Semi-Clifford operations, structure of $\mathcal{C}_k$ hierarchy, and gate complexity for fault-tolerant quantum computation

Bei Zeng, Xie Chen, and Isaac L. Chuang
Department of Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
(Received 15 January 2008; published 16 April 2008)

Teleportation is a crucial element in fault-tolerant quantum computation and a complete understanding of its capacity is very important for the practical implementation of optimal fault-tolerant architectures. It is known that stabilizer codes support a natural set of gates that can be more easily implemented by teleportation than any other gates. These gates belong to the so-called $\mathcal{C}_k$ hierarchy introduced by Gottesman and Chuang [Nature (London) **402**, 390 (1999)]. Moreover, a subset of $\mathcal{C}_k$ gates, called semi-Clifford operations, can be implemented by an even simpler architecture than the traditional teleportation setup [X. Zhou, D. W. Leung, and I. L. Chuang, Phys. Rev. A **62**, 052316 (2000)]. However, the precise set of gates in $\mathcal{C}_k$ remains unknown, even for a fixed number of qubits n, which prevents us from knowing exactly what teleportation is capable of. In this paper we study the structure of $\mathcal{C}_k$ in terms of semi-Clifford operations, which send by conjugation at least one maximal Abelian subgroup of the n-qubit Pauli group into another one. We show that for $n=1,2$, all the $\mathcal{C}_k$ gates are semi-Clifford, which is also true for $\{n=3,k=3\}$. However, this is no longer true for $\{n>2,k>3\}$. To measure the capability of this teleportation primitive, we introduce a quantity called "teleportation depth," which characterizes how many teleportation steps are necessary, on average, to implement a given gate. We calculate upper bounds for teleportation depth by decomposing gates into both semi-Clifford $\mathcal{C}_k$ gates and those $\mathcal{C}_k$ gates beyond semi-Clifford operations, and compare their efficiency.

DOI: 10.1103/PhysRevA.77.042313 PACS number(s): 03.67.Pp, 03.67.Lx

I. INTRODUCTION

The discovery of quantum error-correcting codes and the theory of fault-tolerant quantum computation have greatly improved the long-term prospects for quantum computing technology [1,2]. To implement fault-tolerant quantum computation for a given quantum error-correcting code, protocols for performing fault-tolerant operations are needed. The basic design principle of a fault-tolerant operation protocol is that if only one component in the procedure fails, then the failure causes at most one error in each encoded block of qubits' output from the procedure.

The most straightforward protocol is to use transversal gates whenever possible. A transversal operation has the virtue that an error occurring on the kth qubit in a block can only ever propagate to the kth qubit of other blocks of the code, no matter what other sequence of gates we perform before a complete error-correction procedure [3,4]. Unfortunately, it is widely believed in the quantum information science community that there does not exist a quantum error correcting code, upon which we can perform universal quantum computations using just transversal gates [4], and recently this belief is proved for a special case when the code is a stabilizer code [5].

However, most known quantum codes are stabilizer codes. We therefore have to resort to other techniques, for instance, quantum teleportation [6] or state distillation [7]. The $\mathcal{C}_k$ hierarchy is introduced by Gottesman and Chuang to implement fault-tolerant quantum computation via teleportation [6]. The starting point is, if we can perform the Pauli operations and measurements fault tolerantly, we can then perform all Clifford group operations fault tolerantly by teleportation. We can then use a similar technique to boot strap the way to universal fault-tolerant computation, using teleportation, which gives a $\mathcal{C}_k$ hierarchy of quantum teleportation, as defined below.

Definition 1. The sets $\mathcal{C}_k$ are defined in a recursive way as sets of unitary operations U that satisfy

$$\mathcal{C}_{k+1} = \{U | U\mathcal{C}_1 U^\dagger \subseteq \mathcal{C}_k\}, \quad (1)$$

where $\mathcal{C}_1$ is the Pauli group. We call a unitary operation an n-qubit $\mathcal{C}_k$ gate if it belongs to the set $\mathcal{C}_k$ and acts nontrivially on at most n qubits.

Note by definition $\mathcal{C}_2$ is the Clifford group, which takes the Pauli group into itself. And $\mathcal{C}_k \supset \mathcal{C}_{k-1}$, but $\mathcal{C}_k$ for $k \geq 3$ is no longer a group.

All the gates in $\mathcal{C}_k$ can be performed with the two-bit teleportation scheme (Fig. 1) in a fault-tolerant manner. Because, as proved in [4], it is possible to fault tolerantly prepare the ancilla state $|\Psi_U^n\rangle$, apply the classically controlled correction operation $R'^{\dagger}_{xy}$, and measure in Bell basis on a stabilizer code. However, the precise set of gates which form $\mathcal{C}_k$ is unknown, even for a fixed number of qubits. It is dem-

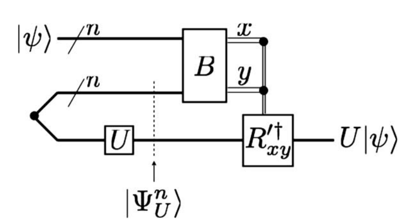

FIG. 1. Two-bit teleportation scheme. "<" denotes an Einstein-Podolsky-Rosen (EPR) pair, B represents Bell-basis measurement, and $R'_{xy} = UR_{xy}U^\dagger$, where R_{xy} is a Pauli operator. The double wires carry classical bits and a single wire carries qubits. Any gate in the $\mathcal{C}_k$ hierarchy can be implemented fault tolerantly using this teleporation scheme.

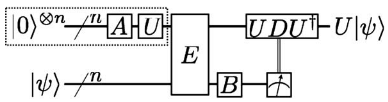

FIG. 2. One-bit teleportation scheme. For Z teleportation, $A=I$, $B=H$, $D=Z$, and E is a CNOT gate with the first qubit as its target. For X teleportation, $A=H$, $B=I$, $D=X$, and E is a CNOT gate with the first qubit as its control. All semi-Clifford $\mathcal{C}_k$ gates can be implemented fault tolerantly using this scheme.

onstrated in [8] that a subset of $\mathcal{C}_k$ gates could be implemented by a different architecture than the standard teleportation, called one-bit teleportation, as shown in Fig. 2. Those gates adopt the form L_1VL_2, where V is a diagonal gate in $\mathcal{C}_k$ and L_1,L_2 are two Clifford operations. Gates of this form are recently studied in literature and are called semi-Clifford operations [9]. In the following we will denote the n-qubit Pauli group as $\mathcal{P}_n$ and a semi-Clifford operation is defined to be a gate which sends at least one maximal Abelian subgroup of $\mathcal{P}_n$ to another maximal Abelian one under conjugation.

Due to the fact that one-bit teleportation needs only half the number of ancilla qubits per teleportation than the standard two-bit teleportation, it is important to understand the difference of capabilities between one- and two-bit teleportation for the practical implementations of fault-tolerant architecture. It is conjectured in [8] that those two capabilities coincide for $\{n=2,k=3\}$, which means that all the $\mathcal{C}_3$ gates for two qubits are semi-Clifford operations.

In this paper, we prove this conjecture for a more general situation where $\{n=1,2,\ \forall k\}$, and $\{n=3,k=3\}$. We then disprove it for parameters $\{n>2,k>3\}$ by explicit construction of counterexamples. We leave open the question for the parameters $\{n>2,k=3\}$, and a more general problem of fully characterizing the structure of $\mathcal{C}_k$: we conjecture that all gates in $\mathcal{C}_k$ are something we refer to as generalized semi-Clifford operations, i.e., a natural generalization of the concept of semi-Clifford operations to the case including classical permutations. Our results about this semi-Clifford operations versus $\mathcal{C}_k$ gates relation can be visualized in Fig. 3.

Just as in the usual circuit model, different gates are implemented with different levels of complexity using this teleportation scheme. It is then natural to ask the questions of how to characterize this concept of gate complexity with concrete physical quantities, how does this measure based on teleportation schemes compare with the usual circuit depth, and what it implies for the practical construction of quantum computation architecture. To answer these questions, we introduce a quantity as a measure of gate complexity for fault-tolerant quantum computation based on the $\mathcal{C}_k$ hierarchy, called teleportation depth, which characterizes how many teleportation steps are necessary, on average, to implement a given gate. We demonstrate the effect of the existence of non-semi-Clifford operations in $\mathcal{C}_k$ on the estimation of the upper bound for the teleportation depth, as well as some quantitative difference between the capabilities of one- and two-bit teleportation.

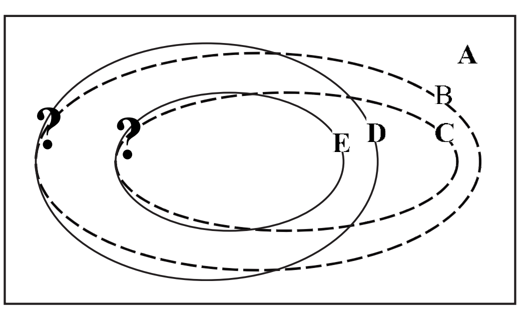

FIG. 3. Semi-Clifford operations versus $\mathcal{C}_k$ gates. A: all gates; B: generalized semi-Clifford gates; C: semi-Clifford gates; D: $\mathcal{C}_k$ gates; E: $\mathcal{C}_3$ gates. C is strictly contained in B and E is strictly contained in D. The two question marks indicate two open problems we have: whether D is a subset of B; and whether E is a subset of C.

The paper is organized as follows: Sec. II gives definition and basic properties of semi-Clifford operations and generalized semi-Clifford operations; in Sec. III we study the structure of $\mathcal{C}_k$ hierarchy in terms of semi-Clifford and generalized semi-Clifford operations; Sec. IV is devoted to the discussion of teleportation depth and how it depends on the structure of $\mathcal{C}_k$; and with Sec. V, we conclude our paper.

II. SEMI-CLIFFORD OPERATIONS AND ITS GENERALIZATION

The concept of semi-Clifford operations was first introduced in [9], to characterize the property of gates transforming Pauli matrices acting on a single qubit. Here we generalize it to the n-qubit case, through the following definition.

Definition 2. An n-qubit unitary operation is called semi-Clifford if it sends by conjugation at least one maximal Abelian subgroup of $\mathcal{P}_n$ to another maximal Abelian subgroup of $\mathcal{P}_n$. That is, if U is an n-qubit semi-Clifford operation, then there must exist at least one maximal Abelian subgroup G of $\mathcal{P}_n$, such that $UGU^\dagger$ is another maximal Abelian subgroup of $\mathcal{P}_n$.

A simple example of the semi-Clifford operation is any diagonal gate. Denote $\langle S_i\rangle$ the group generated by a set of operators $\{S_i\}$. Then any diagonal gate keeps the group $\langle Z_i\rangle_{i=1}^n\times\{\pm 1\pm i\}$ invariant, which is a maximal Abelian subgroup of $\mathcal{P}_n$. In fact, any semi-Clifford operation can be related to diagonal gates via some Clifford operations. This most basic property of a semi-Clifford operation is given by the following proposition.

Proposition 1. If R is a semi-Clifford operation, then there exist Clifford operations L_1,L_2 such that L_1RL_2 is diagonal.

Proof. Z_i represents the Pauli Z operation on the ith qubit. If R is an n-qubit semi-Clifford operation, then there must exist n-qubit operations $L_1,L_2\in\mathcal{C}_2$ such that $RL_2Z_iL_2^\dagger R^\dagger=L_1^\dagger Z_iL_1$ [10], i.e., $L_1RL_2Z_iL_2^\dagger R^\dagger L_1^\dagger=Z_i$ holds for any $i=1\ldots n$. Therefore, $(L_1RL_2)Z_i=Z_i(L_1RL_2)$, i.e., the n-qubit gate L_1RL_2 is diagonal. ■

In other words, semi-Clifford operations are those gates diagonalizable "up to Clifford multiplications." Thus the structure problem of the whole set of semi-Clifford operations is reduced to that of the diagonal subset within it.

As we shall see later, the notion of semi-Clifford operations is useful in characterizing some but not all gates in the $\mathcal{C}_k$ hierarchy. More generally, we might also consider those gates with properties of transforming the span, or in other words the group algebra over the complex field, of a maximal Abelian subgroup of $\mathcal{P}_n$.

Definition 3. A generalized semi-Clifford operation on n qubits is defined to send by conjugation the span of at least one maximal Abelian subgroup of $\mathcal{P}_n$ to the span of another maximal Abelian subgroup of $\mathcal{P}_n$.

Denote the span of the group $\langle S_i\rangle$ as $\mathfrak{C}(\langle S_i\rangle)$. Then in a more mathematical form we can write the above definition as follows:

If U is a generalized semi-Clifford operation on n qubits, then there must exist at least one maximal Abelian subgroup $G=\langle g_i\rangle$ of $\mathcal{P}_n$, such that for all $s\in\mathfrak{C}(\langle g_i\rangle)$, $UsU^\dagger\in\mathfrak{C}(U\langle g_i\rangle U^\dagger)$, where $UGU^\dagger$ is another maximal Abelian subgroup of $\mathcal{P}_n$.

A simple example of the generalized semi-Clifford operation is any classical permutation (which is some permutation of computational basis states). A classical permutation keeps $\mathfrak{C}(\langle Z_i\rangle_{i=1}^n\times\{\pm 1\pm i\})$ invariant, since it maps any diagonal gate to another diagonal gate. In fact, any generalized semi-Clifford operation can be related to a classical permutation via some semi-Clifford operations. This most basic property of a generalized semi-Clifford operation is given by the following proposition.

Proposition 2. If R is a generalized semi-Clifford operation, then there exist Clifford operations L_1,L_2 and a classical permutation operator P such that PL_1RL_2 is diagonal.

Proof. If R is a generalized semi-Clifford operation, then there must exist $L_1,L_2\in\mathcal{C}_2$ such that $RL_2\mathfrak{C}(\langle Z_i\rangle_{i=1}^n)L_2^\dagger R^\dagger=L_1^\dagger\mathfrak{C}(\langle Z_i\rangle_{i=1}^n)L_1$, i.e., $L_1RL_2\mathfrak{C}(\langle Z_i\rangle_{i=1}^n)L_2^\dagger R^\dagger L_1^\dagger=\mathfrak{C}(\langle Z_i\rangle_{i=1}^n)$. That is, L_1RL_2 maps all the diagonal matrices to diagonal matrices; therefore L_1RL_2 must be a monomial matrix, i.e., there exist a permutation matrix P and a diagonal matrix V, such that $L_1RL_2=P^\dagger V\Rightarrow PL_1RL_2$ is diagonal. ■

Note for the single qubit case, i.e., $n=1$, the concepts of semi-Clifford operation and generalized semi-Clifford operation coincide.

III. THE STRUCTURE OF $\mathcal{C}_k$

In this section we study the structure of gates in $\mathcal{C}_k$. To begin with, we study some basic properties of $\mathcal{C}_k$ gates. Then we give our main results as structure theorems, which state that all the $\mathcal{C}_k$ gates are semi-Clifford when $\{n=1,2,\ \forall\ k\}$ and $\{n=3,k=3\}$, but for $\{n>2,k>3\}$ there are examples of $\mathcal{C}_k$ gates which are non-semi-Clifford. We then discuss the open question for the parameters $\{n>2,k=3\}$, and based on the constructed counterexamples we conjecture that all $\mathcal{C}_k$ gates are generalized semi-Clifford operations.

It should be noted that the set of n-qubit $\mathcal{C}_k$ gates is always strictly contained in the set of n-qubit $\mathcal{C}_{k+1}$ gates. In [6], explicit examples are given to support this statement. If we denote as $\Lambda_{n-1}(U)$ the n-qubit gate which applies U to the nth qubit only if the first $n-1$ qubits are all in the state $|1\rangle$, then $\Lambda_{n-1}(\mathrm{diag}(1,e^{2\pi/2^m}))$ is in $\mathcal{C}_{m+n-1}\backslash\mathcal{C}_{m+n-2}$.

A. Basic properties

We first state an important property of gates in $\mathcal{C}_k$, which reduces the problem of characterizing the structure of $\mathcal{C}_k$ into a problem of characterizing a certain subset of gates in $\mathcal{C}_k$.

Proposition 3. If $R\in\mathcal{C}_k$, then $L_1RL_2\in\mathcal{C}_k$, where $L_1,L_2\in\mathcal{C}_2$, $k\geq 2$.

Proof. We prove this proposition by induction.

(i) It is obviously true for $k=2$.

(ii) Assume it is true for k.

(iii) For $k+1$, $R\in\mathcal{C}_{k+1}$ implies $RAR^\dagger\in\mathcal{C}_k$, where $A\in\mathcal{C}_1$. If we conjugate A by L_1RL_2, we obtain

$$L_1RL_2A(L_1RL_2)^\dagger=L_1R(L_2AL_2^\dagger)R^\dagger L_1^\dagger. \quad (2)$$

Since $L_1,L_2\in\mathcal{C}_2$, $L_1^\dagger,L_2^\dagger$ are in $\mathcal{C}_2$ also. And because $L_2AL_2^\dagger\in\mathcal{C}_1$, $R(L_2AL_2^\dagger)R^\dagger\in\mathcal{C}_k$. According to assumption (ii), $L_1R(L_2AL_2^\dagger)R^\dagger L_1^\dagger\in\mathcal{C}_k$. Finally, as we can see from Eq. (2), $L_1RL_2\in\mathcal{C}_{k+1}$. ■

According to Proposition 3, in order to characterize the full structure of $\mathcal{C}_k$, we only need to characterize the structure of a subset of it which generates the whole set with Clifford multiplications.

It is known that $\mathcal{C}_k$ is not a group for $k>2$ and its structure is in general hard to characterize. However, if we denote all the diagonal gates in $\mathcal{C}_k$ as $\mathcal{F}_k$, then we have the following:

Proposition 4. $\mathcal{F}_k$ is a group. If we can characterize the group structure of $\mathcal{F}_k$, then the structure of the $\mathcal{C}_k$ subset $\{L_1F_kL_2\}$ is known to us ($L_1,L_2\in\mathcal{C}_2,F_k\in\mathcal{F}_k$). According to Proposition 1, this is just the set of all semi-Clifford operations in $\mathcal{C}_k$. In the next section, we will repeatedly use this fact to gain knowledge about semi-Clifford $\mathcal{C}_k$ gates from the group structure of $\mathcal{F}_k$ and for now we will give a brief proof of the above proposition.

Proof. We prove by induction.

(i) It is of course true for $k=2$.

(ii) Assume it is true for k, i.e., $\mathcal{F}_k$ is a group.

(iii) Then for $k+1$, note for any $F_{k+1}\in\mathcal{F}_{k+1}$, $F_{k+1}MF_{k+1}^\dagger=F_kM=MF_k'$, for nondiagonal $M\in\mathcal{C}_1$, where $F_k,F_k'\in\mathcal{F}_k$.

(a) If $F_{k+1}\in\mathcal{F}_{k+1}$, then $F_{k+1}^\dagger\in\mathcal{F}_{k+1}$, since $F_{k+1}^\dagger MF_{k+1}=F_k^\dagger M=MF_k'^\dagger$, which is in $\mathcal{F}_k$ by assumption (ii).

(b) If $F_{1k},F_{2k}\in\mathcal{F}_k$, then $F_{1k}F_{2k}\in\mathcal{F}_k$, since $F_{1k-1}F_{2k-1}\in\mathcal{F}_{k-1}$. ■

According to this proposition, all semi-Clifford $\mathcal{C}_k$ gates can be characterized by the group structure of diagonal $\mathcal{C}_k$ gates.

B. Structure theorems

Our main results about the structure of $\mathcal{C}_k$ are the following three theorems, which state that all the $\mathcal{C}_k$ gates are semi-Clifford when $\{n=1,2,\ \forall\ k\}$ and $\{n=3,k=3\}$, but it is no longer true for $\{n>2,k>3\}$.

Theorem 1. All gates in $\mathcal{C}_k$ are semi-Clifford operations for $(n=1,2,\ \forall\ k)$.

Proof. Here we prove the case of $n=2$. The proof of the $n=1$ case is similar but can also be checked by direct calculation and lead to a complete classification of all one-qubit $\mathcal{C}_k$ gates according to the group structure of diagonal one-qubit $\mathcal{C}_k$ gates. We give details for the $n=1$ case in Appendix A.

For $n=2$, we prove this theorem by induction.

(i) It is obviously true for $k=1,2$.

(ii) Assume it is true for k.

(iii) For $k+1$:

(a) We calculate the set $S_1=\{L_1V\}$ for all $L_1\in\mathcal{C}_2$, where $V\in\mathcal{F}_k$. Note by assumption (ii), S_1 gives us all the elements in $\mathcal{C}_k$ up to Clifford conjugation.

(b) Note in general $V=\text{diag}\{e^{i\alpha},e^{i\beta},e^{i\gamma},e^{i\delta}\}$ for some angles α, β, γ, and δ. By exhaustive calculation with all $L_1\in\mathcal{C}_2$ we show that if there exists an element $V_s\in S_1$ such that V_s is trace zero and Hermitian, then $V=\text{diag}\{e^{-i\theta_1},e^{-i\theta_2},e^{i\theta_2},e^{i\theta_1}\}$ for some θ_1 and θ_2. Furthermore, we can again show by exhaustive calculation with all $L_1\in\mathcal{C}_2$ that the only trace zero and Hermitian $V_s\in S_1$ is of the following form up to Clifford conjugation:

$$V_s=\begin{pmatrix}0&0&0&e^{-i\theta_1}\\0&0&e^{-i\theta_2}&0\\0&e^{i\theta_2}&0&0\\e^{i\theta_1}&0&0&0\end{pmatrix}. \tag{3}$$

(c) We calculate the set $S_2=\{L_1V_sL_1^\dagger\}$ for all $L_1\in\mathcal{C}_2$, which by assumption (ii) and fact (b) gives all the elements in $\mathcal{C}_k$ which are trace zero and Hermitian.

(d) We show that for any two-qubit gate U such that $UV_sU^\dagger=Z_1$ and $\{U\mathcal{P}_2U^\dagger\}\subseteq S_2$, there exist $L_1,L_2\in\mathcal{C}_2$ such that L_1UL_2 is diagonal. This can be started from studying the eigenvectors of V_s, which can be chosen of the form

$$U=\frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&1\\0&1&1&0\\0&e^{i\theta_2}&-e^{i\theta_2}&0\\e^{i\theta_1}&0&0&-e^{i\theta_1}\end{pmatrix}, \tag{4}$$

and carefully considering the possible phase of each eigenvector and the possible superposition of the eigenvectors due to the degeneracy of the eigenvalues, similar to the process shown in Appendix A. ■

Theorem 2. All gates in $\mathcal{C}_k$ are semi-Clifford operations for $\{n=3,k=3\}$.

Proof. We prove this theorem exhaustively using the following proposition:

Proposition 5. An n-qubit $\mathcal{C}_k$ gate U is semi-Clifford if and only if the group $\{U\mathcal{P}_nU^\dagger\}\cap\mathcal{P}_n$ contains a maximally Abelian subgroup of $\mathcal{P}_n$.

Proof. Suppose $U=L_1VL_2$, then $U\mathcal{P}_nU^\dagger=L_1VL_2\mathcal{P}_nL_1^\dagger V^\dagger L_1^\dagger=L_1V\mathcal{P}_nV^\dagger L_1^\dagger\supset\{L_1Z_iL_1^\dagger\}_{i=1}^n$.

On the contrary, if $\{U\mathcal{P}_nU^\dagger\}\cap\mathcal{P}_n$ contains a maximal Abelian subgroup of $\mathcal{P}_n$, then there must exist $L_1,L_2\in\mathcal{C}_2$ such that $UL_1^\dagger Z_iL_1U^\dagger=L_2Z_iL_2^\dagger$, i.e., $L_2^\dagger UL_1^\dagger Z_iL_1U^\dagger L_2=Z_i$ holds for any $i=1\ldots n$. Therefore, $(L_2^\dagger UL_1^\dagger)Z_i=Z_i(L_2^\dagger UL_1^\dagger)$, $\Rightarrow L_2^\dagger UL_1^\dagger$ is diagonal. If we denote this diagonal gate as V, $L_2^\dagger UL_1^\dagger=V\Rightarrow U=L_1VL_2$.

Therefore, by exhaustive study with the subgroups of the three-qubit Clifford group which are isomorphic to $\mathcal{P}_3$, we complete the proof of this theorem. More detailed analysis about this is given in Appendix B. The calculation is done using GAP [11]. ■

Theorem 3. Not all gates in $\mathcal{C}_k$ are semi-Clifford operations for $(n>2,k>3)$.

Proof. Actually we only need to prove this theorem for $n=3$, $k=4$ then it naturally holds for all the other parameters of $\{n>2,k>3\}$. However, we would like to explicitly construct examples for all $\{n=3,k>4\}$. Define W_k as in Fig. 4.

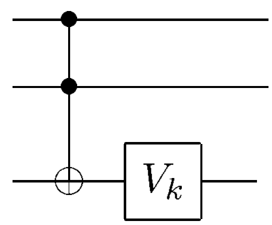

FIG. 4. A non-Clifford-diagonalizable $\mathcal{C}_k$ gate W_k. $V_k=\text{diag}(1,e^{i\pi/2^{k-1}})$.

Proposition 6. The gate

$$W_k=T(c_1,c_2,t_3)\otimes V_{3,k} \tag{5}$$

is a $\mathcal{C}_{k+1}$ operation but not a semi-Clifford operation, where $T(c_1,c_2,t_3)$ is a Toffoli gate with the first and second qubits as its control and the third qubit as its target, and $V_{3,k}$ is single qubit operator $\text{diag}(1,\exp(i\pi/2^{k-1}))$ on the third qubit.

Proof. To prove that W_k is in $\mathcal{C}_{k+1}$:

(i) When $k=2$, $V_k=\text{diag}\{1,i\}\in\mathcal{C}_2$. W_2 is of the form LR, where L is a Clifford operation and R is the Toffoli gate. According to Proposition 3, W_2 and the Toffoli gate are both in $\mathcal{C}_3$.

(ii) For $k>2$, direct calculation shows that $\{W_kZ_iW_k^\dagger\}\subset\mathcal{C}_2$, $i=1,2,3$. $W_kX_1W_k^\dagger\in\mathcal{C}_k$, $W_kX_2W_k^\dagger\in\mathcal{C}_k$, $W_kX_3W_k^\dagger\in\mathcal{C}_{k-1}$. The images of X_i's under the conjugation of W_k can all be written in the form $W_kX_iW_k^\dagger=X_iF_{ki}=F'_{ki}X_i$, where F_{k1}, F'_{k1}, F_{k2}, F'_{k2} are diagonal gates in $\mathcal{C}_k$ and F_{k3}, and F'_{k3} are diagonal single qubit gates in $\mathcal{C}_{k-1}$ acting on the third qubit.

The image of the whole three-qubit Pauli group $\{W_k\mathcal{P}_3W_k^\dagger\}$ is generated by the six elements shown above. As multiplication by Clifford gates preserves the $\mathcal{C}_k$ hierarchy, we only need to check the images of Pauli operations which are composed of two or more X_i's and see if their images are still in $\mathcal{C}_k$.

This is obviously true considering the special form of $\{W_kX_iW_k^\dagger\}$. Multiplication of any two of them is of the form $W_kX_iX_jW_k^\dagger=X_iF_{ki}F'_{kj}X_j$. This is in $\mathcal{C}_k$ as the diagonal $\mathcal{C}_k$ gates form a group. Furthermore, multiplication of all of them takes the form $W_kX_1X_2X_3W_k^\dagger=X_1F_{ki}F'_{kj}X_2F'_{k3}X_3$. As F'_{k3} is a single qubit operation on the third qubit, $W_kX_1X_2X_3W_k^\dagger=X_1F_{ki}F'_{kj}F'_{k3}X_2X_3$. This is again a $\mathcal{C}_k$ gate because of the group structure of diagonal $\mathcal{C}_k$ gates.

Therefore, we have checked explicitly that $W_k\in\mathcal{C}_{k+1}$.

To prove that W_k is not semi-Clifford, we can exhaustively calculate $\{W_k\mathcal{P}_3W_k^\dagger\}$ and find its intersection with $\mathcal{P}_3$. The fact that $\{W_k\mathcal{P}_3W_k^\dagger\}\cap\mathcal{P}_3$ does not contain a maximally Abelian subgroup of $\mathcal{P}_3$ implies that W_k is not semi-Clifford, due to Proposition 5.

With this example we have directly proved Theorem 3. ■

C. Open problems

Let us try to understand more about the structure theorems we have in the previous section.

First recall from [8] that the controlled-Hadamard gate $\Lambda_1(H)$, which is a $\mathcal{C}_3$ gate, is explicitly shown to be semi-

Clifford. We can also view this from the perspective of Proposition 5, by noting that $\Lambda_1(H)Z_1\Lambda_1(H)^\dagger = Z_1$, $\Lambda_1(H)Y_2\Lambda_1(H)^\dagger = Z_1 \otimes -Y_2$, which means that the maximal Abelian subgroup of the Pauli group generated by $\langle Z_1, Y_2\rangle \times \langle \pm 1, \pm i\rangle$ is in the image of $\Lambda_1(H)$. However, if we consider W_3 from the perspective of Proposition 5, we obtain $W_3Z_1W_3^\dagger = Z_1$, $W_3Z_2W_3^\dagger = Z_2$, $W_3Z_3W_3^\dagger = \Lambda_1(Z_2)\otimes Z_3$. Note THAT this does not give us a maximal Abelian subgroup of the Pauli group $\langle Z_1, Z_2, Z_3\rangle \times \langle \pm 1, \pm i\rangle$, due to the effect of $\Lambda_1(Z_2)$ caused by conjugating through the Toffoli gate. This intuitively explains why Theorem 3 could be true, but no counterexample to Theorem 2 exists.

Note that W_k is actually a generalized semi-Clifford operation, which is apparent from its form. Also, the construction of the series of gates W_k, as well as their extensions to $n>3$ qubits, cannot give any non-semi-Clifford $\mathcal{C}_3$ gate. We then have the following conjectures on the open problem of the structure of $\mathcal{C}_k$ hierarchy in general.

Conjecture 1. All gates in $\mathcal{C}_3$ are semi-Clifford operations.

Conjecture 2. All gates in $\mathcal{C}_k$ are generalized semi-Clifford operations.

IV. THE TELEPORTATION DEPTH

Teleportation, as a computational primitive, is a crucial element providing universal quantum computation to fault-tolerant schemes based on stabilizer codes. However, not all gates are of equal complexity in this scheme. To actually incorporate this technique in the construction of practical computational architecture, it is useful to know which gates are easier to implement and which are harder, so that we could achieve optimal efficiency in performing a computational task. In the circuit model of quantum computation, we face the same problem and in that case "circuit depth" was introduced [12] to characterize the number of simple one- and two-qubit gates needed to implement an operation. While this provides a good measure of gate complexity, it does not take into consideration of fault tolerance. It is interesting to have measures quantifying fault-tolerant gate complexity to be compared with "circuit depth" to give us a better understanding of the computational tasks at hand.

Based on the $\mathcal{C}_k$ hierarchy introduced in [6] and the knowledge of its structure gained in the previous section, we define a measure of gate complexity for the teleportation protocol, called teleportation depth, which characterizes how many teleportation steps are necessary, on average, to implement a given gate. Since any teleportation unavoidably causes randomness, we need to figure out a certain point to start with, i.e., we should assume in advance that some kind of gates can be performed fault tolerantly. We know that a fault-tolerant protocol is usually associated with some quantum error-correcting codes. Self-dual Calderbank-Shor-Steane codes, such as the seven-qubit Steane code, admit all gates in the Clifford group to be transversal [10]. In such a situation, we only need to teleport the gate outside the Clifford group, and in the following, we will assume this as a starting point. The advantage of doing this, in practice, is that due to Proposition 1, we have the freedom of preparing the ancilla states up to some Clifford multiplications.

A. Definition of the teleportation depth

With the standard two-bit teleportation scheme (Fig. 1) in mind, it is easy to see that all gates in the $\mathcal{C}_k$ hierarchy can be teleported fault tolerantly as a whole in a recursive manner. Suppose U is an n-qubit $\mathcal{C}_k$ gate. The ancilla state can be fault tolerantly prepared and all the elements in the teleportation circuit of U are in $\mathcal{C}_2$ and can be performed fault tolerantly, except the classically controlled operation $U_1 = R'_{xy} = UR_{xy}U^\dagger$, where R_{xy} is an operator in $\mathcal{C}_1$ which depends on the (random) Bell-basis measurement outcomes xy. However, as U is in $\mathcal{C}_k$, U_1 is in general a $\mathcal{C}_{k-1}$ operation and can be implemented again by teleportation. In this way, after each teleportation step, a $\mathcal{C}_k$ gate is mapped to another gate one level lower. This recursive procedure terminates when U_i is in $\mathcal{C}_2$.

Based on the above picture we give a more formal definition of teleportation, which characterizes its randomness nature.

Definition 4. The teleportation map f takes an n-qubit operator A to a set of operators via the following manner:

$$f: A \to \{AP_{j_1}A^\dagger\}_{j_1=1}^{4^{n+1}}, \tag{6}$$

where P_i are elements of the n-qubit Pauli group $\mathcal{P}_n$.

Note that

$$f\circ f: A \to \{(AP_{j_1}A^\dagger)P_{j_2}(AP_{j_1}A^\dagger)^\dagger\}_{j_1,j_2=1}^{4^{n+1}} \tag{7}$$

and

$$\begin{aligned} f\circ f\circ f: A \\ &\to \{[(AP_{j_1}A^\dagger)P_{j_2}(AP_{j_1}A^\dagger)^\dagger]P_{j_3} \\ &\times[(AP_{j_1}A^\dagger)P_{j_2}\times(AP_{j_1}A^\dagger)^\dagger]^\dagger\}_{j_1,j_2,j_3=1}^{4^{n+1}}, \ldots . \end{aligned} \tag{8}$$

Each element in the image of the map $f^{\circ m}$ on A is associated with a set

$$S = \{j_1, j_2, \ldots, j_m\}. \tag{9}$$

Denote $f_S^{\circ m}(A)$ as the element in the image of the map $f^{\circ m}$ on A associated with the set S. Each element in the image occurs with equal probability.

Definition 5. $f_S^{\circ m}(A)$ terminates if $f_S^{\circ m}(A)\in\mathcal{C}_2$.

If $f_S^{\circ m_1}(A)$ terminates, then $f_{S'}^{\circ m_2}(A)$ terminates for any $m_2 \geq m_1$, and $S' = \{j_1, j_2, \ldots, j_{m_1}, \ldots, j_{m_2}\}$. Therefore, for each $f_S^{\circ m}(A)$ that terminates, there must exist a set S_{min} with the minimal size such that $f_{S_{min}}^{\circ|S_{min}|}(A)$ terminates, where $S_{min} = \{j_1, j_2, \ldots, j_{m'}\}$ ($m' = |S_{min}|$). In our following discussions, we will only consider sets S which are minimal in this sense.

This mapping procedure works directly on $\mathcal{C}_k$ gates. If W is an n-qubit $\mathcal{C}_k$ gate, then there is no need to decompose it into consecutive applications of several other gates and we say we can "direct teleport" W. W is in $\mathcal{C}_k$ iff $\forall S$, $f_S^{\circ(k-2)}(A)\in\mathcal{C}_2$, and $\exists S'$, such that $f_{S'}^{\circ(k-3)}(A)\notin\mathcal{C}_2$.

Among all $\mathcal{C}_k$ gates, the set of semi-Clifford operations have the special property that they can be teleported with only half the ancilla resources as in a standard teleportation scheme. This "one-bit teleportation scheme" is illustrated in Fig. 2. This scheme also complies with the mapping description given above. Instead of Bell basis measurement, randomness in a one-bit teleportation scheme comes from single qubit measurement and P_j belongs to a maximal Abelian subgroup of the whole n-qubit Pauli group in general.

To teleport an arbitrary n-qubit gate A, we can first decompose A into the $\mathcal{C}_k$ hierarchy, $A=A_1A_2\ldots A_r$, where $A_i \in \mathcal{C}_{k_i}$, because we only know how to teleport $\mathcal{C}_k$ gates fault tolerantly. We call this procedure "decomposition of A into $\mathcal{C}_\infty$." Suppose that to teleport each gate A_i, m_i maps are needed on average, with the average taken over all possible sets $S=\{j_1,j_2,\ldots,j_m\}$. Then the teleportation depth of A is defined as follows.

Definition 6. The teleportation depth of a gate A, denoted as T, is the minimal sum of all m_i—the average number of teleportation steps needed to implement each component gate of A—where the minimum is taken over all possible decompositions of A into $\mathcal{C}_\infty$.

Due to Definition 6, in order to calculate the teleportation depth of a given gate A, one needs to find all possible decompositions of A into $\mathcal{C}_\infty$ gates and calculate the corresponding depth, then minimize over all of them. This is generally intractable, but one may expect to upper bound the depth with some particular decomposition of A into $\mathcal{C}_\infty$ gates.

Let us first consider the case of an n-qubit $\mathcal{C}_k$ gate.

Definition 7. $T(n,k)$ is the teleportation depth of an n-qubit $\mathcal{C}_k$ gate.

As such a gate can be teleported directly, $T(n,k)$ is upper bounded by the average number of steps needed in this direct teleportation scheme to terminate the teleportation procedure.

$$T(n,k) \le \frac{1}{N}\sum_S |S|, \qquad (10)$$

where the summation is over all possible (minimal) sets S and N is the number of such sets.

However, when $k\to\infty$, it is not obvious that the above summation will converge. We will show that this is true. Then for an arbitrary gate A, by decomposing A into a finite series of $\mathcal{C}_k$ gates, we can see that the teleportation depth of A turns out to be finite. Then we do not actually require the procedure to terminate within a finite number of steps.

Different teleportation schemes, for example, one-bit and two-bit teleportation, give different upper bounds on teleportation depth for a certain circuit. While for some circuits one scheme is obviously more efficient than others, the comparison among different schemes in other cases may not be so straightforward and may depend sensitively on various parameters in the circuit. In the following sections, we study such dependence and present surprising results beyond our usual expectation with examples from important quantum circuits.

B. Teleportation depth of semi-Clifford $\mathcal{C}_k$ gates

We first calculate explicitly an upper bound for the teleportation depth of semi-Clifford n-qubit $\mathcal{C}_k$ gates. We know from [8] that this kind of gate can be teleported directly with the architecture of one-bit teleporation and we denote the upper bound calculated with this "one-bit" "direct" teleportation procedure as $T_1(n,k)$. For a general n-qubit gate, if it is possible to decompose it into a series of semi-Clifford $\mathcal{C}_k$ operations, the upper bound of teleportation depth obtained by teleporting each part separately using the one-bit teleportation scheme is in general denoted as T_1.

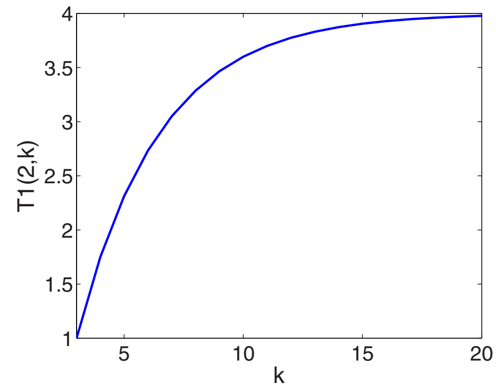

FIG. 5. (Color online) The behavior of $T_1(2,k) = 4[1-(3/4)^{k-2}]$.

Definition 8. T_1 is the average total number of teleportation steps needed to teleport separately each semi-Clifford $\mathcal{C}_k$ component of a quantum circuit using the one-bit teleportation scheme, if such a decomposition is possible. More specifically, $T_1(n,k)$ is the average number of teleportation steps needed to teleport an n-qubit semi-Clifford $\mathcal{C}_k$ gate directly (i.e., without decomposition) using the one-bit teleportation scheme.

Apparently we have $T(n,k)\le T_1(n,k)$ in general.

The probability that the teleportation process terminates immediately after one teleportation step equals the percentage weight of a maximal Abelian subgroup in the whole Pauli group, which is $\frac{1}{2^n}$ for an n-qubit Pauli group. Now each teleportation step may have two possible endings: (i) with probability $p=\frac{1}{2^n}$, $\{U\mathcal{P}_nU^\dagger\}\in\mathcal{P}_n$ and the process terminates; (ii) with probability $1-p$, $\{U\mathcal{P}_nU^\dagger\}$ is a general n-qubit $\mathcal{C}_{k-1}$ gate and the process goes on. The upper bound of the teleportation depth calculated with this process is then

$$T_1(n,k) = p\sum_{s=1}^{k-3} s(1-p)^{s-1} + (k-2)(1-p)^{k-3} = 2^n\left[1-\left(1-\frac{1}{2^n}\right)^{k-2}\right]. \qquad (11)$$

It is clearly seen from Eq. (11) that $T_1(n,k)$ converges to 2^n when $k\to\infty$, which means that $T(n,k)$ is in general bounded. For instance, when $n=2$, Eq. (11) tells us that $T(2,k)\le T_1(2,k)=4[1-(3/4)^{k-2}]$. The behavior of $T_1(2,k)$ is shown in Fig. 5. However, since $T_1(2,k)=4[1-(3/4)^{k-2}] \le 4[1-(1/2)^{k-2}]=2T_1(1,k)$, we find that teleporting two single qubit semi-Clifford $\mathcal{C}_k$ gates together using the one-bit teleportation scheme needs fewer teleportation steps than to teleport each of them separately.

Since $1-\frac{1}{2^n}<1$, $T_1(n,k)$ quickly reaches 2^n as k grows. Therefore, generally, the upper bound of the teleportation depth of a $\mathcal{C}_k$ gate given by "direct teleportation" is not de-

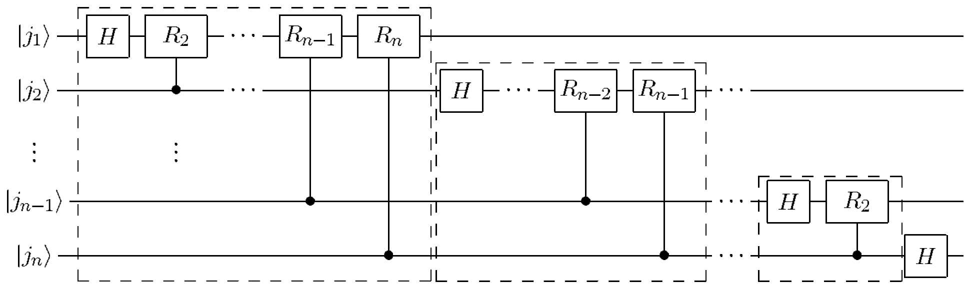

FIG. 6. Circuit for n-qubit quantum Fourier transform.

termined by k, but by the number of qubits n it actually acts on. Moreover, since $T_1(n,\infty)=2^n$, i.e., the upper bound of teleportation depth increases exponentially with n, in general, when n,k are large, it is better to decompose an n-qubit $\mathcal{C}_k$ gate into some one- and two-qubit gates to obtain a lower upper bound. However, if $k \sim P(n)$, where $P(n)$ is a polynomial in n, then $T_1(n,k)$ scales as $P(n)$.

Now we give two examples as applications of the above upper bounds, through which we obtain some idea about the order of teleportation depth in comparison with the usual circuit depth.

1. Teleportation depth of the n-qubit quantum Fourier transform

The first example is the n-qubit quantum Fourier transform (QFT) circuit, as shown in Fig. 6. R_k denotes the unitary transformation $R_k=\text{diag}(1,e^{2\pi i/2^k})$. The circuit depth of n-qubit QFT goes as n^2 and we will soon find that the teleportation depth of this circuit is of the same order.

Each block of gates within a single dashed box (Hadamard plus controlled z rotations on the kth qubit) is a semi-Clifford $(n-k+1)$-qubit $\mathcal{C}_{n-k+2}$ gate, $k=1,\ldots,n-1$, and can be teleported directly using the one-bit scheme. Therefore the whole circuit can be teleported piece by piece by one-bit teleportation. Note that

$$T(n,k=n+1) \le T_1(n,k=n+1) \tag{12}$$

$$=2^n\left(1-\left(1-\frac{1}{2^n}\right)^{n-1}\right) \tag{13}$$

$$\sim n-1 \tag{14}$$

for large n. Actually, numerical data shows that even when n is small, $T_1(n,k=n+1)\sim n-1$ is almost also true.

Therefore, the teleportation depth of the n-qubit QFT is upper bounded by

$$\sum_{j=2}^{n} T(j,k=j+1) \le \sum_{j=2}^{n} T_1(j,k=j+1) \le \sum_{j=1}^{n} (j-1) \tag{15}$$

$$=\frac{1}{2}n(n-1) \sim O(n^2). \tag{16}$$

Numerical calculation show that $\Sigma_{j=2}^{n}T_1(j,k=j+1)$ is almost $\frac{1}{2}n(n-1)-1$.

Note that the probability for the teleportation process to terminate is 1 for teleporting an n-qubit $\mathcal{C}_{k=n+1}$ gate $n-1=k-2$ times. This means that the upper bound we obtained for this block teleportation scheme of QFT is just slightly lower than naively assuming that we need $k-2$ teleportation steps to teleport a $\mathcal{C}_k$ gate. The reason we do not benefit from the average is that for QFT, k is generally comparable with n.

2. Uniformly controlled rotation

Now we consider another example (Fig. 7), the uniformly controlled rotations, which are widely used in analyzing the circuit complexity of an arbitrary n-qubit quantum gate [13,14]. This circuit in general needs $2^{n+2}-4n-4$ CNOT gates and $2^{n+2}-5$ one-qubit elementary rotations to implement. For complexity analysis of this circuit see, for example, [13].

The teleportation depth of this rotation is in general upper bounded by 2^n. However, if each $(n-1)$-qubit-controlled gate is in $\mathcal{C}_k$, we might expect to do better. For instance, when $k=cn$, for any positive constant n, the teleportation depth scales as cn, i.e., linear in n. Moreover, if $k\sim P(n)$, where $P(n)$ is a polynomial in n, then the teleportation depth scales as $P(n)$.

C. Teleportation depth beyond semi-Clifford $\mathcal{C}_k$ gates

Now recall our series of examples of non-semi-Clifford $\mathcal{C}_k$ gates given in Fig. 4. We know that if $V_k\in\mathcal{C}_k$, then $W_k\in\mathcal{C}_{k+1}$. And the group $W_k\mathcal{P}_3W_k^\dagger$ does not contain a maximally Abelian subgroup of $\mathcal{P}_3$, i.e., $W_k\in\mathcal{C}_{k+1}$ is not directly one-bit teleportable.

Therefore, we know that there are some W_k gates in the $\mathcal{C}_k$ hierarchy which can only be teleported directly by the standard two-bit teleportation scheme. Using this scheme, we can calculate another upper bound for the teleportation depth, which we denote as $T_2(n,k)$.

Definition 9. T_2 is the average total number of teleportation steps needed to teleport separately each $\mathcal{C}_k$ component of a quantum circuit using the two-bit teleportation scheme, if

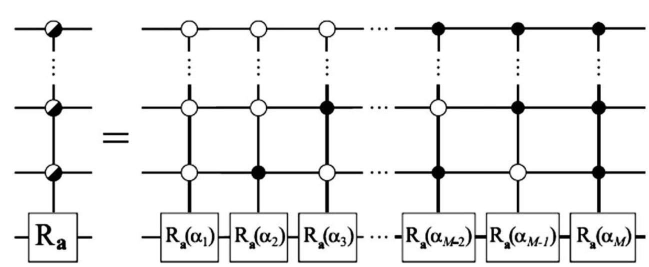

FIG. 7. Definition of the $n-1$-fold uniformly controlled rotation of a qubit about the axis $\vec{a}$.

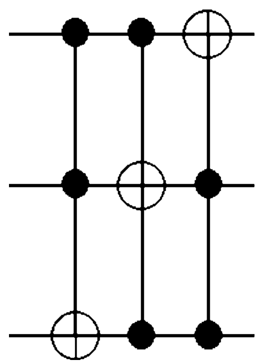

FIG. 8. The R_{c3} gate—three Toffoli gates in series.

such a decomposition is possible. More specifically, $T_2(n,k)$ is the average number of teleportation steps needed to teleport an n-qubit $\mathcal{C}_k$ gate directly (i.e., without decomposition) using the two-bit teleportation scheme.

For a general n-qubit $\mathcal{C}_k$ gate, $T_2(n,k)$ can be calculated by replacing p with $\frac{1}{4^n}$ in Eq. (11),

$$T_2(n,k) = p\sum_{s=1}^{k-3} s(1-p)^{s-1} + (k-2)(1-p)^{k-3}$$
$$= 4^n\left[1-\left(1-\frac{1}{4^n}\right)^{k-2}\right], \qquad (17)$$

which then converges to 4^n when $k\to\infty$.

One may guess that in general to teleport W_k directly using the two-bit scheme will give a lower bound for the teleportation depth than to teleport the Toffoli gate and $V_k = \mathrm{diag}(1, e^{i\pi/2^{k-1}})$ separately using the one-bit scheme. Surprisingly, this is not generally true.

When $V_k \in \mathcal{C}_3$, this is indeed true. Teleporting W_k directly gives a bound of $T_2(3,4)=1.875$, which is less than $T_1(3,4)=2$, i.e., the bound given by teleporting the Toffoli gate and V_k separately with the one-bit scheme. However, when $k\to\infty$, teleporting W_k directly gives a bound of $T_2(3,4)=5.25$, which is greater than $T_1(3,4)=3$, i.e., the bound given by teleporting the Toffoli gate and V_k separately. This means that there exists a critical value k that determines which way is more efficient for teleporting W_k, directly or separately.

Note that if $V_k \in \mathcal{C}_k$, we also have $W_k^\dagger \in \mathcal{C}_{k+1}$. Calculating the bounds of teleportation depth for $W_k^\dagger$ shows a similar behavior as that of W_k, however of a slightly different value. For instance, when $V_k \in \mathcal{C}_3$, teleporting $W_k^\dagger$ directly gives a bound of 1.5, which is less than 2, the bound given by teleporting separately. However, when $k\to\infty$, teleporting $W_k^\dagger$ directly gives a bound of 5.5, but teleporting separately gives only a bound of 3.

Up to now, our discussion is entirely based on the $\mathcal{C}_k$ hierarchy. To summarize the capacity of $\mathcal{C}_k$ for fault-tolerant quantum computation and provide a basis for comparison with non-$\mathcal{C}_k$ schemes discussed below, we introduce another notion of T_k.

Definition 10. T_k is the minimum number of total teleportation steps needed to teleport separately each $\mathcal{C}_k$ component of a quantum circuit using either one-bit or two-bit teleportation scheme.

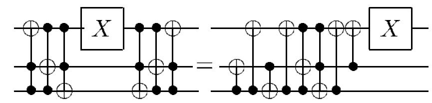

FIG. 9. Conjugating X_1 by R_{c3}.

T_k is defined in a way that represents the maximum capacity of teleportation based on $\mathcal{C}_k$ hierarchy. In general $T_1 \geq T_k$, $T_2 \geq T_k$. To understand exactly how they compare for a given circuit, a full characterization of the structure of $\mathcal{C}_k$ is necessary. Here, based on the structure theorems given in Sec. III, we gave a simple example where T_1 or T_2 could be strictly larger than T_k. The next question to ask is then whether we can go beyond $\mathcal{C}_k$ and this will be discussed in the following section.

D. Teleportation beyond $\mathcal{C}_k$

In the definition of teleportation depth, we require that A be decomposed into a set of $\mathcal{C}_\infty$ gates. This is due to the fact that $\mathcal{C}_\infty$ are the only gates that we know so far how to perform fault tolerantly by teleportation. In general, if we do not require the decomposition to be in $\mathcal{C}_\infty$, then we might obtain a better upper bound on teleportation depth than the one defined previously, i.e., there might exist an upper bound T^* of teleportation depth that is strictly less than T_k. We give two such examples below. We leave open the problem of how to implement teleportations fault tolerantly for a general n-qubit gate.

Example 1. For a general one-qubit gate U, we know that U can be decomposed into three $\mathcal{C}_\infty$ gates, each of which has $T_1<2$. Hence through the decomposition we can bound its total teleportation depth by 6. However, to teleport U directly without decomposition via two-bit teleportation gives a bound of $T_2<4^1=4$ less than T_k.

Example 2. Consider a classical reversible circuit given in Fig. 8. We denote this series of three Toffoli gates as R_{c3}. This gate R_{c3} is not in $\mathcal{C}_k$ hierarchy as can be shown below.

Suppose that $R_{c3} \in \mathcal{C}_k$ is at certain level of the hierarchy; $R_{c3}X_1R_{c3}^\dagger$ must be a gate in $\mathcal{C}_{k-1}$. Calculating explicitly as in Fig. 9 we have that the non-Clifford part of the right-hand side of the equation is a series of two Toffoli gates, and we denote it as R_{c2}. Due to Proposition 3, R_{c2} is also in $\mathcal{C}_{k-1}$.

As shown in Fig. 10, conjugating X_1 by R_{c2} results in $LR_{c2}^\dagger$, where L is a Clifford operation. However, by exchanging the second and third qubits in Fig. 10, we find that $R_{c2}^\dagger X_1 R_{c2} = L' R_{c2}$, i.e., conjugating X_1 by $R_{c2}^\dagger$ gives back R_{c2}. Therefore, R_{c2} cannot be in the $\mathcal{C}_k$ hierarchy and we can conclude that R_{c3} is not a $\mathcal{C}_k$ gate either. ■

If we leave aside the problem of how to teleport gates beyond $\mathcal{C}_k$ fault tolerantly, we can teleport R_{c3} directly and

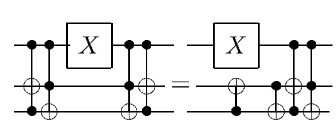

FIG. 10. Conjugating X_1 by R_{c2}.

obtain an upper bound of 2.75, which is less than $T_k=3$, the bound given by teleporting the three Toffoli gates separately.

V. CONCLUSION AND DISCUSSION

In this paper we address the following questions: What is the capacity of the teleportation scheme in practical implementation of fault-tolerant quantum computation and what is the most efficient way to make use of the teleportation protocol? To answer these questions we first notice that one-bit and two-bit teleportation schemes require different resources to implement and are of different capabilities. To understand what kind of gates can be teleported fault tolerantly with these two schemes, respectively, we study the structure of $\mathcal{C}_k$ hierarchy and its relationship with semi-Clifford operations. We show that for $n=1,2$, all the $\mathcal{C}_k$ gates are semi-Clifford operations, which is also true for $\{n=3,k=3\}$. However, this is no longer true for parameters $\{n>2,k>3\}$. Based on the counterexamples we constructed for $\{n=3,k\geq 3\}$, we conjecture that all $\mathcal{C}_3$ gates are semi-Clifford and all $\mathcal{C}_k$ gates are generalized semi-Clifford.

Such an understanding of the $\mathcal{C}_k$ structure has great implications on the optimal design of fault-tolerant architectures. While all $\mathcal{C}_k$ gates can be teleported fault tolerantly, the semi-Clifford subset of it requires less resources to implement than others. To quantify this notion of gate complexity in fault-tolerant quantum computation based on the $\mathcal{C}_k$ hierarchy, we introduce a measure called the teleportation depth T, which characterizes how many teleportation steps are necessary, on average, to implement a given gate. Using different teleportation schemes, we can give different upper bounds on T, for example, T_1, T_2, and T_k. The general assumption was that $T_1=T_2=T_k=T$. However, we showed in this work that, surprisingly, for certain series of gates T_1 could be strictly greater than T_k and T_k could also be strictly greater than T.

The ultimate understanding of the structure of $\mathcal{C}_k$ will provide a clearer clue on how to teleport circuits most efficiently. To achieve this goal, some results from other branches of mathematics might be helpful. It is noted that the Barnes-Wall lattices, whose isometry group is a subgroup of index 2 in the real Clifford group, have been extensively studied and recently their involutions have been classified [15]. It is our hope that the $\mathcal{C}_3$ structure might be further understood once we have a better understanding of the Clifford group.

For $n=1$, we fully characterize the structure of $\mathcal{C}_k$ by further study on the diagonal gates in $\mathcal{C}_k$, which form a group. It is interesting to note some evidence that $\mathcal{C}_k$ gates might be the only non-Clifford gates which could be transversally implemented on a stabilizer code [5]. We also fully characterize the structure of $\mathcal{C}_3$ for $n=3$, but this seems not directly related to allowable transversal non-Clifford gates on stabilizer codes. It is shown that those transversal non-Clifford gates are allowed only if they are generalized semi-Clifford [16]; therefore, we might expect some generalized semi-Clifford $\mathcal{C}_k$ gates transversally implementable on some stabilizer codes. We believe such kind of exploration on the relationship between transversally implementable gates and teleportable gates will shed some light on further understanding of practical implementation of fault-tolerant architectures.

ACKNOWLEDGMENTS

We thank Daniel Gottesman, Debbie Leung, and Carlos Mochon for comments.

APPENDIX A: SINGLE QUBIT $\mathcal{C}_k$ GATES

1. Single qubit gates with eigenvalues ±1

In this section we discuss what kind of single qubit unitary gates could have eigenvalues ± 1 apart from an overall phase factor, i.e., if λ_+,λ_- denote the two eigenvalues of a single qubit unitary U, then what is the condition under which $\lambda_+ + \lambda_- = 0$? This information is useful since only the unitary of this kind can be transformed into elements in the Pauli group under conjugation, i.e., there exists a unitary operator R, such that $RAR^\dagger = e^{i\theta}U$, where $A\in\mathcal{C}_1$. We will see that this kind of unitary has a very restricted form which is given by the following proposition.

Proposition 7. The single qubit unitary gates which have eigenvalues ± 1 apart from an overall phase factor could only be of the following two forms:

$$\Gamma_1(\varphi) = \begin{bmatrix} 0 & 1 \\ e^{i\varphi} & 0 \end{bmatrix}$$

or

$$\Gamma_2(\phi,\xi) = \begin{bmatrix} \cos\phi & \sin\phi e^{i\xi} \\ \sin\phi e^{-i\xi} & -\cos\phi \end{bmatrix}.$$

Proof. We begin to prove this proposition by writing down a general form of single qubit unitary gate as the following:

$$\Gamma = \begin{bmatrix} \cos\phi e^{i\theta} & \sin\phi e^{i\xi} \\ \sin\phi e^{-i\xi} & -\cos\phi e^{-i\theta} \end{bmatrix}. \tag{A1}$$

Direct calculation gives

$$\lambda_\pm = \frac{1}{2}\cos\phi e^{i\theta} - \frac{1}{2}\cos\phi e^{-i\theta} \pm \frac{1}{2}e^{-i\theta}(\cos\phi^2 e^{4i\theta} - 2\cos\phi^2 e^{2i\theta} + \cos\phi^2 + 4e^{2i\theta})^{1/2}. \tag{A2}$$

Therefore $\lambda_+ + \lambda_- = 0$ gives

$$\cos\phi\sin\theta = 0. \tag{A3}$$

If $\cos\phi=0$, the unitary must adopt the form of $\Gamma_1(\varphi)$; if $\sin\theta=0$, then apart from an overall phase, we can simply choose $\theta=0$, which leads to the form of $\Gamma_2(\phi,\xi)$. ■

Note that Γ_1 could be viewed as a special situation of Γ_2 for the case $\cos\phi=0$. However, we list Γ_1 separately for future convenience.

2. Gate series associated with $\Gamma_1(\varphi)$ and $\Gamma_2(\phi,\xi)$

In this section we investigate the gate series associated with $\Gamma_1(\varphi)$ and $\Gamma_2(\phi,\xi)$. It is obvious that if $\Gamma_1(\varphi)$, $\Gamma_2(\phi,\xi)\in\mathcal{C}_k$, then the unitary $U(\varphi)$ whose columns are the eigenvectors of $\Gamma_1(\varphi)$ or $\Gamma_2(\phi,\xi)$ might be in $\mathcal{C}_{k+1}$, given that $U(\varphi)ZU(\varphi)^\dagger=\Gamma_1(\varphi)$.

For $\Gamma_1(\varphi)$, the two normalized eigenvectors can be chosen as

$$|\Gamma_1(\varphi)\rangle_+=\frac{1}{\sqrt{2}}(|0\rangle+e^{i\varphi/2}|1\rangle),$$

$$|\Gamma_1(\varphi)\rangle_-=\frac{1}{\sqrt{2}}(|0\rangle-e^{i\varphi/2}|1\rangle). \tag{A4}$$

We now want a unitary whose columns are eigenvectors of $\Gamma_1(\varphi)$ apart from an overall factor of each eigenvector, i.e.,

$$U(\varphi,\alpha)=(e^{i\alpha}|\Gamma_1(\varphi)\rangle_+,|\Gamma_1(\varphi)\rangle_-)=\frac{1}{\sqrt{2}}\begin{bmatrix} e^{i\alpha} & 1\\ e^{i\alpha}e^{i\varphi/2} & -e^{i\varphi/2}\end{bmatrix}. \tag{A5}$$

If $U(\varphi,\alpha)\in\mathcal{C}_{k+1}$, then $U'=L_1U(\varphi,\alpha)L_2$ is also in $\mathcal{C}_{k+1}$. What is important for us is to find U', which is either of the form Γ_1 or Γ_2, then from its eigenvectors we can generate gates in $\mathcal{C}_{k+1}$. It is noticed that if we choose $\alpha=0$, then

$$U(\varphi,0)=(|\Gamma_1(\varphi)\rangle_+,|\Gamma_1(\varphi)\rangle_-)=\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1\\ e^{i\varphi/2} & -e^{i\varphi/2}\end{bmatrix} \tag{A6}$$

and

$$U(\varphi,0)HX=\begin{bmatrix} 0 & 1\\ e^{i\varphi/2} & 0\end{bmatrix}=\Gamma_1(\varphi/2). \tag{A7}$$

Later we will show that for all the allowed values of α, there exist $L_1,L_2\in\mathcal{C}_2$, such that $L_1U(\varphi,0)L_2=U(\varphi,\alpha)$, so it is sufficient to consider the case of $\alpha=0$.

Therefore we obtain a set of unitary given by

$$V_k(\varphi)=\Gamma_1(\varphi/2^k); \tag{A8}$$

if $\Gamma_1(\varphi)\in\mathcal{C}_2$ then $\Gamma_1(\varphi/2^k)$ could be in $\mathcal{C}_k$. We already know that $\Gamma(\pi/2)$ is in $\mathcal{C}_2$; then we have

$$V_k=\Gamma_1(2\pi/2^k) \tag{A9}$$

in $\mathcal{C}_k$.

Note that

$$S_kX=V_k, \tag{A10}$$

and we already know that $S_k\in\mathcal{C}_k$. Therefore by deriving V_k we obtain nothing new due to Proposition 1.

Now we come to the $\Gamma_2(\phi,\xi)$ case. Similarly, we begin from the two normalized eigenvectors of $\Gamma_2(\phi,\xi)$, which can be chosen as

$$|\Gamma_2(\phi,\xi)\rangle_+=\frac{1}{\sqrt{2}}\left(\cos\frac{\phi}{2}|0\rangle+\sin\frac{\phi}{2}e^{-i\xi}|1\rangle\right),$$

$$|\Gamma_2(\phi,\xi)\rangle_-=\frac{1}{\sqrt{2}}\left(\sin\frac{\phi}{2}e^{i\xi}|0\rangle-\cos\frac{\phi}{2}|1\rangle\right). \tag{A11}$$

We now construct a unitary whose columns are eigenvectors of $\Gamma_2(\varphi)$ apart from an overall factor of each eigenvector, i.e.,

$$U(\phi,\xi,\beta)=(e^{i\beta}|\Gamma_2(\phi,\xi)\rangle_+,|\Gamma_2(\phi,\xi)\rangle_-)=\frac{1}{\sqrt{2}}\begin{bmatrix} e^{i\beta}\cos\frac{\phi}{2} & \sin\frac{\phi}{2}e^{i\xi}\\ e^{i\beta}\sin\frac{\phi}{2}e^{-i\xi} & -\cos\frac{\phi}{2}\end{bmatrix}. \tag{A12}$$

If $U(\phi,\xi,\beta)\in\mathcal{C}_{k+1}$, then $U'=L_1U(\phi,\xi,\beta)L_2$ is also in $\mathcal{C}_{k+1}$. It is noticed that if we choose $\beta=0$, then

$$U(\phi,\xi,0)=(|\Gamma_2(\phi,\xi)\rangle_+,|\Gamma_2(\phi,\xi)\rangle_-)=\frac{1}{\sqrt{2}}\begin{bmatrix} \cos\frac{\phi}{2} & \sin\frac{\phi}{2}e^{i\xi}\\ \sin\frac{\phi}{2}e^{-i\xi} & -\cos\frac{\phi}{2}\end{bmatrix}. \tag{A13}$$

Also later we will show that for all the allowed values of α, there exist $L_1,L_2\in\mathcal{C}_2$, such that $L_1U(\phi,\xi,0)L_2=U(\phi,\xi,\beta)$, so it is sufficient to consider the case of $\beta=0$.

Therefore we obtain a set of unitary given by

$$W_k(\phi,\xi)=\Gamma_2(\phi/2^{k-1},\xi); \tag{A14}$$

if $\Gamma_2(\phi,\xi)\in\mathcal{C}_2$ then $\Gamma_1(\phi/2^{k-1},\xi)$ could be in $\mathcal{C}_k$. We already know that only when $\Gamma_2(\pi/4,0)$ is in $\mathcal{C}_2$, then we have

$$W_k=\Gamma_2(\pi/2^k,0) \tag{A15}$$

in $\mathcal{C}_k$.

Note that for other possible values of ϕ and ξ, it is straightforward to show that there exist $L_1,L_2\in\mathcal{C}_2$, such that $L_1\Gamma_2(\pi/4,0)L_2=\Gamma_2(\phi,\xi)$, so it is sufficient to consider the case of $\phi=\pi/4$ and $\xi=0$.

Note that

$$HPW_kPX\sim S_k, \tag{A16}$$

where $\sim$ means up to an overall phase, and we already know that $S_k\in\mathcal{C}_k$. Therefore again by deriving W_k we obtain nothing new due to Proposition 1.

3. Gates in $\mathcal{C}_k\backslash\mathcal{C}_{k-1}$ for single qubit

We conclude this section by presenting the following proposition, which gives the structure of gates in $\mathcal{C}_k\backslash\mathcal{C}_{k-1}$ for a single qubit.

Proposition 8. The set $\mathcal{C}_k\backslash\mathcal{C}_{k-1}$ for a single qubit is given by

$$L_1S_kL_2\in\mathcal{C}_k, \tag{A17}$$

where $L_1,L_2\in\mathcal{C}_2$, $k\geq 2$.

Proof. We almost reached the proof of this proposition by considering the results in Appendixes A 1 and A 2. The only problems left we need to clarify are the following.

(1) What happens when $\mathcal{C}_k$ is diagonal, which cannot be directly obtained by considering the eigenvectors of V_{k-1} and W_{k-1}. The answer is already known, since S_k is the only diagonal gate in $\mathcal{C}_k \backslash \mathcal{C}_{k-1}$.

(2) The values of α and β. This can be answered by noting the fact that the equations

$$UZU^{\dagger} = G_1,$$

$$UXU^{\dagger} = G_2, \tag{A18}$$

with G_1, G_2 known totally determines U up to an overall phase. Let us start from

$$U(\varphi,\alpha) = \frac{1}{\sqrt{2}}\begin{bmatrix} e^{i\alpha} & 1 \\ e^{i\alpha}e^{i\varphi/2} & -e^{i\varphi/2} \end{bmatrix}. \tag{A19}$$

Note that $U(\varphi,\alpha)ZU(\varphi,\alpha)^{\dagger} \sim \Gamma_1(2\phi)$ and

$$U(\varphi,\alpha)XU(\varphi,\alpha)^{\dagger} = \frac{1}{\sqrt{2}}\begin{bmatrix} \cos\alpha & \sin\alpha e^{-i2\varphi} \\ \sin\alpha e^{i2\varphi} & -\cos\alpha \end{bmatrix}. \tag{A20}$$

■

APPENDIX B: DETAILED ANALYSIS ABOUT $\mathcal{C}_3$

1. Notations

Let us first define some notations.

Recall $\mathcal{P}_n$ is the Pauli group for n qubit with order 4^{n+1}. Now let $\widetilde{\mathcal{P}}_n$ be the quotient group $\mathcal{P}_n/Z(\mathcal{P}_n)$ with order 4^n.

Let $\mathcal{C}_2(n)$ denote the Clifford group for n qubit. Define the quotient group $\widetilde{\mathcal{C}}_2(n)=\mathcal{C}_2(n)/Z(\mathcal{C}_2(n))$. Since $\widetilde{\mathcal{P}}_n$ is a normal subgroup of $\widetilde{\mathcal{C}}_2(n)$, we could further define a quotient group $\hat{\mathcal{C}}_2(n)=\widetilde{\mathcal{C}}_2(n)/\widetilde{\mathcal{P}}_n \cong \mathrm{Sp}(2n,2)$. Note that $\mathrm{Sp}(2,2)\cong S_3$ and $\mathrm{Sp}(4,2)\cong S_6$. Denote the set $\mathcal{K}(n)=\{A \mid A\in \mathrm{Sp}(2n,2), A^2=1\}$, i.e., $\mathcal{K}(n)$ are the set of all involutions of the symplectic group $\mathrm{Sp}(2n,2)$.

Denote the order of maximal Abelian subgroup of $\mathcal{K}(n)$ by $a(n)$. Hence $a(1)=2$, $a(2)=8$, $a(n)\le 2^{\frac{n(n+1)}{2}}$ [17].

Define the set $\mathcal{M}(n)=\{U \mid U\in \widetilde{\mathcal{C}}_2(n)\backslash \widetilde{\mathcal{P}}_n \cup \{I\}\}$.

Now recall the definition for $\mathcal{C}_k(n)$:

$$\mathcal{C}_k(n) = \{U \mid UP_nU^{\dagger} \in \mathcal{C}_{k-1}(n)\}. \tag{B1}$$

For any n-qubit $U\in\mathcal{C}_k(n)$, the group $G_U(n)$ is defined by $G_U(n)=U\widetilde{\mathcal{P}}_nU^{\dagger}$.

Define the set $\mathcal{R}_k(n)=\{U \mid U\in\widetilde{\mathcal{C}}_k(n), W^{\dagger}=W, \mathrm{Tr}(W)=0\}$.

And the set $\mathcal{F}_k(n)=\{U \mid U\in\widetilde{\mathcal{C}}_k(n),\ U \text{ is diagonal}\}$.

Denote the group generated by $\{A_i\}_{i=1}^n$ by $\langle\{A_i\}_{i=1}^n\rangle$ for any set of operators A_i.

2. Some facts for calculating $\mathcal{C}_3$ structure

We state some simple facts about $\mathcal{C}_3$ structure which we use to verify Theorem 3 numerically.

Fact 1. We could always choose $G_U(n)\subset\mathcal{R}_{k-1}(n)$ for any U in $\mathcal{C}_k(n)$, because we can always choose Hermitian and trace zero elements in $\mathcal{P}_n$ as the representative element for each element in $\widetilde{\mathcal{P}}_n$.

Fact 2. If all $n-1$-qubit $\mathcal{C}_k$ gates are semi-Clifford, and if $G_U(n)\supset\langle\{B_i\}_{i=1}^n\rangle$, where $B_i\in\widetilde{\mathcal{P}}_n$ and $B_i\neq B_j$, $B_iB_j\neq B_k$ for $i\neq j\neq k$, then $G_U(n)\cap\widetilde{\mathcal{P}}_n\subset K_Z(n)$, because if $\langle\{B_i\}_{i=1}^n\rangle\neq K_Z(n)$, then $U(n)$ could be reduced to $U(1)\otimes U(n-1)$ via Clifford operation.

Fact 3. If $A,B\in\mathcal{M}(n)\cap\mathcal{R}_2(n)$, and A,B correspond to the same element in $\hat{\mathcal{C}}_2(n)$, then $AB\in\mathcal{P}_n$, because if A,B correspond to the same element in $\hat{\mathcal{C}}_2(n)$, then there exists $\alpha\in\widetilde{\mathcal{P}}_n$ such that $A=\alpha B$.

Fact 4. For any n-qubit $\mathcal{C}_3$ gate U, if $G_U(n)\supseteq\langle\{Z_i\}_{i=1}^m\rangle$, where $m\le n$, then the quotient group $G_U(n)/\langle\{Z_i\}_{i=1}^m\rangle\in\mathcal{K}(n)$ is Abelian, because elements of $G_U(n)\in\widetilde{\mathcal{C}}_2(n)$ are either commuting or anticommuting, the corresponding elements in $\hat{\mathcal{C}}_2(n)$ should commute.

3. $n=1$ case

Since $\mathrm{Sp}(2,2)\cong S_3$, $a(1)=2<4$. Hence $G_U(2)\cap\widetilde{\mathcal{P}}_2$ contains at least one element in $\widetilde{\mathcal{P}}_1$, i.e., $G_U(1)\cap\widetilde{\mathcal{P}}_1\supseteq K_Z(1)$ holds for any single qubit $\mathcal{C}_3$ gate.

Furthermore, it is noted that any $U\in\mathcal{R}_k(1)$ can be parametrized by

$$U(\theta,\varphi) = \begin{bmatrix} \cos\theta & \sin\theta e^{i\varphi} \\ \sin\theta e^{-i\varphi} & -\cos\theta \end{bmatrix},$$

and starting from elements in $\mathcal{R}_2(1)$ and calculating their eigenvectors, we understand that φ can only be of the values $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ for $\cos\theta\neq 0$. This directly leads to the fact that all $\mathcal{C}_3(1)$ gates are semi-Clifford.

4. $n=2$ case

Since $\mathrm{Sp}(4,2)\cong S_6$, $a(2)=8<16$. Hence $G_U(2)\cap\widetilde{\mathcal{P}}_2$ contains at least one element in $\widetilde{\mathcal{P}}_2$. However, this is not enough to claim $G_U(2)\cap\widetilde{\mathcal{P}}_2$ holds for any two-qubit U. We need to examine the structure of $G_U(2)\cap\widetilde{\mathcal{P}}_2$ in more detail.

Considering the maximal Abelian subgroup in $\mathcal{K}(2)$ of order 8, and its corresponding elements in $\widetilde{\mathcal{C}}_2(n)$, direct calculation shows it does not contain a subgroup of structure $\widetilde{\mathcal{P}}_1\times Z_2$. Hence we need to further consider Abelian subgroup in $\mathcal{K}(2)$ of order 4. Due to Lemma 3, we result in $G_U(2)\cap\widetilde{\mathcal{P}}_2\supseteq K_Z(2)$ holds for any two-qubit $\mathcal{C}_3$ gate.

Then using Lemma 1 and Lemma 2, we could calculate $\mathcal{C}_4(2)$ numerically. The result then shows that all the $\mathcal{C}_3(2)$ gates are semi-Clifford.

5. $n=3$ case

Since $a(3)=64$, and direct calculation of this group shows that not all the elements could be in $\mathcal{R}_2(3)$, hence $G_U(3)\cap\widetilde{\mathcal{P}}_3$ contains at least one element in $\widetilde{\mathcal{P}}_3$. Again, this is not enough to claim $G_U(3)\cap\widetilde{\mathcal{P}}_3\supseteq K_Z(3)$ holds for any three-qubit U. We need to examine the structure of $G_U(3)\cap\tilde{\mathcal{P}}_3$ in more detail to dig out two more elements in $\tilde{\mathcal{P}}_3$.

Using Facts 1, 2, and 3, we could calculate $\mathcal{C}_3(3)$ numerically. The result shows that the conjecture is also true in this case. See the next section for more about $\mathcal{C}_3(3)$.

6. Diagonal gates in $\mathcal{C}_3$

Define a diagonal matrix A by $A_{jk}=\delta_{jk}e^{i\theta_j}$, where $j=1,\ldots,N$, $N=2^n$, for the n-qubit case.

We now prove the following:

Lemma 1. If $A\in\mathcal{C}_3$, if we choose $A_{11}=1$, then $A_{jj}=e^{im_j\pi/4}$ for any $j\neq 1$, where m_j are some integers.

Proof. We first prove for $j=N$. Note that we choose $A_{11}=1$ to cancel out the overall phase of A. Denote $A'=X^{\otimes n}AX^{\otimes n}A^{\dagger}$, and $A''=X^{\otimes n}A'X^{\otimes n}A'^{\dagger}$. Note that A', A'' are also diagonal. Since $A\in\mathcal{C}_3$, A'' must be in Pauli apart from an overall phase. And we also have $A''_{11}=e^{2i\theta_N}$, $A''_{NN}=e^{-2i\theta_N}$. Hence we must have $\frac{A''_{11}}{A''_{NN}}=e^{4i\theta_N}=\pm 1$, i.e., $\theta=\frac{m_N\pi}{4}$ for some integer m_N.

For $j\neq N$, there always exists a Clifford group operation which keeps $|j\rangle$ invariant but maps $|1\rangle\leftrightarrow|N+1-j\rangle$. Hence the above procedure applies to any $j\neq N$. ■

Note that the similar idea applies to the diagonal $\mathcal{C}_k$ gates, i.e., if $A\in\mathcal{C}_k$, if we choose $A_{11}=1$, $A_{jj}=e^{im_j\pi/2^{k-1}}$ for any $j\neq 1$, where m_j are some integers.

Now we consider some concrete gates:

Proposition 9. For $n=3$, the three-qubit diagonal $\mathcal{C}_3$ gates are given by a group generated by the $\pi/8$ gate, control-phase gate, and control-control-Z gate.

Proof. The proof is directly given by numerical calculation, based on Lemma 1. ■

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

[2] J. Preskill, in *Introduction to Quantum Computation and Information*, edited by H. K. Lo, S. Popescu, and T. Spiller (World Scientific Publishing Company, Singapore 2001), pp. 213–269.

[3] P. Shor, *37th Symposium on Foundations of Computing* (IEEE Computer Society Press, Los Alamitos, CA, 1996), pp. 56–65.

[4] D. Gottesman, in *Encyclopedia of Mathematical Physics*, edited by J.-P. Francoise, G. L. Naber, and S. T. Tsou (Elsevier, Oxford, 2006), Vol. 4, pp. 196–201.

[5] B. Zeng, A. W. Cross, and I. L. Chuang, e-print arXiv: 0706.1382.

[6] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).

[7] Sergei Bravyi and Alexei Kitaev, Phys. Rev. A **71**, 022316 (2005).

[8] X. Zhou, D. W. Leung, and I. L. Chuang, Phys. Rev. A **62**, 052316 (2000).

[9] D. Gross and M. Van den Nest, Quantum Inf. Comput. **8**, 263 (2008).

[10] D. Gottesman, e-print arXiv:quant-ph/9705052.

[11] GAP—Groups, Algorithms, Programming—A System for Computational Discrete Algebra, http://www.gap-system.org/

[12] A. Yao, *Proceedings of Thirty-fourth IEEE Symposium on Foundations of Computer Science* (IEEE, Palo Alto, CA, 1993), pg. 352

[13] M. Mottonen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, Quantum Inf. Comput. **5**, 467 (2005).

[14] V. V. Shende, S. S. Bullock, and I. L. Markov, IEEE Trans. Comput.-Aided Des. **25**, 1000 (2006).

[15] R. L. Griess, Jr., e-print arXiv:math.GR/0511084.

[16] X. Chen, H. Chung, A. W. Cross, B. Zeng, and I. L. Chuang, e-print arXiv:0801.2360.

[17] M. J. J. Barry, J. Aust. Math. Soc. Ser. B, Appl. Math. **27**, 59 (1979).