Permutation gates in the third level of the Clifford hierarchy

Zhiyang He*, Luke Robitaille*, and Xinyu Tan*

*Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, USA

The Clifford hierarchy

- Let $\mathcal{C}_1 = \mathcal{P}$ be the Pauli group on n qubits, and inductively define
$$\mathcal{C}_k = \{U : \forall P \in \mathcal{P}, UPU^{-1} \in \mathcal{C}_{k-1}\}.$$
The Clifford Hierarchy is defined as $\mathcal{CH} := \cup_{k=1}^{\infty} \mathcal{C}_k$; we say $\mathcal{C}_k$ is its kth layer.
- $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \mathcal{C}_3 \subseteq \cdots$ where $\mathcal{C}_1$ is the Pauli group, and $\mathcal{C}_2$ is the Clifford group. Non-Clifford gates are necessary for universal quantum computation!
- The Clifford hierarchy was introduced by Gottesman and Chuang [1] in 1999 in the context of gate teleportation, but has since been studied in its own right.
- For $k \geq 3$, $\mathcal{C}_k$ is not a group! For such a fundamental object in quantum computation, the structure of $\mathcal{CH}$ is not well understood.

What is known?

There has been lots of work aiming to understand the structure of $\mathcal{CH}$ or $\mathcal{C}_3$.

- A semi-Clifford gate is $\phi_1 d \phi_2$ for Clifford gates ϕ_1, ϕ_2 and diagonal gate d.
- A generalized semi-Clifford gate is $\phi_1 \pi d \phi_2$ for Clifford gates ϕ_1, ϕ_2, permutation gate π, and diagonal gate d.
- Zeng, Chen, and Chuang [2] conjectured in 2007 that all elements of $\mathcal{C}_3$ are semi-Clifford, and all elements of $\mathcal{CH}$ are generalized semi-Clifford.
- Beigi and Shor [3] showed in 2008 that all elements of $\mathcal{C}_3$ are generalized semi-Clifford. We don't know if this is true for higher levels!
- Gottesman and Mochon [3] gave a non-semi-Clifford element of $\mathcal{C}_3$ on $n = 7$ qubits, as shown in Figure 1. Before our paper, this was the only known example of a non-semi-Clifford $\mathcal{C}_3$ gate!

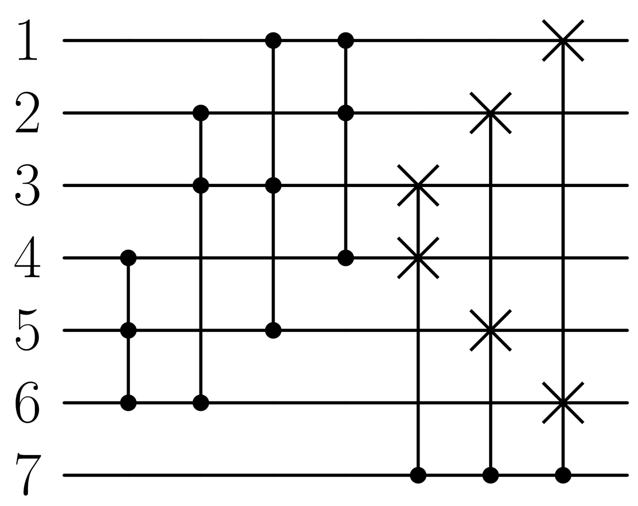

Figure 1: $\text{CSWAP}_{7,1,6}\text{CSWAP}_{7,2,5}\text{CSWAP}_{7,3,4} \cdot \text{CCZ}_{1,2,4}\text{CCZ}_{1,3,5}\text{CCZ}_{2,3,6}\text{CCZ}_{4,5,6}$.

Permutation gates in $\mathcal{C}_3$ are staircases

- A permutation gate is a gate that permutes the computational basis states; there are $(2^n)!$ permutation gates on n qubits.
- For example, X gates and CNOT gates are permutation gates.
- A Toffoli gate acts on three qubits by
$$|a_1\rangle \otimes |a_2\rangle \otimes |a_3\rangle \mapsto |a_1\rangle \otimes |a_2\rangle \otimes |a_3 + a_1a_2\rangle.$$
We denote by $\text{TOF}_{i,j,k}$ a Toffoli gate with qubits i and j as controls and qubit k as target.

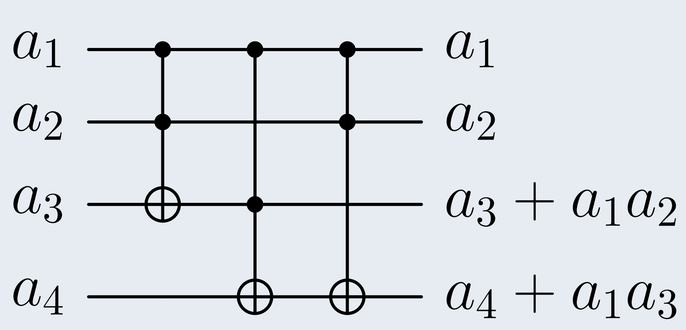

Figure 2: This circuit is for $\text{TOF}_{1,2,4}\text{TOF}_{1,3,4}\text{TOF}_{1,2,3}$.

- Permutation gates are important for implementing circuits and algorithms, such as a quantum adder.

- We say that a product of distinct Toffoli gates is in staircase form if
  - each gate $\text{TOF}_{i,j,k}$ that appears has $i < j < k$, and
  - the target qubits are in nondecreasing order in the order the gates are applied.

  For example, Figures 2 and 3 are in staircase form.

Result 1: Any permutation gate in $\mathcal{C}_3$ can be written as a product of Toffoli gates in staircase form, up to multiplying by Clifford permutations on both sides.

- However, not every product of Toffoli gates in staircase form is in $\mathcal{C}_3$.

A family of non-semi-Clifford $\mathcal{C}_3$ permutations

- We reject two conjectures of Anderson [4]:

Result 2: Not all permutations in $\mathcal{C}_3$ are semi-Clifford, and $n = 7$ is the smallest number of qubits for which a non-semi-Clifford $\mathcal{C}_3$ permutation gate exists.

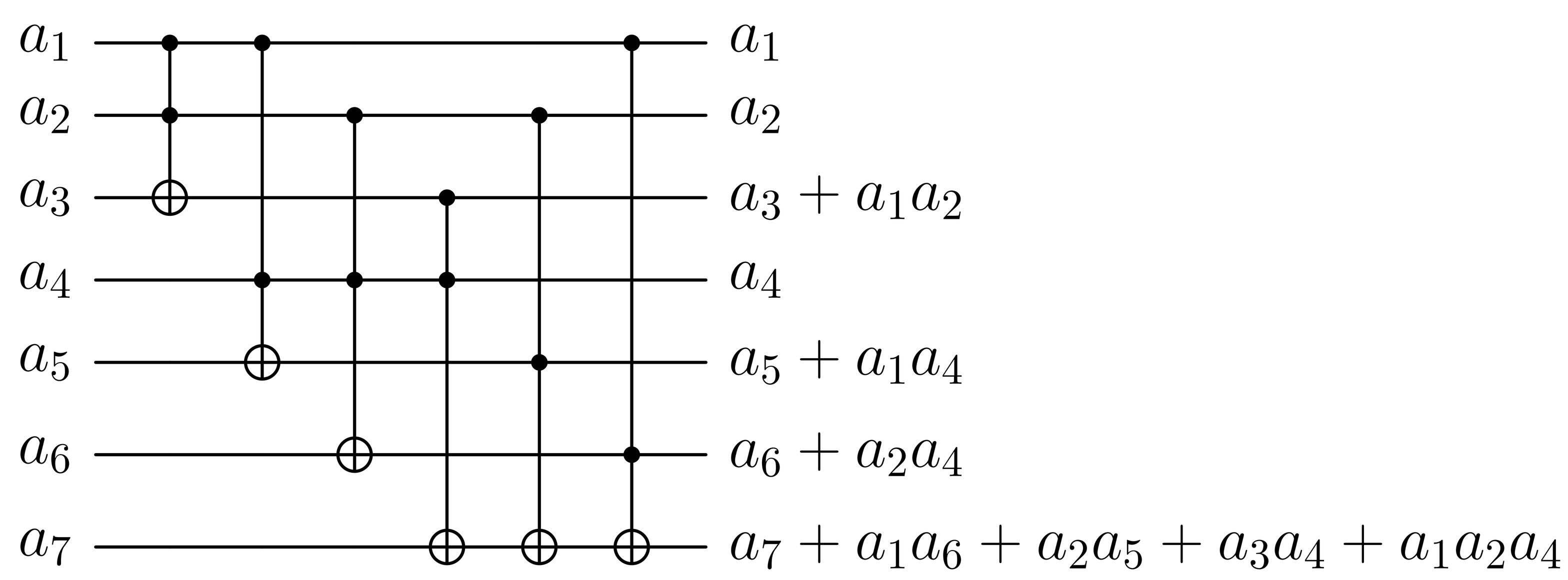

Figure 3: The above gate, denoted as U_3, is in $\mathcal{C}_3$ but not semi-Clifford because $U_3^{-1} \notin \mathcal{C}_3$. In fact, this gate is conjugate to the gate in Figure 1 by a Clifford gate.

- More surprisingly, this U_3 gate in Figure 3 is the first gate in an infinite family!

Result 3: For each $k \geq 3$, we find a permutation gate U_k on $n = 2^k - 1$ qubits such that $U_k \in \mathcal{C}_3$ but $U_k^{-1} \notin \mathcal{C}_k$. Furthermore, U_k achieves the minimal number of qubits for a $\mathcal{C}_3$ permutation containing a degree-k monomial (e.g., U_3 has $a_1a_2a_4$).

- Construction of U_k:
  - for each pair of indices $i < j$ that do not have any 1s in the same place as each other in binary, apply $\text{TOF}_{i,j,i+j}$;
  - specifically, apply these Toffoli gates in nondecreasing order of target gate (so the result is in staircase form).
- What does this family of gates mean operationally?—There exist gates with cheap fault-tolerant implementation via gate teleportation (level-three), yet whose inverses can be made arbitrarily costly (can lie at any prescribed level).

A bijection to descending multiplications

- We say that a map $\mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$, denoted by juxtaposition, is a descending multiplication if
  - it is linear in each coordinate (distributive), associative, and commutative,
  - for all $i \in [n]$, we have $e_ie_i = e_i^2 = 0$, and
  - for all $i < j \in [n]$, we have e_ie_j is in the span of $\{e_k : k > j\}$.

  Here $e_1, \ldots, e_n$ is the standard basis of $\mathbb{F}_2^n$.

Result 4: There is a bijection between descending multiplications and permutations in $\mathcal{C}_3$ that can be written in staircase form.

- A multiplication and its corresponding gate π satisfy $\pi|e_i + e_j\rangle = |e_i + e_j + e_ie_j\rangle$.

Summary of our main results

- Any permutation in $\mathcal{C}_3$ can be written, up to multiplying by Clifford permutations on both sides, as a product of Toffoli gates in staircase form.
- $\exists$ permutation gate U_k on $n = 2^k - 1$ qubits with $U_k \in \mathcal{C}_3$ but $U_k^{-1} \in \mathcal{C}_k$. U_k minimizes the number of qubits for a $\mathcal{C}_3$ permutation with a degree-k monomial.
- The smallest number of qubits for which there exists a non-semi-Clifford permutation in $\mathcal{C}_3$ is $n = 7$.
- There is a bijection between descending multiplications and permutations in $\mathcal{C}_3$ that can be written in staircase form.

References

1. D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, vol. 402, no. 6760, pp. 390–393, Nov. 1999. DOI: 10.1038/46503. [Online]. Available: http://dx.doi.org/10.1038/46503.
2. B. Zeng *et al.*, "Semi-Clifford operations, structure of $\mathcal{C}_k$ hierarchy, and gate complexity for fault-tolerant quantum computation," *Phys. Rev. A*, vol. 77, p. 042313, 4 Apr. 2008. DOI: 10.1103/PhysRevA.77.042313. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.77.042313.
3. S. Beigi and P. W. Shor, *$\mathcal{C}_3$, semi-Clifford and generalized semi-Clifford operations*, 2009. arXiv: 0810.5108 [quant-ph]. [Online]. Available: https://arxiv.org/abs/0810.5108.
4. J. T. Anderson, "On groups in the qubit Clifford hierarchy," *Quantum*, vol. 8, p. 1370, Jun. 2024. DOI: 10.22331/q-2024-06-13-1370. [Online]. Available: http://dx.doi.org/10.22331/q-2024-06-13-1370.