CHARACTERIZATION OF PERMUTATION GATES IN THE THIRD LEVEL OF THE CLIFFORD HIERARCHY

ZHIYANG HE, LUKE ROBITAILLE, AND XINYU TAN

The Clifford hierarchy is a ubiquitous structure in quantum computation which classifies unitary operations based on their conjugate actions on the Pauli group. Precisely, the first level $\mathcal{C}_1$ of the hierarchy $\mathcal{CH}$ is the Pauli group $\mathcal{P}$, and its subsequent levels are defined recursively: $\mathcal{C}_k$ is the set of all unitaries U such that $UPU^\dagger \in \mathcal{C}_{k-1}$ for all Pauli operators P. Within $\mathcal{CH}$, gates in the third level are of unique importance to the study of fault-tolerant quantum computation (FTQC) [Sho95; Sho96; Got97], as established by several foundational works. The Gottesman-Knill theorem [Got98] states that any circuits made of Pauli and Clifford gates, which are the first two levels of $\mathcal{CH}$, can be efficiently simulated by a classical computer. In contrast, adding any non-Clifford gate to the Clifford group forms a universal gate set. Among the non-Clifford unitaries, gates in $\mathcal{CH}$ can be implemented fault-tolerantly by gate teleportation [GC99], where higher-level gates are performed using resource states and lower-level gates. From this perspective, gates in $\mathcal{C}_3$ are the "easiest-to-implement" non-Clifford gates. Consequently, $\mathcal{C}_3$ gates have been at the center of study for FTQC, with decades of extensive research studying their fault-tolerant implementations [Sho96; BK05], synthesis into unitaries [DN05], algorithmic resource costs [Dal+23], and more.

Despite its importance, the mathematical structure of the Clifford hierarchy is not well understood. There is no known closed-form characterization, which means the precise set of gates in $\mathcal{C}_k$ for $k \geq 3$ is unknown. In particular, $\mathcal{C}_k$ is neither closed under multiplication nor closed under inverse for any $k \geq 3$. Ample work has been done to elucidate structures within the hierarchy, which we review in Section 1.3. In this paper, we study the permutation gates, which are n-qubit unitaries that permute the 2^n computational basis states, in $\mathcal{C}_3$. We denote these gates by $\mathcal{C}_3^{\text{sym}}$, and remark that they are both interesting and important for a few reasons.

(1) Permutation gates correspond to all reversible classical computations on n bits. Gates in $\mathcal{C}_3$, on the other hand, can be implemented fault-tolerantly using resource states and Clifford gates. $\mathcal{C}_3^{\text{sym}}$ therefore captures classical gates and computational subroutines which are relatively low-cost to implement for FTQC. The canonical example is the Toffoli gate TOF, which is classically universal and ubiquitous in quantum circuits.

(2) Unfortunately, products of Toffoli gates (which capture all permutations) are notoriously unruly. For instance, while a single Toffoli gate is in $\mathcal{C}_3$, a product of as few as two Toffoli gates can leave the hierarchy.[1] Prior work by Anderson [And24] conjectured that $\mathcal{C}_3^{\text{sym}}$ are precisely products of pairwise commuting Toffoli gates (up to multiplying on both sides by Clifford permutations), and that $\mathcal{C}_k^{\text{sym}}$ is closed under inverse for all k. We disprove both of these conjectures in this work.

(3) Furthermore, permutation gates are important components for gates in $\mathcal{CH}$. Beigi and Shor [BS09] proved that all gates in $\mathcal{C}_3$ are *generalized semi-Clifford*, which means they can be written as $\phi_1 \pi d \phi_2$ for Clifford gates ϕ_1, ϕ_2, a diagonal gate d, and a permutation gate π. The conjecture that all gates in $\mathcal{CH}$ are generalized semi-Clifford remains open [ZCC08]. In [CGK17], Cui, Gottesman, and Krishna fully characterized all the diagonal gates in $\mathcal{CH}$. Therefore, characterizing the permutation gates is a crucial step towards characterizing all gates in $\mathcal{C}_3$ and potentially $\mathcal{CH}$.

In this work, we present a complete characterization of $\mathcal{C}_3^{\text{sym}}$ (Result 1, Result 2), elucidating an essential substructure of $\mathcal{C}_3$. We further present a family of gates in $\mathcal{C}_3^{\text{sym}}$ that disproves Anderson's conjectures and challenges conventional understanding of $\mathcal{C}_3$ (Result 3). Finally, we derive lower

[1] Specifically, $\text{TOF}_{1,2,3}\text{TOF}_{1,3,2}$ is not in $\mathcal{CH}$; see equation (E.2) of [And24].

bounds on the number of qubits a gate in $\mathcal{C}_3^{\text{sym}}$ must be supported on, showing that our construction is optimal (Result 4).

For TQC Reviewers, an earlier version of this work [HRT24] was submitted to TQC 2025. [HRT24] made preliminary progress and proved Result 1, but did not have any of Results 2 to 4. Our new collection of results is significantly stronger, which we detail next.

Main results and techniques

To characterize the gates in $\mathcal{C}_3^{\text{sym}}$, we study structured products of Toffoli gates. We define a product of distinct Toffoli gates to be in *staircase form* if each gate $\text{TOF}_{i,j,k}$ in the product has $i, j < k$ and the target qubit indices are nondecreasing in the order that the gates are applied. For example, the gate in Fig. 1 is in staircase form.

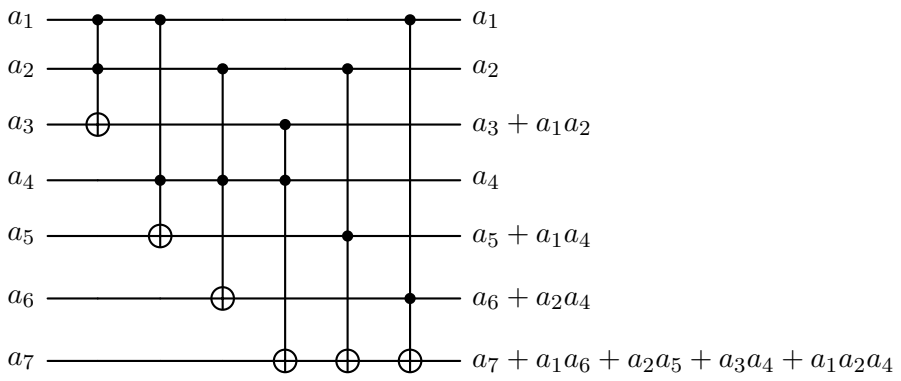

FIGURE 1. A permutation gate in staircase form, consisting of 6 Toffoli gates.

Our first main result, which was presented in an earlier version of this paper [HRT24], states that every permutation in $\mathcal{C}_3^{\text{sym}}$ can be written in staircase form (up to multiplying on both sides by Clifford permutations).

Result 1. If $\pi \in \mathcal{C}_3$ is a permutation gate, then there exist Clifford permutations ϕ_1, ϕ_2 and a product μ of Toffoli gates in *staircase form* such that $\mu \in \mathcal{C}_3$ and $\pi = \phi_1 \mu \phi_2$.

We remark that there are permutations in staircase form which are not in $\mathcal{C}_3$. To derive a full characterization, we consider bilinear products defined over vectors of $\mathbb{F}_2^n$, which we denote by juxtaposition. For a commutative and associative bilinear product, we call it a *descending multiplication* if it is associative and commutative and, for standard basis vectors $\{e_i\}_{i\in[n]}$, it holds that $e_i e_i = 0$, and $e_i e_j$ (for $i < j$) is in the span of $\{e_k : k > j\}$. Our second main result identifies a one-to-one correspondence between gates in $\mathcal{C}_3^{\text{sym}}$ and descending multiplications.

Result 2. Every staircase form permutation gate in $\mathcal{C}_3$ induces a descending multiplication over $\mathbb{F}_2^n$. In correspondence, every descending multiplication over $\mathbb{F}_2^n$ induces a staircase form permutation gate in $\mathcal{C}_3$.

Using this characterization, we construct a novel family of permutation gates in $\mathcal{C}_3$. For each integer $k \geq 3$, we take $n = 2^k - 1$ and label a basis of $\mathbb{F}_2^n$ as e_S for nonempty subsets $S \subseteq [n]$. Define a bilinear product operation by setting $e_S e_T = e_{S \cup T}$ if $S \cap T = \emptyset$, and $e_S e_T = 0$ if $S \cap T \neq \emptyset$, and extending linearly. This gives a descending multiplication, which induces a staircase form $\mathcal{C}_3$ permutation gate U_k.

Result 3. For all $k \geq 3$, we have $U_k \in \mathcal{C}_3$ but $U_k^\dagger \notin \mathcal{C}_k$.

We note that the permutation in Fig. 1 is precisely U_3. This construction brings new understanding to the study of $\mathcal{C}_3$ gates in a few ways. First of all, $\{U_k\}_k$ are the first examples of permutation gates

in $\mathcal{C}_3$ whose inverses leave $\mathcal{C}_3$ (in fact, leave any fixed level of $\mathcal{CH}$). As a result, they disprove both conjectures of Anderson [And24]. Previously, Gottesman and Mochon presented a gate in $\mathcal{C}_3$ (which is not a permutation, see Lemma 2.6 of main text) whose inverse is not in $\mathcal{C}_3$. Our U_3 is actually equivalent to their example up to conjugation by a Clifford gate.

The permutation implemented by U_k is also interesting. For a permutation π on n bits, we represent it by n Boolean polynomials in the n input variables, one polynomial for each output bit. For example, $\mathrm{CNOT}_{1,2}$ maps $(a_1, a_2) \mapsto (a_1, a_2 + a_1)$ and $\mathrm{TOF}_{1,2,3}$ maps $(a_1, a_2, a_3) \mapsto (a_1, a_2, a_3 + a_1 a_2)$. For U_k, if we consider qubits $1, 2, 4, 8, \ldots, 2^{k-1}$ as "controls", and set the other $2^k - 1 - k$ "ancilla" input variables to be zero, then the $2^k - 1$ output polynomials representing U_k are precisely all the non-constant monomials of $a_1, a_2, a_4, a_8, \ldots, a_{2^{k-1}}$. In other words, arbitrarily powerful classical computation can be implemented using one $\mathcal{C}_3$ gate followed by CNOT gates, at the expense of a large number of ancilla qubits. This extra ancilla cost is, in fact, optimal: using the characterization with descending multiplications, we show the following lower bound.

Result 4. Any permutation gate in $\mathcal{C}_3$ with a polynomial of degree at least k must be supported on at least $2^k - 1$ qubits.

These results open a few exciting future directions to be pursued, which we discuss next.

Future directions

Combining these four results, our characterization discovers and delineates a novel design space within $\mathcal{C}_3^{\mathrm{sym}}$. By constructing descending multiplications, which are much easier to reason with than Toffoli circuits, we can derive permutation gates in $\mathcal{C}_3$ that encode different classical computations. These computations can then be implemented in FTQC via gate teleportation, where the majority of the cost is offloaded to resource state preparation. It would be interesting to explore whether the cost of important FTQC primitives, such as arithmetic, can be reduced with this approach.

In addition to gate design and teleportation, it would be interesting to explore whether our results can be generalized to higher levels of $\mathcal{CH}$. Evidently, characterizing more or all of the permutation gates in $\mathcal{CH}$ is consequential to our understanding of $\mathcal{CH}$. Our results mark a significant step in this direction.

Another important direction of research is to understand the product of permutation and diagonal gates. Significant progress was made in [And24], where Anderson showed several results which, in the case of $\mathcal{C}_3$, imply that if $\pi d \in \mathcal{C}_3$, then $\pi \in \mathcal{C}_3$ and $d \in \mathcal{CH}$. Since every gate in $\mathcal{C}_3$ is generalized semi-Clifford, given our characterization of permutation gates in $\mathcal{C}_3$ and the characterization of diagonal gates in $\mathcal{CH}$ by [CGK17], can we characterize all of $\mathcal{C}_3$? Such a characterization would have significant implications for our study of FTQC, given the unique importance of $\mathcal{C}_3$ gates.

Finally, our Result 4 raises an interesting complexity theory question. Specifically, while $\{U_k\}_k$ demonstrate that polynomials of arbitrarily high degree can be encoded into a single $\mathcal{C}_3$ gate, such encodings necessarily incur an exponential ancilla cost. In contrast, implementing a degree k monomial in $\mathcal{C}_{k+1}$ takes only one k-controlled NOT gate, supported on $k + 1$ qubits. How does this tradeoff between polynomial degree and ancilla cost transform through the different levels of $\mathcal{CH}$? What implications does this tradeoff have on the fundamental cost of gate teleportation, which is ubiquitous in FTQC?

As the study of the Clifford hierarchy continues, our work elucidates important substructures and pathways in this structure-elusive space. We believe our results are of theoretical significance for the study of FTQC as well as quantum information more generally, and align well with the interests of the broad audience at TQC.

References

[And24] Jonas T. Anderson. *On Groups in the Qubit Clifford Hierarchy* (2024). In: *Quantum* 8, p. 1370.

[BK05] Sergey Bravyi and Alexei Kitaev. *Universal quantum computation with ideal Clifford gates and noisy ancillas* (2005). In: *Phys. Rev. A* 71 2, p. 022316.

[BS09] Salman Beigi and Peter W. Shor. *C_3, Semi-Clifford and Generalized Semi-Clifford Operations* (2009).

[CGK17] Shawn X. Cui, Daniel Gottesman, and Anirudh Krishna. *Diagonal gates in the Clifford hierarchy* (2017). In: *Phys. Rev. A* 95 1, p. 012329.

[Dal+23] Alexander M Dalzell, Sam McArdle, Mario Berta, Przemyslaw Bienias, et al. *Quantum algorithms: A survey of applications and end-to-end complexities* (2023). In: *arXiv preprint arXiv:2310.03011*.

[DN05] Christopher M Dawson and Michael A Nielsen. *The solovay-kitaev algorithm* (2005). In: *arXiv preprint quant-ph/0505030*.

[GC99] Daniel Gottesman and Isaac L. Chuang. *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations* (1999). In: *Nature* 402.6760, pp. 390–393.

[Got97] D. Gottesman. *Stabilizer Codes and Quantum Error Correction* (1997). In: *arXiv:quant-ph/9705052*.

[Got98] Daniel Gottesman. *The Heisenberg Representation of Quantum Computers* (1998).

[HRT24] Zhiyang He, Luke Robitaille, and Xinyu Tan. *Permutation gates in the third level of the Clifford hierarchy* (2024). In: *arXiv preprint arXiv:2410.11818*.

[Sho95] Peter W Shor. *Scheme for reducing decoherence in quantum computer memory* (1995). In: *Physical review A* 52.4, R2493.

[Sho96] P.W. Shor. *Fault-tolerant quantum computation* (1996). In: *Proceedings of 37th Conference on Foundations of Computer Science*. Pp. 56–65.

[ZCC08] Bei Zeng, Xie Chen, and Isaac L. Chuang. *Semi-Clifford operations, structure of C_k hierarchy, and gate complexity for fault-tolerant quantum computation* (2008). In: *Phys. Rev. A* 77 4, p. 042313.