B \end{pmatrix}. \quad (91)$$

Since C is symplectic, $B^T A + E^T F = I$ and $A^T F, E^T B$ are symmetric. Also, $Cb = b$ is equivalent to

$$Ax + Ey = x, \qquad Fx + By = y. \quad (92)$$

where

$$b = \begin{pmatrix} x \\ y \end{pmatrix}. \quad (93)$$

By the definition of d,

$$\begin{aligned} d = diag(C^T JC) &= diag \begin{pmatrix} A^T F & A^T B \\ E^T F & E^T B \end{pmatrix} \\ &= diag \begin{pmatrix} F^T A & F^T E \\ E^T F & E^T B \end{pmatrix} \\ &= diag \left[\begin{pmatrix} F^T & 0 \\ 0 & E^T \end{pmatrix} C \right]. \end{aligned} \quad (94)$$

Since the last matrix is symmetric, and the operations are on a field of characteristic 2, we have

$$d^T b = b^T \begin{pmatrix} F^T & 0 \\ 0 & E^T \end{pmatrix} C\, b = b^T \begin{pmatrix} F^T & 0 \\ 0 & E^T \end{pmatrix} b = x^T F^T x + y^T E^T y. \quad (95)$$

Then we should show that $x^T F^T x + y^T E^T y = 0$. In fact, we can prove a stronger equality:

$$b'^T \begin{pmatrix} F^T & 0 \\ 0 & E^T \end{pmatrix} b = x'^T F^T x + y'^T E^T y = 0,$$

where

$$b' = \begin{pmatrix} x' \\ y' \end{pmatrix} \quad (96)$$

is another eigenvector of C with eigenvalue one.

Using $B^TA + E^TF = I$, we have $y'^TB^TAx + y'^TE^TFx = y'^Tx$, and by Eq. (92) we conclude that

$$\begin{aligned} 0 &= y'^TB^TAx + y'^TE^TFx + y'^Tx \\ &= y'^TB^T(x + Ey) + y'^TE^T(y + By) + y'^Tx \\ &= y'^TB^Tx + y'^TE^Ty + y'^Tx \\ &= y'^TE^Ty + (y'^T + x'^TF^T)x + y'^Tx \\ &= y'^TE^Ty + x'^TF^Tx, \end{aligned} \tag{97}$$

where in the third line we use $B^TE = E^TB$.

Lemma .1 *The map $S(b) = b^T lows(C^TJC + dd^T)b$ that is defined on the set of eigenvectors of C with eigenvalue one is a linear map. As a result, there exists a vector α such that $S(b) = \alpha^Tb$.*

Proof: It is sufficient to show that $b^T lows(C^TJC + dd^T)b' + b'^T lows(C^TJC + dd^T)b = 0$ for two eigenvectors b and b' with eigenvalue one.

$$\begin{aligned} & b^T lows(C^TJC + dd^T)b' + b'^T lows(C^TJC + dd^T)b \\ &= b^T lows(C^TJC + dd^T)b' + b^T lows(C^TJC + dd^T)^Tb' \\ &= b^T \left[lows(C^TJC + dd^T) + lows(C^TJC + dd^T)^T \right] b' \\ &= b^T \left[\begin{pmatrix} F^T & 0 \\ 0 & E^T \end{pmatrix} C + dd^T \right] b' \\ &= b^T \begin{pmatrix} F^T & 0 \\ 0 & E^T \end{pmatrix} b' + b^T dd^T b' \\ &= 0, \end{aligned} \tag{98}$$

where in the fourth line we used the same idea as in Eq. (94), and the fact that $d = diag\,(dd^T)$ which gives

$$diag \left[\begin{pmatrix} F^T & 0 \\ 0 & E^T \end{pmatrix} C + dd^T \right] = 0. \tag{99}$$

□

Now, let us return to Eq. (90). If $r_a \neq 0$, then for any b such that $Cb = b$ we have

$$(-1)^{b^TJ\,a} = (-1)^{h^Tb + b^T lows(C^TJC + dd^T)b}(-1)^{a^TJ\,b}, \tag{100}$$

or equivalently

$$a^TP\,b + h^Tb + b^T lows(C^TJC + dd^T)b = 0. \tag{101}$$

Using Lemma .1, we can write this equality as

$$(Pa + h + \alpha)^Tb = 0. \tag{102}$$

Suppose $dim\,Ker(I + C) = s$, i.e., there are s independent eigenvectors of C with eigenvalue one. Thus, by Eq. (102), there are s independent linear constraints on the vectors a for which $r_a \neq 0$. Therefore, there are at most 2^{2n-s} vectors a such that $r_a \neq 0$. On the other hand, if r_a is non-zero, then by Eq. (89), $r_{a+e} \neq 0$, for every vector e in the image of $I + C$. Moreover, $dim\,Im(I + C) = 2n - s$, and then the number of such vectors e is equal to 2^{2n-s}. This means that all of vectors a' for which $r_{a'}$ is non-zero, are of the form $a' = a + e$ for some $e \in Im(I + C)$.

As a summary, we have the following theorem.

Theorem .1 *Let Q be a Clifford operation represented by the pair (C, h), and let r_a, $a \in \mathbf{Z}_2^{2n}$, be the coefficients of Q as a linear combination of Pauli matrices as in Eq. (85). Also, let α be the vector defined in Lemma .1. Then, r_a is non-zero for $a = P(h + \alpha)$. Moreover, every a' where $r_{a'} \neq 0$, is of the form $a' = P(h + \alpha) + b + Cb$ for some b. In this case, r_a and $r_{a'}$ are related by Eq. (89). In particular, $|r_a| = |r_{a'}|$.* □

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000

[2] D. Gottesman and I. L. Chuang, *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations*, Nature, 402 pp. 390-392, 1999

[3] Jeroen Dehaene, Bart De Moor, *The Clifford group, stabilizer states, and linear and quadratic operations over GF(2)*, Phys. Rev. A 68, 042318 (2003)

[4] Bei Zeng, Xie Chen, Isaac L. Chuang, *Semi-Clifford operations, structure of $\mathcal{C}_k$ hierarchy, and gate complexity for fault-tolerant quantum computation*, Phys. Rev. A 77, 042313 (2008)

[5] D. Gross and M. Van den Nest, *The LU-LC conjecture, diagonal local operations and quadratic forms over GF(2)*, Quantum Inf. Comput. 8, 263 (2008)

[6] Loo-Keng Hua, *On the Automorphisms of the Symplectic Group Over Any Field*, The Annals of Mathematics, Second Series, Vol. 49, No. 4, Oct. 1948, pp. 739-759