Classification of Sub-Universal Quantum Gatesets

Rachel Castro[†]

Abstract—**This paper investigates the algebraic structure of known sub-universal quantum gate sets, with an emphasis on recent foundational results, to identify directions for future classification. While classical circuits have long been organized into a complete hierarchy, only certain subgroups of quantum gates have been similarly classified. We begin by examining the algebraic properties of the Clifford gate set Cliff, a widely-used and well-studied gate set with notable results in classical complexity theory. Then we review the full classification of all Cliff circuits. Finally, we highlight the areas of future research towards the broader goal of classifying all quantum circuits on their algebraic and computational properties.**

I. Introduction and Motivation

Quantum computation has been the subject of great interest as a mathematical model and actual implementation since Feynman suggested the concept in the spring of $'81$ [1]. Questions about the kinds of problems quantum machines could compute more efficiently has guided the study of the field and inherently entangled it with the study of complexity theory. One such result was the Gottesman-Knill theorem of '98 [2], which showed that circuits comprised of Clifford gates could be simulated efficiently on a classical computer (with certain restrictions.) The class of computation capable a Clifford circuit is capable of is a subset of all quantum computation, motivating our study to find other subsets of quantum computation that might also be easily simulable on a classical computer. Another such example is Valiant's matchgates [3], which can be efficiently simulated on a classical computer, and has algebraic properties similar to the Clifford gate set. Thus we focused our project on understanding the complete classification of Clifford gates as presented in Grier and Schaeffer's 2022 paper [4] to further understand how sub-universal gatesets interact with algebraic structure. We hope that by understanding how these subgroups of gates structured, we can begin to identify and classify other gatesets that may be efficiently simulable.

II. Background

A. Sub-Universal Gatesets

Quantum computation is usually described in terms of gates, which are unitary matrices. We consider the set of all quantum gates over n qubits as the special unitary group $SU(2^n)$. Then a finite set of gates over n qubits $G = \{G_1, G_2, ...G_n\}$, is considered to be universal if the closed subset it generates $H = \langle G_1, G_2, ..., G_n\rangle$ under matrix multiplication and tensor product with inverses is capable of "simulating" any gate $U \in SU(2^n)$. This means that for any qubit $|\psi\rangle \in \mathbb{C}^{2^n}$, there exists some sequence of gates G_n such that $G_n |\psi\rangle = U |\psi\rangle$. We can formalize this notion of universality using the group structure of quantum gates.

Definition II.1 (Strict Universality)**.** A set G of quantum gates on n qubits is **strictly universal** for quantum computation if it generates a dense subgroup of $SU(2^n)$. [5]

A dense subgroup $H = \langle G_1, ..., G_n\rangle$ of $SU(2^n)$ has exactly the qualities we described above: if, for any matrix $U \in SU(2^n)$, there exists a sequence of gates $\{G_n\}$ with $G_i \in G$ such that for arbitrarily small $\varepsilon > 0$, $||G_n - U||_{op} < \varepsilon$.

Some gatesets that are strictly universal are $\{TOFFOLI, H\}$ or $\{X, Y, S, T\}$.

Next we consider what happens when we remove gates from a universal gateset. Consider $\{TOFFOLI, H\}$, which is universal. When we remove $TOFFOLI$ we obtain just $\{H\}$ which is not universal. In fact, the group Hadamard alone generates is much simpler: $H^\dagger H = HH = I$, thus $\langle H\rangle = \{H, I\} \cong \mathbb{Z}_2$. This example is uninteresting in terms of computing power, as it can only apply and remove superposition to qubits. However, it is demonstrative in the fact that considering subsets of universal gatesets can create groups with well-known structure. Thus next we consider the most famous example, the Clifford gate set **Cliff**.

B. Clifford Gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Students of physics may be familiar with the **Pauli** $= \{X, Y, Z\}$ matrices, a set of traceless hermitian matrices which describe the interactions between spin-$\frac{1}{2}$ particles and an external electromagnetic field. As unitary matrices with determinant 1, the **Pauli** matrices generate a subgroup of $SU(2^n)$. Specifically, as the **Pauli** s satisfy a number of nice properties:

- They are **hermitian**, thus $P^2 = I$ for all $P \in$ **Pauli**.
- $XY = iZ$, $YZ = iX$, and $ZX = iY$
- They **anticommute**, thus $P_1P_2 = -P_2P_1$ for all $P \in Pauli$

[6] Then we can characterize the group generated by **Pauli** as

$$\mathcal{P}_n = \{\mu P_1 \otimes ... \otimes P_n | P_i \in \{Pauli, I\}, \mu \in \{1, -1, i, -i\}\}$$

[6] Where we are not concerned by the multiplication of a norm 1 scalar μ, called "global phase" in quantum computing. [1]

[1] The motivation behind overlooking this is that measurement of any individual qubit overlooks this global phase, unless we purposefully encode it using phase estimation.

[†] *Department of Mathematics, Tufts University*

We have determined $\mathcal{P}_n$ as a subgroup of $SU(2^n)$, and as group theorists we have a few questions that follow naturally:

1) Is it dense in $SU(2^n)$?
2) Is it isomorphic to anything we know?
3) Is it normal? If not, what is its normalizer?

The answer to the first two questions follows from this example. Consider $\mathcal{P}_2$, the set of 2-qubit Pauli strings of the form $\mathcal{P}_2 = \{I \otimes I, I \otimes X, ..., Z \otimes Z\}$ with an associated ± 1 or $\pm i$. It is clear that this is not dense because it generates a finite group of order 16, and dense subgroups of $SU(4)$ are infinite. It is not obviously isomorphic to anything we know well, although readers familiar with the group of quaternions $\mathbb{H}$ may see similarities. [2]

Finally, we can ask if it is normal. A normal subgroup is closed under conjugation by any other element in the group. A short check shows that conjugation by $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ of any gate in $\mathcal{P}_n$ creates a gate not in the subgroup. Then $\mathcal{P}_n$ is not normal, so what changes can we apply to normalize it? The answer is a set of additional gates, and in combination with **Pauli** is known as the Clifford gateset **Cliff**.

Definition II.2 (Clifford Gateset **Cliff**). The clifford gateset **Cliff** in n qubits is the normalizer of $\mathcal{P}_n$ in $SU(2^n)$. Generators of this group include $\{S, H, CNOT\}$, $\{R_X, R_Z\}$, $\{H, CZ, X, Z\}$.

As discussed in the introduction of this paper, **Cliff** naturally arises from study of the algebraic properties of quantum gates. It is also one of the most well-studied gatesets, as seen in the Gottesman-Knill result [2] and further classification that will be the subject of the rest of the paper.

III. Classification Results

A. Classifying Computation

Classifying universal (and sub-universal) computation has been the object of fixation for mathematicians for almost a century. In classical computing, the capabilities of different circuits are described in terms of which boolean functions they compute. Boolean functions on n bits are of the form $f : \{0,1\}^n \to \{0,1\}$ and can be described by different invariant characteristics. Some of these invariants are whether or not they are 0-preserving (return zeroes on an input of all zeroes), monotonicity, and self-duality.

In 1941, mathematician Leon Post classified all possible sub-classes of boolean functions, which are closed under composition of functions. This foundational work was revisited in the 2010s when computer scientists attempted to extend this result to quantum computing. In 2015, Scott Aaronson, Daniel Grier, and Luke Schaeffer classified all reversible classical bit operations [7]. This result was key because unlike classical computation, all gates in quantum computing must be reversible. Then in 2022, Grier and Schaeffer continued their work to classify all subsets of **Cliff** into 57 classes [4]. This work is explored in detail in the following sections.

B. Class Closure

While Post's classes of boolean functions are closed under composition, the **Cliff** classification is slightly more complex. Closure is exactly the idea as discussed above in the context of group theory: given any set of gates $\{G_1, ..., G_n\}$, their closure is the set of all gates that can possibly be generated by a sequence of G_n. As we showed above, **Cliff** is not dense in $SU(2^n)$, and thus as some subset of **Cliff** any class must also not be dense in $SU(2^n)$. Grier and Schaeffer's main result is thus:

Theorem III.1 (**Cliff** Classification). *Any set of **Cliff** gates generate exactly one of the* 57 *distinct classes. Each class is uniquely determined by invariants and uniquely finitely generated.*

Definition III.1 (**Cliff** Class Closure). Let $G = \{G_1, ..., G_n\}$ a set of gates in **Cliff**. For all $G_1, G_2 \in G$ the class C generated by these gates is closed under

- Composition: $G_1 \circ G_2 \in C$
- Tensor product: $G_1 \otimes G_2 \in C$
- $SWAP$: $SWAP(G_1 \otimes G_2) \in C$
- Arbitrary ancillas, minus magic states. For any G_1 in C, $\exists G_2 \in C$ and $|\psi\rangle \in \mathbb{C}^{2^n}$ such that
$$G_1(|x\rangle \otimes |\psi\rangle) = G_2(|x\rangle) \otimes |\psi\rangle, \forall |x\rangle \in \mathbb{C}^{2^n}$$

It is easy to see that it follows that any class also includes the identity. Simply observe $SWAP \circ SWAP = I$.

We can also construct the inverse of any gate in C to also be in C using group theory. We know that the group **Cliff** is finite, thus any subgroup will also be finite. Then any gate $G_1 \in G$ where G is finite will have finite order σ, such that $G_1^\sigma = I$. Then $G_1^{\sigma-1} G_1^\sigma = G_1^\sigma G_1^{\sigma-1} = I$, then by definition $G_1^{\sigma-1}$ is the inverse of G_1.

Associativity clearly follows from the group operation of matrix multiplication, and thus each **Cliff** class C is also a group.

As discussed in Theorem III.1, each class is uniquely finitely generated. One such example is the familiar **Pauli**, the generators of which have already been discussed. Another example is the class generated by R_X, which is the $\pi/2$ rotation about the X axis. It is clear that this isomorphic just the cyclic group $\langle R_X \rangle \cong C_4$.

In the complete classification, the authors use the following set of gates to describe the finite generation of each class.

Single-qubit gates

Gate Name	Geometric Representation
$\mathcal{P}_n$	π rotations around axes
R_X, R_Y, R_Z	$\pi/2$ rotations around axes
$\theta_{P_1 \pm P_2}$	π rotation around an edge
$\Gamma_{\pm\pm\pm}$	$2\pi/3$ rotations around major diagonal

[3]

[2] And in fact, modding out ± 1 to leave only a $\pm i$ factor on each of the terms is $\cong \mathbb{H}$.

[3] The geometric explanation behind these gates is closely related to the fact that $SU(4)/\mathbb{Z}_2 \cong SO(3)$ but is unfortunately beyond the scope of this paper.

Multi-qubit gates

Gate Name	Description
$SWAP$	Swaps two qubits
$C(P,Q)$	Generalized $CNOT$
T_4	If $\bigoplus_{i\in I} \|x\rangle_i = 1$, return $\neg \|x\rangle_i$, else identity.

While we can consider these classes in terms of which gates they can be generated by, the authors offer another method. Similarly to Post's lattice, Grier and Schaeffer distinguish each class by a unique set of invariants.

C. Invariants

An invariant is a property of gates such that if it is positive for all generators of a class, it will be true for every gate in the class. In this section we will examine each of the invariants and a class that exemplifies it.

- **P-preserving**
  A gate $G \in$ **Cliff** is P-preserving, for $P \in$ **Pauli**, if it maps P-basis states to other P-basis states, with an optional change of phase. We associate P-basis states by considering the plus/minus eigenspaces of each **Pauli** gate. For example, $X = |+\rangle\langle+| - |-\rangle\langle-|$, and thus the X-basis is $|+\rangle$, $|-\rangle$. Then a P-preserving gate would be one that maps $|+\rangle \mapsto |+\rangle$ or $|+\rangle \mapsto |-\rangle$. For example, $CNOT$ is both X and Z preserving in that $CNOT(|1\rangle \otimes |0\rangle) \mapsto |1\rangle \oplus |1\rangle$ and $CNOT(|+\rangle \otimes |0\rangle) \mapsto |+\rangle \otimes |+\rangle$.
- **Egalitarian**
  A gate G in **Cliff** is egalitarian if conjugation by $\Gamma = \Gamma_{+++}$ then application of gate M yields the same results as application of M. For example, X is egalitarian, such that:
  $$M(\Gamma X \Gamma^\dagger) = M(X)$$
  for all M in **Cliff**.
- **Degenerate**
  A gate G is degenerate if, when it is applied to a gate in $\mathcal{P}_n$, changing exactly one **Pauli** in the input will change exactly one output. To see this, consider the **Pauli** string $X \otimes X \otimes Z$, and the gate $I \otimes R_X \otimes I$. Applying them obtains $XI \otimes XR_X \otimes ZI = X \otimes XR_X \otimes Z$. It is straightforward to see that every single-qubit gate is degenerate, and every degenerate gate is composed of single-qubit gates and $SWAP$.
- **P-degenerate**
  A gate $G \in$ **Cliff** is P-degenerate, for $P \in$ **Pauli**, it is P-preserving and flipping any bit in the classical basis $(|0\rangle, |1\rangle)$ flips exactly one bit of the output. An example is R_Z or any of the $\mathcal{P}_n$ gates.
- **P-orthogonal**
  A gate G is P-orthogonal for $P \in$ **Pauli** if it can be built from T_4 and P-preserving gates. An example is T_4.
- **Single-qubit gates**
  Single qubit gates are all degenerates, minus $SWAP$ applications.

The authors consider two main sets of the classification: degenerate classes, as defined above, and non-degenerate classes. The most interesting classes are non-degenerate and are arranged in a symmetric poset across the three **Pauli** gates.

IV. Future Work

Grier and Schaeffer's classification of all **Cliff** gates on n qubits is foundational work in the field. After understanding these results, the natural question that forms is: Where next can we apply classification in the world of quantum gatesets?

Naturally, one turns to other non-dense subgroups of $SU(2^n)$ to look for next candidates. In the smallest setting, $SU(2)$, there is little work left to be done in terms of classification. When phase is modded out, we can consider the subgroups of $SO(3)$, which is the well-understood group of symmetry in three dimensions. However, even adding just one qubit and studying $SU(4)$ results in a much more complicated system with poorly understood symmetry.

Next, we can turn to other known subgroups of gates. One such candidate is Valiant's matchgates, which similarly to **Cliff** can be simulated efficiently on a classical computer. Some progress has been made in this area [8] but a complete classification is yet to be formed.

An avenue that appears to be somewhat unexplored by a literature search is using Lie group theory to classify other non-dense subgroups of $SU(2^n)$. Specifically, semisimple Lie groups can be understood by studying their underlying arithmetic groups which describe lattice structure within them [9]. In future projects, we hope to continue exploring the arithmetic group theory of $SU(2^n)$ to provide a coarse structure of possible quantum gatesets.

References

[1] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, no. 6–7, pp. 467–488, 1982.

[2] D. Gottesman, "The heisenberg representation of quantum computers," 1998.

[3] L. G. Valiant, "Quantum circuits that can be simulated classically in polynomial time," in *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing (STOC'01)*, pp. 114–123, 2001.

[4] D. Grier and L. Schaeffer, "The classification of clifford gates over qubits," 2022.

[5] D. Aharonov, "A simple proof that toffoli and hadamard are quantum universal," 2003.

[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press, 10th anniversary edition ed., 2010.

[7] S. Aaronson, D. Grier, and L. Schaeffer, "The classification of reversible bit operations," 2015.

[8] A. Bampounis, R. S. Barbosa, and N. de Silva, "Matchgate hierarchy: A clifford-like hierarchy for deterministic gate teleportation in matchgate circuits," 2024.

[9] D. W. Morris, "Introduction to arithmetic groups," 2015.