LOWER BOUNDS FOR QUANTUM CIRCUITS

by

Ravi Rai

Submitted in partial fulfillment of the requirements
for the degree of Master of Science

at

Dalhousie University
Halifax, Nova Scotia
August 2021

Table of Contents

Abstract

In quantum computing, computational tasks are represented by quantum circuits. These circuits are composed of gates whose physical realization comes at a cost. Typically, gates from the so-called Clifford group are considered cheap, while non-Clifford gates are considered expensive. Consequently, non-Clifford operations are often seen as a resource whose use should be minimized.

In this thesis, following recent work by Beverland and others, we study lower bounds for the number of non-Clifford gates in quantum circuits. We focus on lower bounds that can be derived from monotones, which are real-valued functions of quantum states that are non-increasing under Clifford operations.

We first provide a detailed presentation of two recently introduced monotones: the stabilizer nullity and the dyadic monotone. We then discuss how these monotones can be used to give lower bounds for the non-Clifford resources for two important quantum operations: the multiply-controlled Pauli Z gate and the modular adder.

Chapter 1

Introduction

In quantum computing, computational tasks are represented by quantum circuits. Quantum circuits are composed of gates that represent operators and wires that represent qubits. These gates transform the state of one or many qubits. Applying these gates comes at a cost, so minimizing this cost is of particular interest. Certain gates and operations are considered cheap, those typically being the gates in the Clifford group, while non-Clifford gates are considered expensive. It is well-known that the Clifford group is not universal for quantum computing, which means that not all operations in quantum computing can be performed with just Clifford gates. Adding a single non-Clifford gate, however, gives the desired universality, making such expensive gates necessary. Common non-Clifford gates used in quantum computing are the so-called T, CS, and CCZ gates. Naturally, the goal in designing quantum circuits is to use the least number of these resources.

Much work has been done to try to reduce the number of non-Clifford gates in quantum circuits, as seen in [14, 15, 2, 6, 8, 3, 7]. Sometimes these circuit optimizations are optimal, as in [14, 6, 7]. But in most cases, these optimizations are heuristic: a method to reduce the number of non-Clifford gates is defined and then empirically evaluated on benchmark circuits. This has prompted recent efforts in finding lower bounds for non-Clifford resources [4, 17, 11]. Lower bounds can help us understand how much more effort to put into optimizing circuits and are the focus of this thesis.

Upper bounds are often obtained from explicit circuit constructions. In contrast, non-trivial lower bounds are notoriously hard to find. In this thesis, we focus on lower bounds that are obtained from monotones, which are real-valued functions of quantum states that are non-increasing under Clifford operations. This follows the work of Beverland and others [4] which provides the main reference for this thesis.

The thesis focuses on two monotones, namely the stabilizer nullity and the dyadic monotone. The resources considered are the previously mentioned T, CS, and CCZ

gates. These monotones are leveraged to provide lower bounds for important quantum operations: the multiply-controlled Pauli Z gate and the modular adder. Two sets of lower bounds are provided, one derived from the stabilizer nullity and another derived from the dyadic monotone. The dyadic monotone gives tighter lower bounds, but with further restrictions. Some well-known upper bounds are provided for contrast as well. In some cases, the upper bounds match the lower bounds, showing that the circuit constructions are optimal.

The thesis is organized as follows: in Chapter 2 we begin with a brief overview of the necessary background information needed. Then, in Chapter 3, we introduce the stabilizer formalism, which is the backbone of our methods to realizing lower bounds for resources. The central concept in this chapter is the stabilizer of a state. In Chapter 4, monotones are introduced in detail, along with some of their important properties, leveraging the stabilizer defined in the previous chapter. Chapter 4 is also where the aforementioned restriction of the dyadic monotone first appears, as it is needed to prove some of its properties. In Chapter 5, we use both monotones to derive lower bounds, considering the T, CS, and the CCZ gates as resources. We calculate lower bounds for two circuits, namely the C^nZ circuit and the modular adder circuit. Finally, the main takeaways of the thesis are briefly stated in Chapter 6, along with open problems for further work.

Chapter 2

Foundational Quantum Computing

In this chapter, we provide the necessary prerequisites to this thesis. In particular, we introduce quantum states, unitary evolutions, measurements, and quantum circuits.

2.1 Preliminaries

2.1.1 Vectors and Matrices

Let $\mathbb{C}$ be the set of complex numbers. We write $\mathbb{C}^n$ to represent the space of n-dimensional column vectors, and we write $\mathbb{C}^{n\times m}$ for the space of matrices with n rows and m columns. Matrices can be multiplied in the usual way.

The *complex conjugate* of a scalar $c \in \mathbb{C}$ is denoted $\bar{c}$, and the *adjoint* of a matrix $M = (c_{ij}) \in \mathbb{C}^{n\times m}$ is $M^\dagger = (\bar{c}_{ji}) \in \mathbb{C}^{m\times n}$. The *trace* of a matrix M, denoted $\mathtt{Tr}(M)$, is the sum of its diagonal entries. Note that $\mathtt{Tr}(BA) = \mathtt{Tr}(BA)$.

For a vector $v \in \mathbb{C}^n$, the *norm* of v is $||v|| = \sqrt{v^\dagger v}$. The vector v is called a *unit vector* if $||v|| = 1$. A matrix $U \in \mathbb{C}^{n\times n}$ is *unitary* if $U^{-1} = U^\dagger$ and *hermitian* if $U = U^\dagger$.

2.1.2 Tensor Products

The *tensor product* is defined as usual and is denoted by $\otimes$. When a basis is fixed, the tensor product can be computed as the *Kronecker product*: the tensor product $w = u \otimes v \in \mathbb{C}^{nm}$ of two vectors is defined by $w_{(i,j)} = u_i v_j$. Similarly, the tensor product $C = A \otimes B \in \mathbb{C}^{nm\times nm}$ of two matrices is defined by $c_{(i,j)(i',j')} = a_{ii'} b_{jj'}$, with pairs (i, j) ordered lexicographically. Note that $\mathbb{C}^n \otimes \mathbb{C}^m = \mathbb{C}^{nm}$ and $\mathbb{C}^{n\times n} \otimes \mathbb{C}^{m\times m} =$

$\mathbb{C}^{nm\times nm}$. For example, the Kronecker product between two 2×2 matrices looks like:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}.$$

A basis for a tensor product of vector spaces can be obtained as the tensor product of the basis elements of the individual vector spaces. For example, if $\{a_1, a_2\}$ and $\{b_1, b_2\}$ are two bases for $\mathbb{C}^2$, then $\{a_1 \otimes b_1, a_1 \otimes b_2, a_2 \otimes b_1, a_2 \otimes b_2\}$ is a basis for $\mathbb{C}^4$. Note that not all elements of $\mathbb{C}^4$ are of the form $a \otimes b$ with $a, b \in \mathbb{C}^2$.

2.1.3 The Dirac Notation

In quantum computing, we make use of the *Dirac notation* to represent vectors and operations. In Dirac notation, we write a column vector v as a *ket*, denoted by $|v\rangle$. The adjoint of a column vector u is written as a *bra*, denoted by $\langle u|$. The inner product between two vectors $|v\rangle$ and $|u\rangle$ is then written as a *braket*, denoted by $\langle u|v\rangle$. For example, the inner product of $\langle 0|$ and $|1\rangle$ is $\langle 0|1\rangle$. The outer product between two vectors is written in the opposite manner, i.e. $|v\rangle\langle u|$. Note this is simple matrix multiplication, where the inner product results in a scalar, and the outer product produces a matrix. In some sense the outer product scales a vector, since for a vector $|w\rangle$, we have $|v\rangle\langle u|\,|w\rangle = \langle u|w\rangle\,|v\rangle$ where $\langle u|w\rangle$ is just a scalar.

Consider the standard basis vectors $[1, 0]^\dagger$ and $[0, 1]^\dagger$. We denote them $|0\rangle$ and $|1\rangle$ respectively. In quantum computing, the basis of $\mathbb{C}^2$ formed by $\{|0\rangle, |1\rangle\}$ is known as the *computational basis*. As mentioned before, one can get a basis for higher dimensional vector spaces by taking tensor products of $|0\rangle$ and $|1\rangle$. For example, a basis for $\mathbb{C}^4$ is $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$. For brevity, the symbol $\otimes$ is often omitted for elements of the higher dimensional computational bases. For example, $|0\rangle \otimes |0\rangle$ is written as $|00\rangle$ and $|0\rangle \otimes |1\rangle$ is written as $|01\rangle$. In this way, the j-th basis vector of $\mathbb{C}^{2^n}$ is denoted $|b_1 b_2 \cdots b_n\rangle$ where $b_1, b_2, \cdots, b_n \in \mathbb{Z}_2$ and $b_1 b_2 \cdots b_n$ is the binary expansion of j. Alternatively, we sometimes also write j as an integer instead. For example, $|3\rangle = |11\rangle = |1\rangle \otimes |1\rangle$. These notations are all equivalent and interchangeable, thus we use whichever one is most convenient.

2.1.4 Quantum Bits

The fundamental unit of information in classical computing is the *bit*. In quantum computing the basic unit of information is called a *quantum bit* or *qubit* for short. In classical computing the classical bit can be in the *states* 0 or 1, but in quantum computing the state of a qubit is a unit vector in $\mathbb{C}^2$. Hence, the state of a qubit can be any complex linear combination $\alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ and satisfy $|\alpha| + |\beta| = 1$. The complex numbers α and β are called the *amplitudes* of the state. Note that $|0\rangle$ and $|1\rangle$ are valid states, corresponding to $\alpha = 1$ and $\beta = 0$, and to $\alpha = 0$ and $\beta = 1$ respectively. We sometimes call these states *classical*. A state whose amplitudes are both nonzero is said to be a state in *superposition*. For example, a qubit in the state

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

is in (equal) superposition.

Similarly, the state of a collection of n qubits (sometimes called a *register*) is described by a unit vector in $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = \mathcal{C}^{2^n}$. For example, a 2-qubit system could be in the state

$$\frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}.$$

Interestingly, the state of a multi-qubit system cannot always be expressed as the tensor product of the states of the qubits composing the system. Consider for example the 2-qubit state

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

It can be verified using the definition of the tensor product given in Section 2.1.2 that there are no single-qubit states $|v\rangle$ and $|w\rangle$ such that

$$|v\rangle \otimes |w\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

If two qubits are such that their state can be expressed as a tensor product $|v\rangle \otimes |w\rangle$ then the qubits are said to be *separable*. Otherwise, the qubits are said to be *entangled*. For example if a pair of qubits is in the state

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

then the qubits are entangled.

In what follows, we will sometimes write $\mathcal{S}(n)$ for the set of all n-qubit states and $\mathcal{S}$ for the collection of all states. That is $\mathcal{S} = \cup_n \mathcal{S}(n)$. In addition to the computational basis states defined above, other important states include

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

and

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Finally, if $|\psi\rangle$ is a state we write $|\psi\rangle^{\otimes n}$ for the n-fold tensor product of $|\psi\rangle$ with itself $|\psi\rangle \otimes |\psi\rangle \otimes \cdots \otimes |\psi\rangle$.

2.2 Quantum Operations

To compute with qubits, one can act on them using two types of operations: unitary evolutions and measurements.

2.2.1 Unitary Evolution

In this case, the state of a quantum system is transformed by applying a unitary transformation to it. For example, say a quantum system is described by the column vector $|\psi\rangle$ and U is some unitary matrix. Then the state, after having evolved under U, is given by $U|\psi\rangle$. Observe that unitary matrices are isometries since $||Uv|| = ||v||$ holds for all v if U is unitary, and vice versa when U is a square matrix. A unitary transformation on an n qubit system is also called an n-ary *quantum gate*. The following are some notable single qubit gates that will be used extensively in this thesis, and are as follows: the Pauli X, Y, and Z gates, the Hadamard gate H, the phase gate S, and the T gate. The Pauli matrices are

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \text{and} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

and the others are

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad \text{and} \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}.$$

Note that the X gate is synonymous with the *Not* gate, which can be though of as a simple bit flip gate, i.e. $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$.

If U is an n-qubit unitary, we write CU for the $(n+1)$-qubit unitary whose action on basis states is defined as $CU\,|c\rangle\,|t\rangle = |c\rangle\,U^c\,|t\rangle$, for $c \in \mathbb{Z}_2$ and $t \in \mathbb{Z}_2^n$. The gate CU is called a *controlled-U gate*. The intuition is that there is a single qubit that acts as a *control* qubit so that the U gate is only applied to the other qubits depending on the state of the control qubit. The qubits that U acts on are called the *target* qubits. Gates can be multiply-controlled as well. We write C^nU for the multiply-controlled U gate with n controls. Its action on the computational basis is given by $C^nU\,|c_1\rangle \ldots |c_n\rangle\,|t\rangle = |c_1\rangle \ldots |c_n\rangle\,U^{c_1 \cdots c_n}\,|t\rangle$, where $c_1, \cdots c_n$ is the product of the bits $c_1, \ldots, c_n$ in $\mathbb{Z}_2$. Knowing this, there are important controlled gates that will be used later in great detail. They are the CS gate, $CNOT$ (or CX) gate, and the Toffoli gate (or CCX), and they have matrices:

$$CS = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}, \quad CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

and

$$CCX = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

2.2.2 Measurement

Aside from unitary transformations, we can also act on a quantum state by *measuring* it. Measurement is a probabilistic process, and we think of it as observing the state. A quantum state collapses due to a measurement, and if you were to measure it again this would yield the same result. Measurements can be performed with respect to different bases of $\mathbb{C}^j$. In this thesis, an important basis is the computational basis. If a qubit is in the state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, and it is measured in the computational

basis, then the post-measurement state will be $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$.

More formally, quantum measurements are described by a collection of *measurement operators* $\{M_m\}$ [13, p. 85]. These operators are Hermitian, idempotent, and satisfy the completion rule: $\sum_m M_m^\dagger M_m = I$. The index m refers to the corresponding measurement outcome. When measuring some state $|\phi\rangle$ the probability that the outcome m occurs is $p(m) = \langle\phi|M_m^\dagger M_m|\phi\rangle$ and in this case the post-measurement state is $\frac{M_m|\phi\rangle}{\sqrt{\langle\phi|M_m^\dagger M_m|\phi\rangle}}$. Naturally, these probabilities sum to 1, which can also be seen from the completeness equation: $1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle$. Moreover, in the computational basis for $\mathbb{C}^2$, we have $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. Measuring the state $|\psi\rangle$ above with these formal terms will give the same result as before.

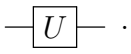
Measurement is of course not restricted to just a single qubit. This formal method can describe measurement on multiple qubits. Consider an n-qubit system described by the state $|\Psi\rangle$. Then measuring in the computational basis, the probability of observing the outcome j is still just $\langle\Psi|M_j^\dagger M_j|\Psi\rangle$, where $M_j = |j\rangle\langle j|$ and j is taken to be in binary form. For example, on 3 qubits one possible outcome is $|001\rangle$ as this is one of the computational basis states in $\mathbb{C}^4$. Then $M_{001} = |001\rangle\langle 001|$ is used to find the probability that the measurement outcome will be $|001\rangle$. One can also measure an m qubit state in an n qubit system for $m \leq n$, i.e. one can measure only part of a quantum system.

A type of measurement that we will be especially interested in is the *Pauli measurement*. Recall that X, Y, and Z are the Pauli matrices defined above. An n-qubit Pauli operator is obtained by taking a tensor product of n elements of $\{I, X, Y, Z\}$. An n-qubit Pauli can be decomposed as a sum of measurement operators. Let P be a n-qubit Pauli and $|\psi\rangle$ an n-qubit state. Note that for any Pauli P, only two eigenvalues occur, namely the -1 eigenvalue and the $+1$ eigenvalue. Recall that by the spectral decomposition theorem, we have matrices $P_{\pm 1}$ which are projectors for their corresponding eigenspaces. These matrices satisfy the following equations: $P = (+1)P_{+1} + (-1)P_{-1}$, and $I = P_{+1} + P_{-1}$. Now for a Pauli measurement on P the probability of a $+1$ outcome is $\langle\psi|P_{+1}|\psi\rangle$, with post measurement state $|\phi\rangle = \frac{P_{+1}|\psi\rangle}{\sqrt{\langle\psi|P_{+1}|\psi\rangle}}$. Finally, from the above equations we get that $P_{-1} = P_{+1} - P$ and $P_{-1} = I - P_{+1}$, so by subtracting these equations we eliminate P_{-1} and get that

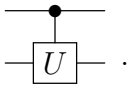
$P_{+1} = \frac{I+P}{2}$. Hence, we now can write the post measurement state as $|\phi\rangle = \frac{(I+P)|\psi\rangle}{2\sqrt{\langle\psi|P_{+1}|\psi\rangle}}$.

2.3 Quantum Circuits

A *quantum circuit* describes a sequence of operations acting on a register of qubits. Quantum circuits are made of (horizontal) wires and boxes, where each wire represents a qubit and each box represents a gate. Typically the boxes that represent gates have a label indicating what gate it is. Explicitly, letting U be any single qubit gate, a circuit with one qubit and U gate would look like

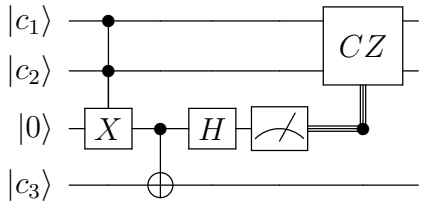


Multi-qubit gates are also boxes but with multiple wires connecting to it. There is a special representation for controlled gates. Controlled operations are represented with a open or closed circle on the control qubit with a vertical wire connecting it to a box on the target qubit. A controlled operation with a closed circle on its control qubit, means apply the controlled gate to the target qubits only if the control qubit is in the $|1\rangle$ state. An open circle on the control qubit means apply the gate if the control qubit is in the state $|0\rangle$. The circuit for a controlled operation CU where U is a single-qubit unitary is



The circuit representation for a multiply controlled gate is written in this fashion also but with multiple control qubits.

Quantum circuits are read from left to right, and can be applied by tracking what the operations do to the input state. It is worth noting that if two circuits give the same output on a general input state then they are equivalent circuits. In fact, the following example is a circuit from [10] that acts exactly as a CCZ gate on qubits c_1, c_2, and c_3, and will be used later on in Chapter 5.



(2.1)

The $\oplus$ symbol in the bottom wire denotes the X gate, making this controlled gate a CNOT or CX gate. The gate with the meter symbol is a measurement gate and performs a measurement with respect to the computational basis. The final CZ gate is a classically controlled gate, represented by the double line attached to it from the third qubit. Classically controlled gates work by only being applied to its qubits if the measurement outcome of the other qubit it is attached to is $|1\rangle$. Also, the third qubit is called an *ancilla*. It is used as "scratch space" during the computation, and a circuit with no ancillas is said to be *ancilla free*. Tracking from left to right starting with the input state, we get the following steps:

$$
\begin{aligned}
& |c_1\rangle\,|c_2\rangle\,|0\rangle\,|c_3\rangle \\
\mapsto\ & |c_1\rangle\,|c_2\rangle\,|(c_1\cdot c_2)\rangle\,|c_3\rangle \\
\mapsto\ & |c_1\rangle\,|c_2\rangle\,|(c_1\cdot c_2)\rangle\,|c_3\oplus(c_1\cdot c_2)\rangle.
\end{aligned}
$$

Now, write out the general states $|c_1\rangle$ and $|c_2\rangle$ as $\alpha_{c_1}|0\rangle+\beta_{c_1}|1\rangle$ and $\alpha_{c_2}|0\rangle+\beta_{c_2}|1\rangle$ respectively. Since the fourth qubit which is in the state $|c_3\oplus(c_1\cdot c_2)\rangle$ remains unchanged from here, we consider only the first three qubits next. We get:

$$
\begin{aligned}
& |c_1\rangle\,|c_2\rangle\,|(c_1\cdot c_2)\rangle \\
=\ & \big(\alpha_{c_1}\alpha_{c_2}|000\rangle+\beta_{c_1}\alpha_{c_2}|100\rangle+\alpha_{c_1}\beta_{c_2}|010\rangle+\beta_{c_1}\beta_{c_2}|111\rangle\big) \\
\mapsto\ & \tfrac{1}{\sqrt{2}}(\alpha_{c_1}\alpha_{c_2}|000\rangle+\beta_{c_1}\alpha_{c_2}|100\rangle+\alpha_{c_1}\beta_{c_2}|010\rangle+\beta_{c_1}\beta_{c_2}|110\rangle)+\tfrac{1}{\sqrt{2}}(\alpha_{c_1}\alpha_{c_2}|001\rangle+ \\
& \beta_{c_1}\alpha_{c_2}|101\rangle+\alpha_{c_1}\beta_{c_2}|011\rangle-\beta_{c_1}\beta_{c_2}|111\rangle) \\
\mapsto\ & \begin{cases}
\big(\alpha_{c_1}\alpha_{c_2}|00\rangle+\beta_{c_1}\alpha_{c_2}|10\rangle+\alpha_{c_1}\beta_{c_2}|01\rangle+\beta_{c_1}\beta_{c_2}|11\rangle\big) & \text{if measurement is } |0\rangle, \\
\big(\alpha_{c_1}\alpha_{c_2}|00\rangle+\beta_{c_1}\alpha_{c_2}|10\rangle+\alpha_{c_1}\beta_{c_2}|01\rangle-\beta_{c_1}\beta_{c_2}|11\rangle\big) & \text{if measurement is } |1\rangle
\end{cases} \\
\mapsto\ & \begin{cases}
\big(\alpha_{c_1}\alpha_{c_2}|00\rangle+\beta_{c_1}\alpha_{c_2}|10\rangle+\alpha_{c_1}\beta_{c_2}|01\rangle+\beta_{c_1}\beta_{c_2}|11\rangle\big) & \text{if measurement is } |0\rangle, \\
\big(\alpha_{c_1}\alpha_{c_2}|00\rangle+\beta_{c_1}\alpha_{c_2}|10\rangle+\alpha_{c_1}\beta_{c_2}|01\rangle+\beta_{c_1}\beta_{c_2}|11\rangle\big) & \text{if measurement is } |1\rangle
\end{cases} \\
=\ & |c_1\rangle\,|c_2\rangle.
\end{aligned}
$$

Finally, bringing the fourth qubit back into consideration we arrive with

$$|c_1\rangle\,|c_2\rangle\,|c_3\oplus(c_1c_2)\rangle$$

as the final state of the system, which is exactly the operation of a CCZ gate on the first, second, and fourth qubits, as expected. The first few steps follow naturally by applying the gates one-by-one, while the rest are less trivial. In particular, the sixth step follows from the fact that $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$, which can be verified by direct computation. The seventh step comes after we measure the third qubit, where we observe either the $|0\rangle$ or the $|1\rangle$ state, both with probability $1/2$. The only difference here between observing either of these states is that there is a negative sign attached to the $\beta_{c_1}\beta_{c_2}|11\rangle$ component. The final step fixes this issue by applying the CZ gate to the first two qubits, provided the $|1\rangle$ state was observed. This results in having the same output state regardless of the measurement outcome, hence the final result.

Note that a circuit that does not contain any measurements can be straightforwardly interpreted as a matrix by interpreting the horizontal composition of gates as matrix multiplication and the vertical composition of gates as tensor products.

Chapter 3

The Clifford Group and Its Universal Extensions

In this chapter, we introduce Clifford circuits, discuss their computational power, and present several universal extensions of the Clifford group.

3.1 The Pauli Operators

Recall the *Pauli matrices* X, Y, and Z from Chapter 2:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \text{and} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

If S is a set of matrices then $S^{\otimes n}$ is the set of matrices comprised of tensor products of elements in S.

Definition 3.1.1. The *Pauli group on n qubits* $\mathcal{P}(n)$ is the matrix group with elements $\{\pm I, \pm X, \pm Y, \pm Z, \pm iI, \pm iX, \pm iY, \pm iZ\}^{\otimes n}$.

Note that the ± 1 and $\pm i$ factors in the elements of $\mathcal{P}(n)$ ensures the closure of the group.

Proposition 3.1.2. *We have* $|\mathcal{P}(n)| = 4^{n+1}$.

Proof. By induction, first let $n = 1$. Then from definition 3.1.1 we see that there are $16 = 4^2$ elements in $\mathcal{P}(1)$, so the base case is true. Now assume that the statement is true for m qubits, i.e. $|\mathcal{P}(m)| = 4^{m+1}$. Then $\mathcal{P}(m+1)$ has elements that are tensor products of elements in $\mathcal{P}(m)$ and I, X, Y, and Z. Thus there are $4 \cdot 4^{m+1} = 4^{(m+1)+1}$ elements in $\mathcal{P}(m+1)$. Note that we only count these tensor products since e.g., $P \otimes -iX = P' \otimes X$ where $P' = -iP$, for $P, P' \in \mathcal{P}(m)$. □

3.2 The Clifford Operators

Recall the gates H, S, and CNOT defined in Chapter 2:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

and

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

We use these gates to define the *Clifford* group.

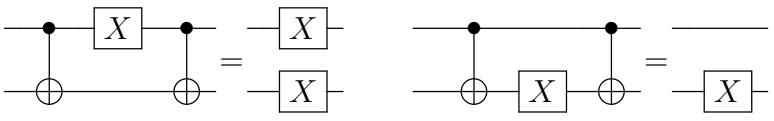
Definition 3.2.1. The Clifford group on n qubits $\mathcal{C}(n)$ consists of the matrices that can be represented by an ancilla-free circuit on n qubits over the gate set $\{H, S, CNOT\}$.

Clifford operators are sometimes referred to as *Stabilizer* operators.

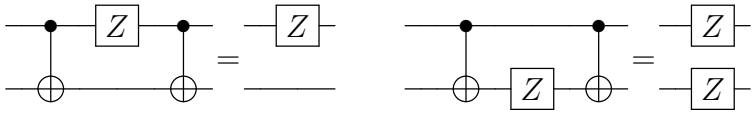
Proposition 3.2.2. *H, S, and $CNOT$ act on Paulis as follows:*

$$HXH^\dagger = Z \text{ and } HZH^\dagger = X, \; SXS^\dagger = Y \text{ and } SZS^\dagger = Z.$$

For $CNOT$, we write its action on Paulis in circuit notation. For X we have the following.



And for Z we have:



Note that we need not specify the action on Y since $Y = iXZ$, so the action on X and Z gives and fixes the action on Y.

Proposition 3.2.3. *If $P \in \mathcal{P}(n)$ and $C \in \mathcal{C}(n)$ then $CPC^\dagger \in \mathcal{P}(n)$.*

Proof. It is sufficient to show that the generators of $\mathcal{C}(n)$ map the generators of Pauli matrices to Pauli matrices. The Clifford generators are H, S in $\mathcal{C}(1)$ and $CNOT$ in $\mathcal{C}(2)$, while the generators of $\mathcal{P}(1)$ are iI, X and Z. Note that for Pauli matrices in $\mathcal{P}(n)$, we can write them as a tensor product of Pauli matrices in $\mathcal{P}(1)$. Moreover, we can also write a gate in $\mathcal{C}(n)$ as a tensor product of any combination of H, S and $CNOT$.

We can use this and Proposition 3.2.2 to give us that, for a Pauli $P \in \mathcal{P}(n)$ and some $C \in \mathcal{C}(n)$ $CPC^\dagger \in \mathcal{P}(n)$. This follows by writing P and C as tensor products as explained above, and then using the distributive law of tensor products. □

The previous proposition shows that Cliffords map Paulis to Paulis under conjugation. We now show that, in fact, any unitary operator that maps Paulis to Paulis under conjugation is an element of the Clifford group (up to a scalar). Our proof follows [13].

Lemma 3.2.4. *Let $P \in \{\pm X, \pm Y, \pm Z\}$. Then there exists a $C \in \langle H, S\rangle$ such that $CXC^\dagger = P$.*

Proof. To prove this we simply list all possible C circuits required for each P:

- If $P = X$ then $C = I$.
- If $P = -X$ then $C = S^2$.
- If $P = Y$ then $C = S$.
- If $P = -Y$ then $C = HS$.
- If $P = Z$ then $C = H$.
- If $P = -Z$ then $C = HS^2$.

□

Lemma 3.2.5. *Let $Q \in \{\pm Y, \pm Z\}$. Then there exists a $D \in \langle H, S\rangle$ such that $DQD^\dagger = Z$ and $DXD^\dagger = X$.*

Proof. To prove this we simply list all possible D circuits required for each Q:

- If $Q = Y$ then $D = S^\dagger H S^\dagger$.
- If $Q = -Y$ then $D = (S^\dagger H)^2 (S^\dagger)^2 H$.
- If $Q = Z$ then $D = I$.
- If $Q = -Z$ then $D = HS^2$.

□

Theorem 3.2.6. *Let U be a unitary operator that maps Paulis to Paulis under conjugation. Then, up to a global phase, U may be composed of H, S, and $CNOT$ gates.*

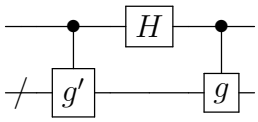
Proof. We proceed by induction on n, the number of qubits, following the method outlined in [13]. For the base case, let U be a single qubit unitary operator that maps $\mathcal{P}(1)$ to itself under conjugation.

Now, let $UXU^\dagger = Q$ and $UZU^\dagger = R$. Note that since U is an automorphism it cannot map X or Z to $\pm I$, so neither R nor Q can be $\pm I$. Then by Lemma 3.2.4, there exists some $V \in \langle H, S \rangle$ such that $VXV^\dagger = Q$. Now let $F = V^\dagger U$. Thus $FXF^\dagger = X$ and $FZF^\dagger = V^\dagger R V = R'$ for some $R' \in \mathcal{P}(1)$. Note that since F is an automorphism it is bijective, so it cannot map Z to $\pm X$, which implies that $R' \in \{\pm Y, \pm Z\}$. Then, by Lemma 3.2.5, there exists a G such that $GR'G^\dagger = Z$ and $GXG^\dagger = X$. So:

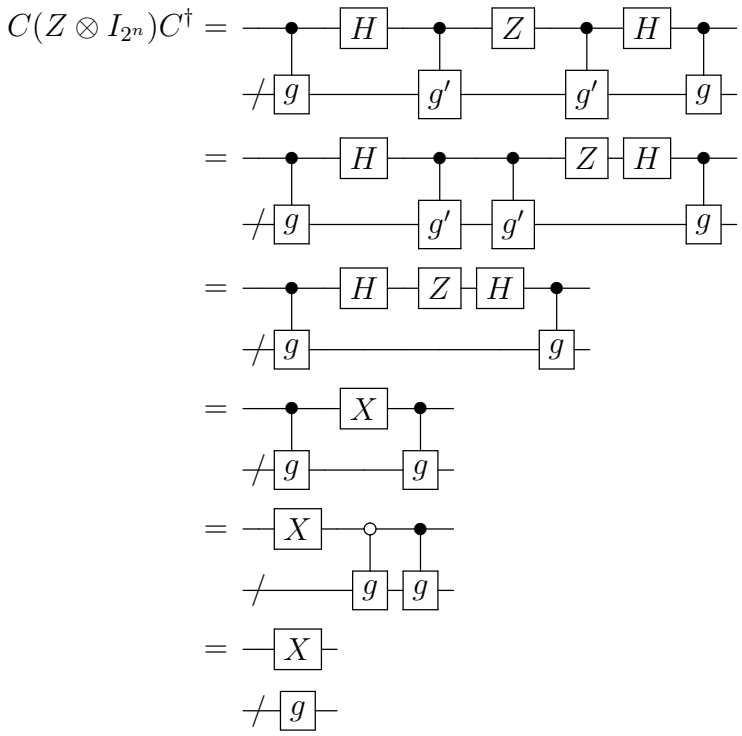
$$GFXF^\dagger G^\dagger = GXG^\dagger = X \quad \text{and} \quad GFZF^\dagger G^\dagger = GR'G^\dagger = Z.$$

Since $\mathcal{P}(1)$ is generated by X, Z, and the scalar i, we have $GFPF^\dagger G^\dagger = P$ for all Pauli operators P. Now, following the arguments from [16], observe that every complex 2×2-matrix can be written in the form $aI + bX + cY + dZ$, for $a, b, c, d \in \mathbb{C}$. It follows that $GFMF^\dagger G^\dagger = M$ for all operators M. This implies that GF is a scalar, which means that $U = VG^\dagger$ up to a global phase. From this, up to a global phase, U is comprised of only H and S gates as desired.

Now, suppose U is an $n+1$ qubit unitary that maps Paulis to Paulis under conjugation and first suppose that $U(Z \otimes I_{2^n})U^\dagger = X \otimes g$ and $U(X \otimes I_{2^n})U^\dagger = Z \otimes g'$ for some $g, g' \in \mathcal{P}_n$. Now, define a circuit C as:



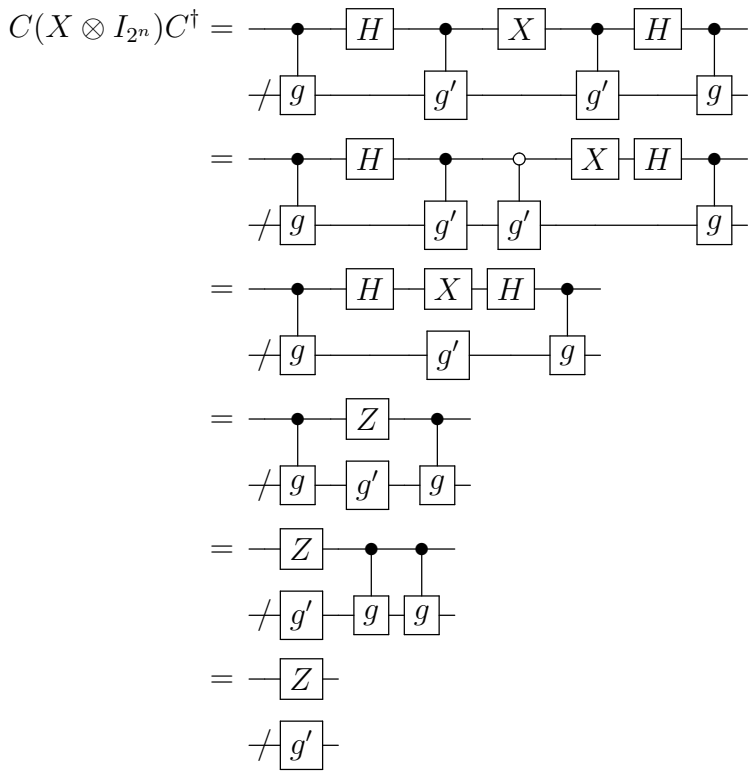
where the "strike" on the bottom wire indicates that g and g' possibly act on multiple qubits. Now observe that $C(Z \otimes I_{2^n})C^\dagger = X \otimes g$ as follows:



Note that g and g' commute, as can be seen below:

$$\begin{aligned} XZ \otimes gg' &= (X \otimes g)(Z \otimes g') \\ &= U(Z \otimes I_{2^n})U^\dagger U(X \otimes I_{2^n})U^\dagger \\ &= -U(X \otimes I_{2^n})(Z \otimes I_{2^n})U^\dagger \\ &= -U(X \otimes I_{2^n})U^\dagger U(Z \otimes I_{2^n})U^\dagger \\ &= -(Z \otimes g')(X \otimes g) \\ &= -(ZX \otimes g'g) \\ &= XZ \otimes g'g \end{aligned}$$

Then we have that $I \otimes gg' = I \otimes g'g$, which implies that $gg' = g'g$. Now we make use of this commutation to show that $C(X \otimes I_{2^n})C^\dagger = Z \otimes g'$:



Note here that g and g' are multiqubit gates, and the wire it is on is representing n wires or n qubits. Now, consider $U' := C^\dagger U$. Then

$$U'(X \otimes I_{2^n})U'^\dagger = C^\dagger U(X \otimes I_{2^n})U^\dagger C = C^\dagger(Z \otimes g')C = (X \otimes I_{2^n})$$

and

$$U'(Z \otimes I_{2^n})U'^\dagger = C^\dagger U(Z \otimes I_{2^n})U^\dagger C = C^\dagger(X \otimes g)C = (Z \otimes I_{2^n}).$$

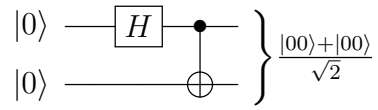
Now note that for any n-qubit Pauli operator P, we have $U'(I \otimes P)U'^\dagger = I \otimes Q$ for some $Q \in \mathcal{P}(n)$. This is because $I \otimes P$ commutes with both $X \otimes I$ and $Z \otimes I$, and therefore so must $U'(I \otimes P)U'^\dagger$. It follows that there is some U'' such that for all R in $\mathcal{P}(n+1)$, $U'RU'^\dagger = (I_2 \otimes U'')R(I_2 \otimes U'')^\dagger$. We can apply similar arguments as above to get that $U' = I_2 \otimes U''$ up to a global phase, say $U' = \phi(I_2 \otimes U'')$. Now note that C is a Clifford circuit since the controlled g and g' gates are controlled Pauli gates, which can be realized by conjugating the $CNOT$ gate with some combinations of H and S gates. By the induction hypothesis, there is a Clifford circuit D that is equal to U'' up to some global phase, say $U'' = \psi D$. Hence $U = CU' = \phi C(I_2 \otimes U'') = \phi\psi C(I_2 \otimes D)$ as desired.

Now, suppose U is instead an arbitrary unitary matrix, that is not the identity, without the condition that $U(Z \otimes I_{2^n})U^\dagger = X \otimes g$ and $U(X \otimes I_{2^n})U^\dagger = Z \otimes g'$. We can still acquire these restrictions by conjugating U with other Clifford circuits as follows. Let $P = U(Z \otimes I_{2^n})U^\dagger$ and $Q = U(X \otimes I_{2^n})U^\dagger$. Then P and Q must be self-inverse Pauli operators, thus $P = \pm P_1 \otimes \cdots \otimes P_{n+1}$ and $Q = \pm Q1 \otimes \cdots \otimes Q_{n+1}$. Moreover, since $Z \otimes I_{2^n}$ and $X \otimes I_{2^n}$ anti-commute, so do P and Q. It follows that there is some j such that P_j and Q_j anti-commute. Assume without loss of generality that $j = 1$ (because otherwise we could apply a Clifford operator to swap the 1^{st} and j^{th} qubits). Then by Lemma 3.2.4 there exists some Clifford circuit E such that $X = E^\dagger P_1 E$, so that $(E^\dagger \otimes I_{2^n})U(Z \otimes I_{2^n})U^\dagger(E \otimes I_{2^n}) = X \otimes g$, where $g = P_2 \otimes \cdots \otimes P_{n+1}$. Now let $K = (E^\dagger \otimes I_{2^n})U$ and note that it also maps Paulis to Paulis. Hence, $K(X \otimes I_{2^n})K^\dagger = r \otimes g'$ for some $r = E^\dagger Q_1 E \in \{\pm Y, \pm Z\}$ and $g' \in \mathcal{P}(n)$. This allows us to use Lemma 3.2.5 to obtain some Clifford circuit F such that $FrF^\dagger = Z$ and $FXF^\dagger = X$. Now let $L = (F \otimes I_{2^n})K$ so that $L(X \otimes I_{2^n})L^\dagger = Z \otimes g'$. Thus, we can use the same arguments above to get that L is made up of H, S, and $CNOT$ gates, and since K, E, and F are also, it follows that U is as well. □

The above theorem, together with Corollary 3.2.3, shows that up to a scalar the Clifford group is the normalizer of the Pauli group.

3.3 Universal Extensions of the Clifford Gates

We can do many interesting things with Clifford circuits. In particular, we can create superpositions and entanglement of states. A superposition is a linear combination of single ket vectors, so simply applying H to $|0\rangle$ would give $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. To achieve entanglement means to find some circuit that when applied to some unentangled qubits the output state is an entangled state. As an example, consider the entangled state $\frac{|00\rangle+|11\rangle}{\sqrt{1}}$, then the following circuit with input $|00\rangle$ will output the entangled state.



Note that the Clifford group is finite. This comes from the fact that it maps Paulis to Paulis under conjugation, effectively meaning that Clifford circuits act as

permutations of the Pauli group. Hence, since there are 4^{n+1} Paulis, there are at most $4^{(n+1)4^{n+1}}$ Cliffords. That is $|\mathcal{C}(n)| \leq 4^{(n+1)4^{n+1}}$. In fact, the exact cardinality of the Clifford group is well known and is $8 \cdot \prod_{i=1}^{n} 2(4^i - 1)4^i$ [16].

Moreover, the Gottesman-Knill theorem shows a relation in power between the quantum computer and classical computer.

Theorem 3.3.1 (Gottesman-Knill Theorem [13])**.** *Suppose a quantum computation is performed which involves only the following elements: state preparations in the computational basis, Hadamard gates, phase gates, controlled-NOT gates, Pauli gates, and measurements of observables in the Pauli group, together with the possibility of classical control conditioned on the outcome of such measurements. Such a computation may be efficiently simulated on a classical computer.*

In short, the Gottesman-Knill theorem states that stabilizer operations can be classically simulated efficiently (in polynomial time). There is an algorithm to do this on a classical computer with $O(n^2 m)$ operations, called the Tableau algorithm.

The Gottesman-Knill theorem (and the finiteness of the Clifford group) means that stabilizer operations are not *universal*. That is, there are quantum computations that cannot be simulated effectively with just the Clifford group and measurements. The next theorem, which is proved in [12], provides a fix for this.

Theorem 3.3.2. *If G is a non-Clifford gate then $\{H, S, CNOT, G\}$ is universal for quantum computing.*

A typical gate used to extend the Clifford group to be universal is the T gate, though the CS and CCZ gates are two other notable gates that will be used. Recall the matrices for the T, CS, and CCZ gates:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \quad CS = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

and

$$CCZ = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}.$$

Note the CCZ gate is used interchangeably with the CCX gate as they are equal upon simple conjugation by a H gate on the target qubit. To see why these gates are not in the Clifford group, simply observe the following example conjugation calculations from [4]:

$$TXT^\dagger = \tfrac{X+Y}{\sqrt{2}}$$

$$CS(X \otimes I)CS^\dagger = CNOT(S \otimes S^\dagger)CNOT(X \otimes I)$$

$$CCX(X \otimes I \otimes I)CCX^\dagger = (X \otimes I) \otimes \tfrac{I+Z_2+X_3-Z_2x_3}{2}$$

where X_3 means X applied to the 3^{rd} qubit, i.e. $X_3 = I \otimes I \otimes X$, and similarly for Z_2.

This naturally gives the sense that non-Clifford gates are a resource that enables full quantum computing, meaning that each non-Clifford gate is an expensive commodity that ideally is used as little as possible. This is also corroborated by the fact that in fault-tolerant quantum computing Clifford gates are typically cheap whereas non-Clifford gates are typically expensive. Thus this is the motivation behind attempting to limit the number of non-Clifford gates used. Finding lower bounds and upper bounds also gives an idea as to whether or not more or less of a certain non-Clifford gate can be used. If there is a circuit that uses the same number of non-Clifford gates as the calculated lower bound, then we know we cannot do any better.

3.4 Computing With States

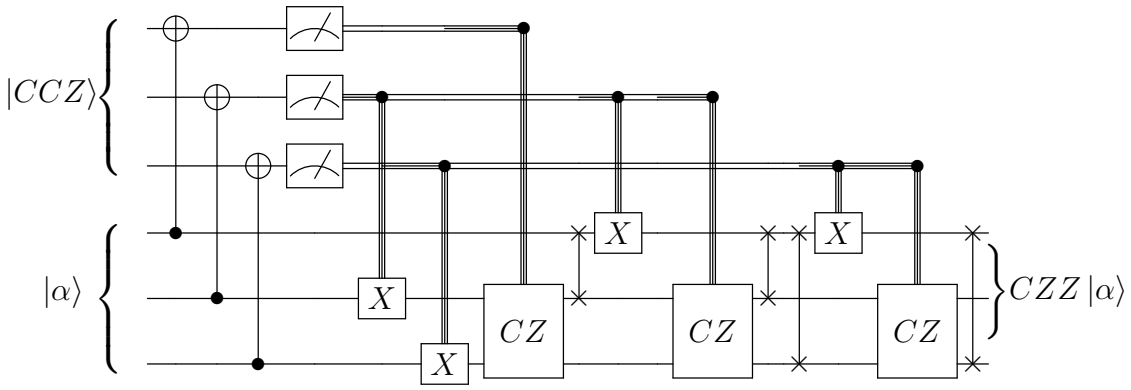
Instead of using non-Clifford gates to perform universal quantum computing, one can use a special kind of state to *inject* the desired gate into a circuit. The useful states for this purpose are defined below.

Definition 3.4.1. We define the following resource states:

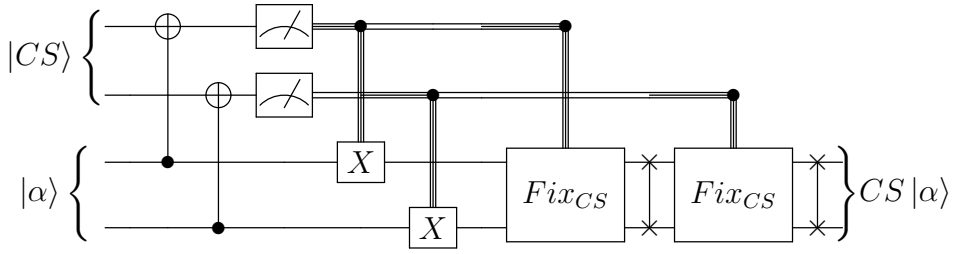
$$|T\rangle = T\,|+\rangle\,,\ \ |CS\rangle = CS\,|+\rangle^{\otimes 2}\,,\ \text{and}\ \ |CCZ\rangle = CCZ\,|+\rangle^{\otimes 3}\,.$$

The above states can be used to apply the corresponding gates using the injection circuits from [4]. We provide them here for reference.

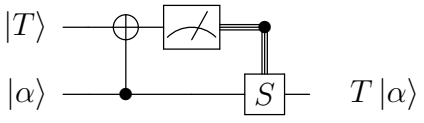
Figure 3.1: Injection circuits



(a) Injection circuit for the CCZ gate

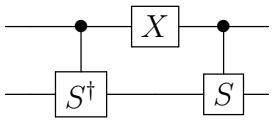


(b) Injection circuit for the CS gate



(c) Injection circuit for the T gate

The Fix_{CS} gate in the circuit for the $|CS\rangle$ state is



and

represents a SWAP gate, which simply exchanges the two inputs for each other.

In contrast to resource states, we also define a *stabilizer state*.

Definition 3.4.2. A *stabilizer state* is a state of the form $|\phi\rangle = C|0\rangle^{\otimes n}$ for some Clifford unitary C.

Definition 3.4.3. Let $|\psi\rangle$ be an n-qubit state and U be an operator. Then we say that $|\psi\rangle$ is *stabilized* by U if $U|\psi\rangle = |\psi\rangle$. The *stabilizer* of $|\psi\rangle$ is the subgroup $\mathcal{P}(n)$ consisting of the Paulis that stabilize $|\psi\rangle$. It is denoted by $\text{Stab}|\psi\rangle$.

This means that $\text{Stab}|\psi\rangle = \{P \in \mathcal{P}(n) \mid P|\psi\rangle = |\psi\rangle\}$. States for which the stabilizer contains only the identity matrix are said to have a trivial stabilizer.

The reason behind using this stabilizer formalism is that we can easily describe many quantum states by working with operators that stabilize them, rather than by explicitly working with the states themselves. Next are a few propositions regarding the stabilizer.

Proposition 3.4.4. *Let $|\psi\rangle$ be an n-qubit state. Then we have the following facts about* $\text{Stab}|\psi\rangle$*:*

1. $\text{Stab}|\psi\rangle$ *does not contain* $-I$.
2. *All Pauli group elements contained in* $\text{Stab}|\psi\rangle$ *commute with each other and are Hermitian matrices.*
3. *The cardinality of the stabilizer is equal to some power of two.*
4. *Given any Clifford Unitary C, the cardinality of* $\text{Stab}|\psi\rangle$ *is always equal to the cardinality of* $\text{Stab}(C|\psi\rangle)$.

5. *Finally, the cardinality of the stabilizer is multiplicative for the tensor products of states, that is* $|\text{Stab}(|\psi\rangle\,|\phi\rangle)| = |\text{Stab}\,|\psi\rangle\,| \cdot |\text{Stab}\,|\phi\rangle\,|$.

Proof.

1. If $-I \in \text{Stab}\,|\psi\rangle$, then $-|\psi\rangle = -I\,|\psi\rangle = |\psi\rangle$, which of course is not true for states (since unit vectors have at least one non-zero entry).

2. First note that for any two Paulis P, Q, they either commute or anti-commute. Now suppose $P, Q \in \text{Stab}\,|\psi\rangle$ anti-commute. Then $|\psi\rangle = PQ\,|\psi\rangle = -QP\,|\psi\rangle = -|\psi\rangle$. This implies that $-I \in \text{Stab}\,|\psi\rangle$, which from above can't be true, so P and Q must commute.

3. By Proposition 3.1.2 the cardinality of the Pauli group is a power of two, and since $\text{Stab}\,|\psi\rangle$ is a subgroup of the Pauli group, $|\text{Stab}\,|\psi\rangle\,|$ must divide a power of two, thus it must also be a power of two.

4. Recall that Clifford unitaries normalize Pauli matrices. Now let $P \in \text{Stab}\,|\psi\rangle$ and let C be some Clifford unitary. Then $CPC^\dagger C\,|\psi\rangle = CP\,|\psi\rangle = C\,|\psi\rangle$, so $CPC^\dagger \in \text{Stab}(C\,|\psi\rangle)$. Now consider the map $\theta_C : \text{Stab}\,|\psi\rangle \to \text{Stab}(C\,|\psi\rangle)$ which acts as $P \mapsto CPC^\dagger$. This map has an inverse, $\theta_{C^\dagger} : \text{Stab}(C\,|\psi\rangle) \longrightarrow \text{Stab}(C^\dagger C\,|\psi\rangle)$, which acts as $P' \mapsto C^\dagger P' C$ (where we note that $\text{Stab}(C^\dagger C\,|\psi\rangle) = \text{Stab}\,|\psi\rangle$). Thus θ_C is a bijection, and so we have that $|\text{Stab}\,|\psi\rangle\,| = |\text{Stab}(C\,|\psi\rangle)|$.

5. Let $|\psi\rangle$ and $|\phi\rangle$ be states on n and m qubits, respectively. First note that if P is in $\text{Stab}\,|\psi\rangle$ and Q is in $\text{Stab}\,|\phi\rangle$, then $P \otimes Q$ is in $\text{Stab}\,|\psi\rangle\,|\phi\rangle$. This defines a map $\theta : \text{Stab}\,|\psi\rangle \times \text{Stab}\,|\phi\rangle \longrightarrow \text{Stab}\,|\psi\rangle\,|\phi\rangle$, namely $\theta(P, Q) = P \otimes Q$. We will show that θ is one-to-one and onto, thus establishing a bijection between $\text{Stab}\,|\psi\rangle\,|\phi\rangle$ and a set of size $|\text{Stab}\,|\psi\rangle\,| \cdot |\text{Stab}\,|\phi\rangle\,|$.

   To show that θ is one-to-one, consider P, P' in $\text{Stab}\,|\psi\rangle$ and Q, Q' in $\text{Stab}\,|\phi\rangle$ and assume that $\theta(P, Q) = \theta(P', Q')$, i.e. $P \otimes Q = P' \otimes Q'$. By properties of the tensor product, this implies that there exists some scalar λ such that $P = \lambda P'$ and $Q = \lambda^{-1} Q'$. But since both P and P' are stabilizers of $|\psi\rangle$, we must have $\lambda = 1$. Thus $P = P'$ and $Q = Q'$, showing the θ is one-to-one.

   To show that θ is onto, consider any R in $\text{Stab}\,|\psi\rangle\,|\phi\rangle$. Since R is an nm-qubit Pauli operator, we can write $R = R_1 \otimes R_2$ where R_1 and an n-qubit Pauli and

R_2 is an m-qubit Pauli. We have $R_1 |\psi\rangle \otimes R_2 |\phi\rangle = (R_1 \otimes R_2)(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\phi\rangle$. By properties of the tensor product, there exists some scalar λ such that $R_1 |\psi\rangle = \lambda |\psi\rangle$ and $R_2 |\phi\rangle = \lambda^{-1} |\phi\rangle$. Let $P = \lambda^{-1} R_1$ and $Q = \lambda R_2$. Then $P |\psi\rangle = |\psi\rangle$ and $Q |\phi\rangle = |\phi\rangle$, and hence $P \in \text{Stab} |\psi\rangle$ and $Q \in \text{Stab} |\phi\rangle$. Moreover, $\theta(P, Q) = P \otimes Q = \lambda^{-1} R_1 \otimes \lambda R_2 = R_1 \otimes R_2 = R$. Therefore θ is onto.

□

Theorem 3.4.5. *Let $|\psi\rangle$ be an n-qubit state. Then $|\psi\rangle$ is a stabilizer state if and only if $|\text{Stab} |\psi\rangle| = 2^n$.*

Proof. For the left-to-right direction, recall that $|\psi\rangle = C |0\rangle^{\otimes n}$ for some Clifford circuit C. Then, by fact 4 from Proposition 3.4.4, $|\text{Stab} |\psi\rangle| = |\text{Stab} |0\rangle^{\otimes n}|$. Since the $|0\rangle^{\otimes n}$ vector is the basis vector $[1\ 0\ \cdots\ 0]^\dagger$, it can be seen that the only Pauli matrices that are in $\text{Stab} |0\rangle^{\otimes n}$ are tensor products of the Pauli matrices Z and I. There are 2^n different Pauli matrices of this form, giving us that $2^n = |\text{Stab} |0\rangle^{\otimes n}| = |\text{Stab} |\psi\rangle|$.

For the other direction assume $|\text{Stab} |\psi\rangle| = 2^n$. In [1], Theorem 8 states that $|\psi\rangle$ can be represented by a tableau, which can then be converted into a tableau that represents the $|00\ldots0\rangle$ state using only Clifford operations. Applying these Clifford operators is equivalent to applying Clifford operators to the appropriate qubits of $|\psi\rangle$, thus resulting in a Clifford circuit C such that $C |\psi\rangle = |00\ldots0\rangle$. □

An example of a non-stabilizer state is $|\psi\rangle = (\frac{2}{\sqrt{5}} |00\rangle + \frac{i}{\sqrt{5}} |11\rangle)$, where through computation one can find that it has the following stabilizers: $I \otimes I$ and $Z \otimes Z$. Since there are only 2 stabilizers, and $2 \neq 2^2$, $|\psi\rangle$ cannot be a stabilizer state.

Lemma 3.4.6. *Let $|\psi\rangle$ be an n-qubit state. Then $|\text{Stab} |\psi\rangle| \leq 2^n$.*

Proof. It is known from [1] that any subgroup of the n-qubit Pauli group that is commutative and does not contain $-I$ can have at most 2^n elements. Since $|\text{Stab} |\psi\rangle|$ is such a subgroup, the claim follows.

□

Theorem 3.4.7. *If $|\psi\rangle$ is an n-qubit stabilizer state, then $\text{Stab} |\psi\rangle$ uniquely determines $|\psi\rangle$ up to a phase.*

Proof. First consider the case $|\psi\rangle = |0\rangle$. In this case, the stabilizer is generated by $Z \otimes I \cdots \otimes I$, $I \otimes Z \otimes I \otimes \cdots \otimes I$, $\ldots$, $I \otimes \cdots \otimes I \otimes Z$. Suppose $|\phi\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle$ is another state with the same stabilizer, where $|j\rangle$ denotes the basic state corresponding to the binary expansion of j. If $j \neq 0$, then the binary expansion of j has some non-zero bit, say in position k. Then $(I \otimes \cdots \otimes I \otimes Z \otimes I \otimes \cdots \otimes I)\,|j\rangle = -\,|j\rangle$, where Z appears on the k^{th} qubit. Therefore, $\alpha_j = 0$. This proves that $|\phi\rangle = \alpha_0\,|0\rangle$, so $|\phi\rangle$ differs from $|0\rangle$ only by a phase.

Next, suppose that $|\psi\rangle$ and $|\psi'\rangle$ are stabilizer states that have the same stabilizer. Let C be some Clifford operator such that $C\,|\psi\rangle = |0\rangle$. Note $C\,|\psi\rangle$ and $C\,|\psi'\rangle$ have the same stabilizer, and therefore by the above, $C\,|\psi'\rangle$ differs from $|0\rangle$ by a phase. Hence $|\psi\rangle = |\psi'\rangle$ up to a phase.

□

Chapter 4

Monotones

In this chapter, we introduce *monotones*, which are real-valued functions of states. In the next chapter, we will use these monotones to derive lower bounds for quantum circuits.

4.1 Abstract Monotones

Recall that $\mathcal{S}$ is the collection of all states. We say that a collection of states $\mathcal{I} \subseteq \mathcal{S}$ is *closed under tensor products* if $|\phi\rangle, |\psi\rangle \in \mathcal{I}$ implies $|\phi\rangle \otimes |\psi\rangle \in \mathcal{I}$. Similarly, we say that $\mathcal{I}$ is *closed under the action of stabilizers* if $|\phi\rangle \in \mathcal{I}$ and $C \in \mathcal{C}(n)$ implies $C|\phi\rangle \in \mathcal{I}$.

Definition 4.1.1. Let $\mathcal{J} \subseteq \mathcal{S}$ and suppose that $\mathcal{J}$ is closed under tensor products and the action of stabilizers. A *monotone* for $\mathcal{J}$ is a function $M : \mathcal{J} \to \mathbb{R}^{\geq 0}$ such that:

- $M(|\phi\rangle) = 0$ if and only if $|\phi\rangle$ is a stabilizer state
- if C is a stabilizer operator then $M(C|\phi\rangle) \leq M(|\phi\rangle)$ for all $|\phi\rangle \in \mathcal{J}$.

Proposition 4.1.2. *We may consider the following properties for monotones:*

- $M(|\phi\rangle \otimes |\psi\rangle) = M(|\phi\rangle) + M(|\psi\rangle)$ *(additive)*
- $M(|\phi\rangle \otimes |\psi\rangle) = M(|\phi\rangle) \cdot M(|\psi\rangle)$ *(multiplicative)*
- $M(C|\phi\rangle) \leq M(|\phi\rangle)$ *where C is a Pauli measurement (non-increasing under Pauli measurements)*
- $M(|\phi\rangle) = M(|\phi\rangle|\psi\rangle)$ *for all stabilizer states $|\psi\rangle$ (stable under stabilizer ancillas)*

4.2 The Stabilizer Nullity

Definition 4.2.1 (stabilizer nullity)**.** Let $|\psi\rangle$ be an n-qubit state. The *stabilizer nullity* of $|\psi\rangle$ is denoted by $\nu(|\psi\rangle)$ and is defined as $\nu(|\psi\rangle) = n - \log_2 |\mathrm{Stab}\,|\psi\rangle\,|$.

Proposition 4.2.2. *The stabilizer nullity is a monotone.*

Proof. First, by Proposition 3.4.4 and Lemma , 3.4.6, for any n-qubit state $|\psi\rangle$ we have $|\mathrm{Stab}\,|\psi\rangle\,| \leq 2^n$ and is a power of 2. Hence, $\nu(|\psi\rangle)$ is always a positive integer and so ν is a (non-negative) real valued function. Again, by Proposition 3.4.4 recall that for a Clifford unitary C and a state $|\psi\rangle$ we have that $|\mathrm{Stab}(C\,|\psi\rangle)| = |\mathrm{Stab}\,|\psi\rangle\,|$. Thus $\nu(C\,|\psi\rangle) = n - \log_2 |\mathrm{Stab}(C\,|\psi\rangle)| = n - \log_2 |\mathrm{Stab}\,|\psi\rangle\,| = \nu(|\psi\rangle)$. Next, if $|\psi\rangle$ is a stabilizer state, then $|\mathrm{Stab}\,|\psi\rangle\,| = 2^n$ by Proposition 3.4.4, so $\nu(|\psi\rangle) = n - \log_2(|\mathrm{Stab}\,|\psi\rangle\,|) = n - \log_2(2^n) = 0$. Conversely, if $\nu(|\psi\rangle) = 0$, then $n = \log_2(|\mathrm{Stab}\,|\psi\rangle\,|)$ which implies that $|\mathrm{Stab}\,|\psi\rangle\,| = 2^n$. By Proposition 3.4.4 it follows that $|\psi\rangle$ is a stabilizer state. □

Proposition 4.2.3. *The stabilizer nullity is additive.*

Proof. Let $|\psi\rangle$ and $|\phi\rangle$ be an n-qubit state and an m-qubit state respectively. By Proposition 3.4.4 we have $|\mathrm{Stab}(|\psi\rangle\,|\phi\rangle)| = |\mathrm{Stab}\,|\psi\rangle\,| \cdot |\mathrm{Stab}|\phi\rangle|$. Hence:

$$\begin{aligned}\nu(|\psi\rangle\,|\phi\rangle) &= n + m - \log_2 |\mathrm{Stab}(|\psi\rangle\,|\phi\rangle)| \\ &= n + m - \log_2 |\mathrm{Stab}\,|\psi\rangle\,| - \log_2 |\mathrm{Stab}|\,|\phi\rangle\,| \\ &= \nu(|\psi\rangle) + \nu(|\phi\rangle).\end{aligned}$$

□

Now we want to show that ν is non-increasing under Pauli measurements, but before we do this we need the following Proposition.

Proposition 4.2.4. *If P and Q are Hermitian Pauli operators and $PQ = -QP$ then the operator*

$$C = \frac{I - PQ}{\sqrt{2}}$$

is a Clifford operator.

Proof. Let U be a Pauli. Then

$$CUC^\dagger = \frac{U - U(PQ)^\dagger - (PQ)U + (PQ)U(PQ)^\dagger}{2}.$$

We have two cases now, the first being $PQU = UPQ$ (i.e., PQ and U commute). Then

$$\begin{aligned} CUC^\dagger &= \frac{2U - (U(PQ)^\dagger + UPQ)}{2} \\ &= \frac{2U - (UQP + UPQ)}{2} \\ &= \frac{2U - (-UPQ + UPQ)}{2} \\ &= U. \end{aligned}$$

Naturally the second case is when $PQU = -UPQ$ (i.e., PQ anti-commutes with U). Then

$$\begin{aligned} CUC^\dagger &= \frac{U - U(PQ)^\dagger - UPQ - U}{2} \\ &= \frac{-UQP + UPQ}{2} \\ &= \frac{-UQP - UQP}{2} \\ &= \frac{-2UQP}{2} \\ &= -UQP. \end{aligned}$$

In either case, $CUC^\dagger$ is a Pauli, so C is a Clifford by Proposition 3.2.3. □

Lemma 4.2.5. *Let $|\psi\rangle$ be an n-qubit state and let P be an n-qubit Pauli matrix. Assume that the probability of a $+1$ outcome when measuring P on $|\psi\rangle$ is non-zero and let $|\phi\rangle$ be the state after measurement. Then $|Stab\,|\phi\rangle\,| \geq |Stab\,|\psi\rangle\,|$.*

Proof. Let P be an n-qubit Pauli and $|\psi\rangle$ an n-qubit state. Recall that for a Pauli measurement on P the probability of a $+1$ outcome is $\langle\psi|P_{+1}|\psi\rangle$, with post measurement state $|\phi\rangle = \frac{P_{+1}|\psi\rangle}{\sqrt{\langle\psi|P_{+1}|\psi\rangle}} = \frac{(I+P)|\psi\rangle}{2\sqrt{\langle\psi|P_{+1}|\psi\rangle}}$. With this, we have three different cases to consider. First is the simple case when P is in Stab $|\psi\rangle$. Here we have:

$$|\phi\rangle = \frac{(I+P)\,|\psi\rangle}{2\,\langle\psi|P_{+1}|\psi\rangle} = \frac{|\psi\rangle}{\langle\psi|P_{+1}|\psi\rangle}.$$

Since $|\psi\rangle$ and $|\phi\rangle$ differ by a phase, $|\text{Stab}\,|\phi\rangle\,| = |\text{Stab}\,|\psi\rangle\,|$.

Next consider when P is not in $\text{Stab}|\psi\rangle$. Then we have two alternative possibilities. The first alternative is when P commutes with all elements of $\text{Stab}\,|\psi\rangle$. Let $Q \in \text{Stab}|\psi\rangle$ so that $PQ = QP$. Then

$$Q\,|\phi\rangle = \frac{Q(I+P)\,|\psi\rangle}{2\,\langle\psi|P_{+1}|\psi\rangle} = \frac{(I+P)Q\,|\psi\rangle}{2\,\langle\psi|P_{+1}|\psi\rangle} = \frac{(I+P)\,|\psi\rangle}{2\,\langle\psi|P_{+1}|\psi\rangle} = |\phi\rangle\,.$$

Thus $Q \in \text{Stab}\,|\phi\rangle$ and so $|\text{Stab}\,|\phi\rangle\,| \supseteq |\text{Stab}\,|\psi\rangle\,|$ which implies that $|\text{Stab}\,|\phi\rangle\,| \geq |\text{Stab}\,|\psi\rangle\,|$.

Finally the second alternative is when there exists at least one $Q \in \text{Stab}\,|\psi\rangle$ such that Q and P anti-commute. Note this means that $Q\,|\psi\rangle = |\psi\rangle$ and $QPQ = -P$, so the probability of the $+1$ outcome is $\langle\psi|\,(I+P)\,|\psi\rangle\,/2 = \langle\psi|\,Q(I+P)Q\,|\psi\rangle\,/2 = \langle\psi|\,(I-P)\,|\psi\rangle\,/2$, which is the probability of the -1 outcome. Since these two probabilities must add up to be 1, the probability of both the $+1$ and -1 outcome is $1/2$. Then the post measurement state becomes:

$$|\phi\rangle = \frac{(I+P)\,|\psi\rangle}{2\,\langle\psi|P_{+1}|\psi\rangle} = \frac{(I+P)\,|\psi\rangle}{2\sqrt{1/2}} = \frac{(I+P)\,|\psi\rangle}{\sqrt{2}},$$

where we fixed the normalization condition such that $\langle\phi|\phi\rangle = \langle\psi|\psi\rangle$. Also, observe that we can write $|\phi\rangle = (I+PQ)/\sqrt{2}\,|\psi\rangle$ since Q stabilizes $|\phi\rangle$. Since $(I+PQ)/\sqrt{2}$ is a Clifford unitary by Proposition 4.2.4, we see that $|\phi\rangle$ and $|\psi\rangle$ differ by a Clifford and therefore $|\text{Stab}\,|\psi\rangle\,| = |\text{Stab}\,|\phi\rangle\,|$. □

Corollary 4.2.6. *The stabilizer nullity is non-increasing under Pauli measurements.*

Proof. Let $|\psi\rangle$ be a nonzero n-qubit state, let P be an n-qubit Pauli operator, and let $|\phi\rangle$ be the state after measuring P on $|\psi\rangle$. By Lemma 4.2.5, we have $|\text{Stab}\,|\phi\rangle\,| = |\text{Stab}\,|\psi\rangle\,|$ or $|\text{Stab}\,|\phi\rangle\,| \geq |\text{Stab}\,|\psi\rangle\,|$. Either way, $|\text{Stab}\,|\phi\rangle\,| \geq |\text{Stab}\,|\psi\rangle\,|$ so that $\log_2|\text{Stab}\,|\phi\rangle\,| \geq \log_2|\text{Stab}\,|\psi\rangle\,|$. Hence

$$\begin{aligned}\nu(|\phi\rangle) &= n - \log_2|\text{Stab}\,|\phi\rangle\,| \\ &\leq n - \log_2|\text{Stab}\,|\psi\rangle\,| \\ &= \nu(|\psi\rangle).\end{aligned}$$

□

We finish this section with a notion that will be helpful in computing the stabilizer nullity of states. We write multisets using $\{|$ and $|\}$. Moreover, we sometimes indicate

the multiplicity of an element in brackets. For example the multiset $\{|a, a, b|\}$ will sometimes be written as $\{|a(2), b(1)|\}$.

Definition 4.2.7 (Pauli Spectrum)**.** Let $|\psi\rangle$ be an n-qubit state. The *Pauli spectrum* of $|\psi\rangle$ is denoted by $\mathrm{Spec}|\psi\rangle$ and is defined as:

$$\mathrm{Spec}\,|\psi\rangle = \left\{ \left| \frac{|\,\langle\psi|\,P\,|\psi\rangle\,|}{\langle\psi|\psi\rangle}, P \in \{I, X, Y, Z\}^{\otimes n} \right| \right\}.$$

The Pauli spectrum is a multiset with 4^n elements. These elements are real numbers between 0 and 1. Note that the number of 1's in the Pauli spectrum of $|\psi\rangle$ is $|\mathrm{Stab}\,|\psi\rangle\,|$. Hence the Pauli spectrum can be useful in computing the stabilizer nullity.

Example 4.2.8. Let $\theta \in \mathbb{R}$ and consider the state $|\theta\rangle = (|0\rangle + e^{i\theta}\,|1\rangle)/\sqrt{2}$. To calculate the Pauli spectrum, first note that $|\theta\rangle$ is normalized so $\langle\theta|\,|\theta\rangle = 1$, then by direct computation we have:

- $\langle\theta|\,I\,|\theta\rangle = \langle\theta|\theta\rangle = 1$
- $\langle\theta|\,X\,|\theta\rangle = (\langle 1|\,e^{-i\theta} + \langle 0|)(|1\rangle + e^{i\theta}\,|0\rangle)/2 = (e^{-i\theta} + e^{i\theta})/2 = \cos\theta$
- $\langle\theta|\,Y\,|\theta\rangle = (\langle 1|\,e^{-i\theta} + \langle 0|)(i\,|1\rangle - ie^{i\theta}\,|0\rangle)/2 = i(e^{-i\theta} - e^{i\theta})/2 = i(-2i\sin\theta)/2 = \sin\theta$
- $\langle\theta|\,Z\,|\theta\rangle = (\langle 1|\,e^{-i\theta} + \langle 0|)(|0\rangle - e^{i\theta}\,|1\rangle)/2 = 1 - 1 = 0$

Thus, the Pauli spectrum of $|\theta\rangle$ is $\{1, \cos\theta, \sin\theta, 0\}$. Moreover, if $\theta = 2k\pi/2$ for some integer k, then $X \in \mathrm{Stab}\,|\theta\rangle$, and if $\theta = (2k+1)\pi/2$, then $Y \in \mathrm{Stab}\,|\theta\rangle$. Observe that for all θ, $I \in \mathrm{Stab}\,|\theta\rangle$ and $Z \notin \mathrm{Stab}\,|\theta\rangle$, thus $|\mathrm{Stab}\,|\theta\rangle\,| = 2$ if and only if either X or $Y \in \mathrm{Stab}\,|\theta\rangle$, or more generally if $\theta = m\pi/2$, for some integer m. The state $|\theta\rangle$ is therefore a stabilizer state only for $\theta = m\pi/2$ for some integer m.

4.3 The Dyadic Monotone

Consider quantum states that have entries in $\mathbb{Z}[i, 1/2] = \left\{ \frac{a+ib}{2^k} : a, b, k, \in \mathbb{Z} \right\}$ when written in the computational basis. Indeed, $|C^nZ\rangle$ can be written as vectors with entries in the above set. We have a few noteworthy facts to observe here:

- The set $\mathbb{Z}[i, 1/2]$ is a ring since it is closed under addition, subtraction, multiplication and contains 0 and 1.

- If a state $|\psi\rangle$ has entries in $\mathbb{Z}[i, 1/2]$, then for any Hermitian multi-qubit Pauli operator P, the expectation $\langle\psi|P|\psi\rangle$ is in $\mathbb{Z}[i, 1/2]$. This is because the entries of any Pauli matrix, and $|\psi\rangle$, are in $\mathbb{Z}[i, 1/2]$, so when applying P to $|\psi\rangle$ you get that $P|\psi\rangle \in \mathbb{Z}[i, 1/2]$. Similarly, it follows that $\langle\psi|P|\psi\rangle \in \mathbb{Z}[i, 1/2]$.

- $\langle\psi|P|\psi\rangle$ can be written in the form $a/2^k$ for integers a and k. This follows from the fact that Pauli expectation values are self-adjoint and thus $\langle\psi|P|\psi\rangle \in \mathbb{Z}[1/2]$.

- For stabilizer states Pauli expectations can only be ± 1 and 0.

Before defining the next monotone, we must first introduce a few functions that will be used in its definition. Let us define $\bar{v}_2 : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$. Let $0 \neq q \in \mathbb{Q}$ so we can write $q = n/d$ with $n, d \in \mathbb{Z}$ and $\gcd(n, d) = 1$ (so it is in reduced form). By the fundamental theorem of arithmetic we can write $n = 2^{r_2} \cdot p_1^{r_{p_1}} \cdots p_m^{r_{p_m}}$ and $d = 2^{l_2} \cdot p_1^{l_{p_1}} \cdots p_m^{l_{p_m}}$ for $k_i, l_i \in \mathbb{Z}$ for all $i \in [m]$. So $q = 2^k \cdot p_1^{k_{p_1}} \cdots p_m^{k_{p_m}}$ where $k = r_2 - l_2$ and $k_j = r_{p_j} - l_{p_j}$. This map is unique so we define $\bar{v}_2(q) = k$ and $\bar{v}_2(0) = \infty$.

Remark: Let $q \in \mathbb{Q}$ be in reduced form as above. Then we have three different cases:

1. $n, d \equiv_2 1 \Rightarrow \bar{v}_2(q) = 0$

2. $n \equiv_2 0, d \equiv_2 1 \Rightarrow \bar{v}_2(q)$ is the largest power, k, of 2 such that $2^k | n$.

3. $n \equiv_2 1, d \equiv_2 0 \Rightarrow -\bar{v}_2(q)$ is the largest power, k, of 2 such that $2^k | d$.

Proposition 4.3.1.

- $\bar{v}_2(\pm 1) = 0$

- $\bar{v}_2(-q) = \bar{v}_2(q)$

- $\bar{v}_2(q_1 q_2) = \bar{v}_2(q_1) + \bar{v}_2(q_2)$

Now, we wish to extend $\bar{v}_2$ to the real subsets of $\mathcal{R}_d = \mathbb{Z}[\zeta_{2^{d+1}}, 1/2]$, where $\zeta_{2^{d+1}}$ is the 2^{d+1} primitive root of unity. To do this, first recall that the Galois group of a field extension is a set of automorphisms that fixes the base field, and forms a group under the operation of function composition. We denote the Galois group of a field extension F over its base field E by $Gal(F/E)$, and elements in this group are commonly denoted by σ. Note we are only concerned with field extensions over the field $\mathbb{Q}$, which are called algebraic number fields. Next we need the field norm for an algebraic number field F. This is denoted as $N : F \longrightarrow \mathbb{Q}$ where

$$N(\alpha) = \prod_{\sigma \in Gal(F/\mathbb{Q})} \sigma(\alpha).$$

In fact, for a field extension F and base field E, there is an alternative definition of the Galois group that comes from a polynomial $f \in E[x]$, which is typically called the minimal polynomial. Here f factors as a product of linear polynomials in $F[x]$, and more importantly, all automorphisms $\sigma \in Gal(F/E)$ are defined by mapping a root to other roots. The roots in such a polynomial are called conjugates.

Recall a cyclotomic field extension of $\mathbb{Q}$ is the field $\mathbb{Q}$ adjoined with a primitive root of unity, which we denote as ζ_q. Note in this thesis we are only concerned with ζ_q when $q = 2^{d+1}$. Now, for a cyclotomic field the minimal polynomial is

$$\Phi_{2^{d+1}} = \prod_{\substack{k=1 \\ \gcd(k,2^{d+1})=1}}^{2^{d+1}} (x - \zeta_{2^{d+1}}^k). \tag{4.1}$$

Each $\sigma \in Gal(\mathbb{Q}(\zeta_{2^{d+1}})/\mathbb{Q})$ sends $\zeta_{2^{d+1}}$ to one of its conjugates, and by Equation (4.1) above these are just the numbers $\zeta_{2^{d+1}}^k$ where $\gcd(k, 2^{d+1})$. This means that the σ's are defined in the following way: $\sigma_k(\zeta_{2^{d+1}}) = \zeta_{2^{d+1}}^k$. The next few propositions provide some basic properties of σ_k.

Proposition 4.3.2. *For all $x \in \mathbb{Q}[\zeta_{2^{d+1}}]$, $\sigma_j(\sigma_k(x)) = \sigma_{k \cdot j}(x)$.*

Proof. This follows immediately from the definition of σ_k, and how it simply raises $\zeta_{2^{d+1}}$ to the power of k. □

Proposition 4.3.3. *For all $x \in \mathbb{Q}[\zeta_{2^{d+1}}]$ and all odd k, $\sigma_{k+2^{d+1}}(x) = \sigma_{k \mod 2^{d+1}}(x) = \sigma_k(x)$.*

Proof. This follows from the periodicity of σ_k. □

Proposition 4.3.4. *$x \in \mathbb{Q}[\zeta_{2^{d+1}}]$ is rational if and only if for all odd k $\sigma_k(x) = x$.*

Proof. We prove the backwards direction as the forward direction follows immediately from the definition of σ_k. Consider $x = \sum_{j=0}^{2^d-1} a_j \zeta_{2^{d+1}}^j \in \mathbb{Q}[\zeta_{2^{d+1}}]$ and suppose that $\sigma_{2^d+1}(x) = x$. Observe that for all odd j, $\sigma_{2^d+1}(\zeta_{2^{d+1}}) = -\zeta_{2^{d+1}}$. Applying this to each term in the summand of x we get that $a_j = -a_j$ which implies $a_j = 0$. Then every non-zero term left in the summand of x has an even j, thus having a factor of 2 which implies that $x \in \mathbb{Q}[\zeta_{2^d}]$. Thus repeatedly applying this argument gives us that $x \in \mathbb{Q}$. □

From the Fundamental Theorem of Galois Theory one obtains the isomorphism

$$Gal(\mathbb{Q}(\zeta_{2^{d+1}})/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

which means that elements in $Gal(\mathbb{Q}(\zeta_{2^{d+1}})/\mathbb{Q})$ are precisely the σ_k's where

$$\gcd(k, 2^{d+1}) = 1.$$

Thus k takes only odd values, so that:

$$N_d(\alpha) = \prod_{k-odd} \sigma_k(\alpha) = \prod_{k=0}^{2^d-1} \sigma_{2k+1}(\alpha) \tag{4.2}$$

Remark: If $d \leq d'$ then $\mathbb{Q}(e^{i\cdot\pi/2^d}) \subseteq \mathbb{Q}(e^{i\cdot\pi/2^{d'}})$. Note the following propositions about N_d.

Proposition 4.3.5. *N_0 is trivial, meaning $N_0(x) = x$.*

Proof. $N_0(x) = \sigma_1(x)$, and since $\sigma_1(x)$ is trivial, so is $N_0(x)$. □

Proposition 4.3.6. *Let d be a positive integer. Then N_d is multiplicative.*

Proof. This follows from σ_k being multiplicative. □

Proposition 4.3.7. *The value of N_d is always rational.*

Proof. Observe the following:

$$\begin{aligned}\sigma_j(N_d(x)) &= \prod_{k\in\{1,3,\ldots,2^d-1\}} \sigma_j(\sigma_k(x)) \\ &= \prod_{k\in\{1,3,\ldots,2^d-1\}} \sigma_{j\cdot k \mod 2^{d+1}}(x) \\ &= \prod_{k\in\{1,3,\ldots,2^d-1\}} \sigma_{j\cdot k}(x) \\ &= N_d(x).\end{aligned}$$

The final equality comes from the fact that despite the different index variables we are computing the product for the same odd valued indices. Thus by Proposition 4.3.4 $N_d(x)$ is rational. □

Proposition 4.3.8. *Consider* $N_{d+1} : \mathbb{Q}(e^{i\cdot\pi/2^{d+1}}) \longrightarrow \mathbb{Q}$. *Then when restricting* N_{d+1} *to* $\mathbb{Q}(e^{i\cdot\pi/2^d})$ *we have* $N_{d+1} = N_d^2$.

Proof. For $\alpha \in \mathbb{Q}(e^{i\cdot\pi/2^d})$, we have:

$$\begin{aligned}N_{d+1}(\alpha) &= \prod_{k=0}^{2^{d+1}-1} \sigma_{2k+1}(\alpha) \\ &= \prod_{k=0}^{2^d-1} \sigma_{2k+1}(\alpha) \prod_{k=2^d}^{2^{d+1}-1} \sigma_{2k+1}(\alpha) \\ &= \prod_{k=0}^{2^d-1} \sigma_{2k+1}(\alpha) \prod_{k=0}^{2^d-1} \sigma_{2k+1}(\alpha) \\ &= N_d^2(\alpha).\end{aligned}$$

This follows from the fact that $\sigma_{2\cdot(2^d+i)+1} = \sigma_{1+2i}$ for $i \in \{0,\ldots,2^d-1\}$, since $\zeta_{2^{d+1}}^{2\cdot(2^d+i)+1} = \zeta_{2^{d+1}}^{1+2i}$. □

Recall that $\mathcal{R}_d = \mathbb{Z}[\zeta_{2^{d+1}}, 1/2]$.

Definition 4.3.9. The valuation function $v_2 : \bigcup_d \mathcal{R}_d \longrightarrow \mathbb{Q}$ is defined as

$$v_2(x) = \frac{\bar{v}_2(N_d(x))}{2^d} \tag{4.3}$$

where $d = \min\{y; x \in \mathbb{Q}(e^{i\cdot\pi/2^y})\}$.

Remark: In the above definition we could instead choose any d for which $x \in \mathbb{Q}(e^{i\cdot\pi/2^d})$ since if $d \leq d'$ and $x \in \mathbb{Q}(e^{i\cdot\pi/2^d})$ then $x \in \mathbb{Q}(e^{i\cdot\pi/2^{d'}})$. Then we have that $\frac{\bar{v}_2(N_d(x))}{2^d} = \frac{\bar{v}_2(N_{d'}(x))}{2^{d'}}$.

Proposition 4.3.10. *If $x \in \mathbb{Q}$ then $v_2(x) = \bar{v}_2(x)$.*

Proof. If $x \in \mathbb{Q}$ then $d = 0$ and $N_d(x) = N_0(x) = x$,

$$v_2(x) = \frac{\bar{v}_2(N_d(x))}{2^d} = \frac{\bar{v}_2(x)}{2^0} = \bar{v}_2(x).$$

□

Proposition 4.3.11. *If $x, x' \in \mathcal{R}_d$ then $v_2(x \cdot x') = v_2(x) + v_2(x')$.*

Proof. First we prove this for $\bar{v}_2$. If in their prime decomposition x and x' have factors 2^k and $2^{k'}$, respectively, then $x \cdot x'$ has a factor $2^{k+k'}$. Thus $\bar{v}_2(x \cdot x') = k + k'$. Now, since N_d is multiplicative, we have:

$$\begin{aligned} v_2(x \cdot x') &= \frac{\bar{v}_2(N_d(x \cdot x'))}{2^d} \\ &= \frac{\bar{v}_2(N_d(x) \cdot N_d(x'))}{2^d} \\ &= \frac{\bar{v}_2(N_d(x)) + \bar{v}_2(N_d(x'))}{2^d} \\ &= v_2(x) + v_(x'). \end{aligned}$$

□

The following propositions are required building blocks to be able to prove another important property of v_2 in Proposition 4.3.17.

Proposition 4.3.12. $N_d(1 - \zeta_{2^{d+1}}) = 2$

Proof. We proceed by induction on d. For $d = 0$ we have $N_0(x) = \sigma_1(x) = x$, so it is trivial, and thus $N_0(1 - \zeta_{2^{0+1}}) = 1 - \zeta_2 = 1 - (-1) = 2$. Now suppose the statement is true for d, that is $N_d(1 - \zeta_{2^{d+1}}) = 2$. Recall that $\sigma_k(\zeta_{2^{d+1}}) = \zeta_{2^{d+1}}^k$ so that $\sigma_{2j+1}(1 - \zeta_{2^{d+1}}) = (1 - \zeta_{2^{d+1}}^{2j+1})$. Also observe that $\zeta_{2^{d+1}}^{2^d} = -1$ and $\zeta_{2^{d+1}}^2 = \zeta_{2^d}$. Now by making the appropriate pairings we finish by showing that $N_{d+1}(1 - \zeta_{2^{d+2}}) =$

$N_d(1-\zeta_{2^{d+1}})$ in the following way:

$$\begin{aligned}
N_{d+1}(1-\zeta_{2^{d+2}}) &= \prod_{j=0}^{2^{d+1}-1}(1-\zeta_{2^{d+2}}^{2j+1}) \\
&= \prod_{j=0}^{2^{d}-1}(1-\zeta_{2^{d+2}}^{2j+1})(1-\zeta_{2^{d+2}}^{2j+1+2^d}) \\
&= \prod_{j=0}^{2^{d}-1}(1-\zeta_{2^{d+2}}^{2j+1}-\zeta_{2^{d+2}}^{2j+1+2^{d+1}}+\zeta_{2^{d+2}}^{4j+2+2^{d+1}}) \\
&= \prod_{j=0}^{2^{d}-1}\left(1-\zeta_{2^{d+1}}^{2j+1}-(\zeta_{2^{d+2}}^{2j+1}-\zeta_{2^{d+2}}^{2j+1})\right) \\
&= \prod_{j=0}^{2^{d}-1}(1-\zeta_{2^{d+1}}^{2j+1}) \\
&= N_d(1-\zeta_{2^{d+1}}).
\end{aligned}$$

□

Proposition 4.3.13. *Let $x \in \mathbb{Z}[\zeta_{2^{d+1}}]$, then $N_d(x)$ is an integer. If x' is an element of $\mathcal{R}_d$ then $N_d(x') = a/2^K$ for integers a and K.*

Proof. The first statement of this proposition can be realized by applying the same arguments as in Propositions 4.3.4 and 4.3.7 but for $x \in \mathbb{Z}[\zeta_{2^{d+1}}]$ instead.

Now for $x' \in \mathcal{R}_d$, write it as $x' = x/2^k$ for some $x \in \mathbb{Z}[\zeta_{2^{d+1}}]$ and some integer k. Since $N_d(x)$ is multiplicative and $N_d(1/2^k) = (1/2^k)^{2^d}$, we have that $N_d(x') = N_d(x)/2^K$ for $K = 2^d \cdot k$. Since $N_d(x)$ is an integer, we can write $N_d(x') = a/2^K$ for some integer a. □

To complete the proof of the next proposition, recall the geometric sum formula:

$$\frac{1-x^n}{1-x} = \sum_{k=0}^{n-1} x^k. \tag{4.4}$$

Proposition 4.3.14. *$u_j = \left(1-\zeta_{2^{d+1}}^{2j-1}\right)/\left(1-\zeta_{2^{d+1}}\right)$ is a unit in $\mathbb{Z}[\zeta_{2^{d+1}}]$.*

Proof. Recall that if u_j is a unit then both u_j and u_j^{-1} are in $\mathbb{Z}[\zeta_{2^{d+1}}]$. Note that $1-x^{2j-1}$ is divisible by $(1-x)$, so the geometric formula in Equation (4.4) then gives us that:

$$\frac{1-x^{2j-1}}{1-x} = \sum_{k=0}^{2j-2} x^k.$$

Substituting x with $\zeta_{2^{d+1}}$ gives us that $u_j = \sum_{k=0}^{2j-2} \zeta_{2^{d+1}}^k$, and thus $u_j \in \mathbb{Z}[\zeta_{2^{d+1}}]$. To show that $u_j^{-1} \in \mathbb{Z}[\zeta_{2^{d+1}}]$, observe that $(2j-1)$ and 2^{d+1} are coprime, so by the extended Euclidean algorithm there exists a j' such that $j'(2j-1) = 1 \mod 2^{d+1}$. Using the geometric formula again, but for j' instead, we have:

$$\frac{1-x^{j'}}{1-x} = \sum_{k=0}^{j'-1} x^k.$$

This time by substituting x with $\zeta_{2^{d+1}}^{2j-1}$ we get $\left(1-\zeta_{2^{d+1}}^{(2j-1)j'}\right)/\left(1-\zeta_{2^{d+1}}^{2j-1}\right) \in \mathbb{Z}[\zeta_{2^{d+1}}]$. Indeed, by direct calculation we have that $u_j \cdot \left(1-\zeta_{2^{d+1}}^{(2j-1)j'}\right)/\left(1-\zeta_{2^{d+1}}^{2j-1}\right) = 1$ so that $u_j^{-1} = \left(1-\zeta_{2^{d+1}}^{(2j-1)j'}\right)/\left(1-\zeta_{2^{d+1}}^{2j-1}\right)$. □

Proposition 4.3.15. *$\alpha_d = 1 - \zeta_{2^{d+1}}$ is a prime element of $\mathbb{Z}[\zeta_{2^{d+1}}]$.*

Proof. Recall from number theory that elements of the ring of integers of a number field with a prime norm is a prime element of that ring of integers. In this case the number field is $\mathbb{Q}[\zeta_{2^{d+1}}]$ with ring of integers $\mathbb{Z}[\zeta_{2^{d+1}}]$. Since $N_d(\alpha_d) = 2$ which is a prime number, we get that α_d is a prime element. □

Proposition 4.3.16. *Let x' be an element of $\mathbb{Z}[\zeta_{2^{d+1}}]$. Then $v_2(x') \geq 0$ and for $k = 2^d v_2(x')$, x' can be written as $x''(1-\zeta_{2^{d+1}})^k$ for x'' in $\mathbb{Z}[\zeta_{2^{d+1}}]$ such that $v_2(x'') = 0$.*

Proof. Let $\alpha_d = 1 - \zeta_{2^{d+1}}$ and choose k to be the biggest power of α_d that divides x'. Then we can write $x' = \alpha_d^k x''$ such that x'' is from $\mathbb{Z}[\zeta_{2^{d+1}}]$ and α_d does not divide x''. Since $N_d(x'')$ is an integer by Proposition 4.3.13, if 2 does not divide $N_d(x'')$ then this will imply that $v_2(x'') = 0$.

Let us now suppose that 2 does indeed divide $N_d(x'')$, in an effort to find a contradiction. Then by Proposition 4.3.12, together with the definition of N_d, α_d divides 2 which implies that α_d divides $N_d(x'')$. Also, since α_d is prime by Proposition 4.3.15, α_d must also divide $\sigma_{2k+1}(x'')$ for some k. Note there exists j such that $(2j+1)(2k+1) \equiv 1 \mod 2^{d+1}$ and $\sigma_{2j+1}(\sigma_{2k+1}(x')) = x'$. Then, applying σ_{2j+1} to α_d and $\sigma_{2k+1}(x'')$ we get that $\sigma_{2j+1}(\alpha_d)$ divides x''. However, by Proposition 4.3.14 α_d divides $\sigma_{2j+1}(\alpha_d) = 1 - \zeta_{2^{d+1}}^{2j+1}$ and therefore it divides x''. This contradicts our initial description of x', so $v_2(x'') = 0$.

Finally, we have that

$$\begin{aligned} v_2(x') &= v_2(\alpha_d^k \cdot x'') \\ &= v_2(\alpha_d^k) + v_2(x'') \\ &= k \cdot v_2(\alpha_d) \\ &= k/2^d. \end{aligned}$$

Naturally we now have that $k = 2^d v_2(x')$, as desired. □

Proposition 4.3.17. *For x and $y \in \mathbb{Q}[\zeta_{2^{d+1}}]$ the following inequality holds:*

$$v_2(x+y) \geq \min(v_2(x), v_2(y)).$$

Proof. Note that for x and $y \in \mathbb{Q}[\zeta_{2^{d+1}}]$ there always exists an integer c such that $x' = cx$ and $y' = cy$ are both in $\mathbb{Z}[\exp(i\pi/2^d)]$. Then

$$v_2(x+y) = v_2((1/c)(x'+y')) = v_2(x'+y') + v_2(1/c).$$

Now by Proposition 4.3.16, we can write x' as $x''(1-\zeta_{2^{d+1}})^{k_x}$ and y' as $y''(1-\zeta_{2^{d+1}})^{k_y}$ for $k_x = 2^d v_2(x')$ and $k_y = 2^d v_2(y')$. Note this also means that x'' and y'' are in $\mathbb{Z}[\zeta_{2^{d+1}}]$ and $v_2(x'') = v_2(y'') = 0$. Moreover, let $k = \min(k_x, k_y)$. This way we can write:

$$\begin{aligned} x' + y' &= x''(1-\zeta_{2^{d+1}})^{k_x} + y''(1-\zeta_{2^{d+1}})^{k_y} \\ &= (1-\zeta_{2^{d+1}})^k (x''(1-\zeta_{2^{d+1}})^{k_x-k} + y''(1-\zeta_{2^{d+1}})^{k_y-k}). \end{aligned}$$

Now by Proposition 4.3.11,

$$v_2(x'+y') = v_2\big(1-\zeta_{2^{d+1}})^k\big) + v_2(x''(1-\zeta_{2^{d+1}})^{k_x-k} + y''(1-\zeta_{2^{d+1}})^{k_y-k}\big).$$

Since x'' and y'' are in $\mathbb{Z}[\zeta_{2^{d+1}}]$, $x''(1-\zeta_{2^{d+1}})^{k_x-k} + y''(1-\zeta_{2^{d+1}})^{k_y-k} \in \mathbb{Z}[\zeta_{2^{d+1}}]$ and thus it is also ≥ 0 by Proposition 4.3.16. Hence $v_2(x'+y') \geq v_2(1-\zeta_{2^{d+1}})^k$. Note that

$N_d(1-\zeta_{2^{d+1}})=2$ and recall that N_d is multiplicative. Then we get the following:

$$\begin{aligned}
v_2(1-\zeta_{2^{d+1}})^k &= \frac{\bar{v}_2(N_d((1-\zeta_{2^{d+1}})^k))}{2^d} \\
&= \frac{\bar{v}_2((N_d(1-\zeta_{2^{d+1}}))^k)}{2^d} \\
&= \frac{\bar{v}_2(2^k)}{2^d} \\
&= \frac{k}{2^d} \\
&= \frac{2^d \cdot \min(v_2(x'), v_2(y'))}{2^d} \\
&= \min(v_2(x'), v_2(y')).
\end{aligned}$$

Finally, putting it all together we arrive at

$$\begin{aligned}
v_2(x+y) &= v_2(x'+y') + v_2(1/c) \\
&\geq v_2(1-\zeta_{2^{d+1}})^k + v_2(1/c) \\
&= \min(v_2(x'), v_2(y')) + v_2(1/c) \\
&= \min(v_2(x'/c), v_2(y'/c)) \\
&= \min(v_2(x), v_2(y)).
\end{aligned}$$

□

The power of 2 in the denominator of the Pauli expectation gives us a sense of how "non-stabilizer" the state is. The definition of the dyadic monotone below gives us an intuition for this sort of measure.

Definition 4.3.18. Let $|\psi\rangle$ be an n-qubit state with entries in $\mathcal{R}_d$. Then the dyadic monotone is

$$\mu_2 |\psi\rangle = \texttt{max}\big\{ -v_2(\langle\psi|P|\psi\rangle) : P \in \{I,X,Y,Z\}^{\otimes n}\big\}.$$

The dyadic monotone basically is the maximum power of 2 in the denominator over the Pauli spectrum. Now note that it is invariant under Clifford unitaries because they map the set of all multi-qubit Pauli matrices to the set of all of all Pauli matrices up to a sign and v_2 is insensitive to the sign of its argument. The next proposition shows a similarity between ν and μ_2, namely the additive property under tensor products.

Proposition 4.3.19. *Let $|\phi\rangle$ and $|\psi\rangle$ be states with entries in $\mathcal{R}_d$; then*

$$\mu_2(|\phi\rangle \otimes |\psi\rangle) = \mu_2 |\phi\rangle + \mu_2 |\psi\rangle$$

Proof. Note that for Pauli matrices P and Q the expectations $\langle\phi|P|\phi\rangle$ and $\langle\psi|Q|\psi\rangle$ are non-zero. Thus, using distributive properties of the tensor product and v_2, we get:

$$\begin{aligned} v_2(\langle\phi| \otimes \langle\psi| (P \otimes Q) |\phi\rangle \otimes |\psi\rangle) &= v_2((\langle\phi| P + \langle\psi| Q) \otimes (|\phi\rangle \otimes |\psi\rangle)) \\ &= v_2(\langle\phi|P|\phi\rangle \cdot \langle\psi|Q|\psi\rangle) \\ &= v_2(\langle\phi|P|\phi\rangle) + v_2(\langle\psi|Q|\psi\rangle). \end{aligned}$$

□

Next, we want to show that that the dyadic monotone is minimal for stabilizer states. To do this we will need the following proposition.

Proposition 4.3.20. *Let x be a real element of $\mathcal{R}_d$ such that for all odd k, $|\sigma_k(x)| \leq 1$. Then $v_2(x) \leq 0$ and the equality is achieved if and only if $x = \pm 1$.*

Proof. The condition that $|\sigma_k(x)| \leq 1$ for all odd k implies that $N_d(x) \leq 1$, since $N_d(x)$ is just the product of all these σ's. Because $x \in \mathcal{R}_d$ we can write it as $z/2^k$ for $z \in \mathbb{Z}[\zeta_{2^{d+1}}]$. Then, since N_d is multiplicative by Proposition 4.3.6, $N_d(x) = N_d(z) \cdot N_d(2^k) = n/2^{2^d k}$, where $N_d(z) = n$ is an integer by Proposition 4.3.13. This together with $|N_d(x)| \leq 1$ implies $\bar{v}_2(n/2^k)$ is non-positive, which further implies that $v_2(x)$ is also.

Now, since n is an integer and $|N_d(x)| \leq 1$, $v_2(x) = 0$ if and only if $N_d(x) = n/2^{2^d k} = \pm 1$. Because $|\sigma_k(x)| \leq 1$ for all k, $N_d(x) = \pm 1$ only when $\sigma_k(x) = \pm 1$ for all k. Then by Proposition 4.3.4, $x = \pm 1$. □

Proposition 4.3.21. *Let $|\psi\rangle$ be a state in $\mathcal{R}_d$; then $\mu_2 |\psi\rangle \geq 0$, with equality achieved if and only if $|\psi\rangle$ is a stabilizer state.*

Proof. Consider a Pauli P expectation $\alpha = \langle\psi|P|\psi\rangle$. Because P has eigenvalues ± 1, by the spectral decomposition theorem it follows that $P = P_{+1} - P_{-1}$, where P_{+1} and P_{-1} are projectors that correspond to the eigenspaces $+1$ and -1 respectively. Since $\langle\psi|P_{+1}|\psi\rangle$ and $\langle\psi|P_{-1}|\psi\rangle$ are the probabilities of observing the

$+1$ or -1 outcomes respectively, which by definition are at most 1, we have that $|\langle\psi|P|\psi\rangle| = |\langle\psi|P_{+1}|\psi\rangle - \langle\psi|P_{-1}|\psi\rangle| \leq 1$. For odd k consider $\sigma_k(\alpha)$ and recall that σ_k preserves addition, multiplication, and conjugation. Thus we can write α_k as the expectation $\langle\psi_k|P_k|\psi_k\rangle$ where $|\psi_k\rangle$ and P_k are obtained by applying σ_k to $|\psi\rangle$ and P element-wise. It follows that $\alpha_k = \langle\psi_k|P_k|\psi_k\rangle = \sigma_k(\langle\psi|P|\psi\rangle) = \sigma_k(\alpha)$ and so $|\alpha_k| \leq 1$ since σ_k takes rational numbers to rational numbers. Then by Proposition 4.3.20, $v_2(\alpha) \leq 0$ which implies that μ_2 is always non-negative.

We now show that $\mu_2|\psi\rangle = 0$ if and only if $|\psi\rangle$ is a stabilizer state. If $|\psi\rangle$ is a stabilizer state, then $|\psi\rangle = C|0\rangle^{\otimes n}$ for some Clifford circuit C. But μ_2 is invariant under Clifford operations, so we actually have $\mu_2(|\psi\rangle) = \mu_2(|0\rangle^{\otimes n})$. Hence, since $\mu_2(|0\rangle^{\otimes n}) = 0$, we have $\mu_2(|\psi\rangle) = 0$. We now show the converse implication: if $\mu_2(|\psi\rangle) = 0$, then $|\psi\rangle$ is a stabilizer state.

Suppose that $\mu_2(|\psi\rangle) = 0$. Then all non-zero Pauli expectations of $|\psi\rangle$ are ± 1. The set $\{I, X, Y, Z\}^{\otimes n}$, denoted by $T(n)$, is an orthogonal basis of the space of matrices with respect to the inner product $\langle A, B\rangle = \mathtt{Tr}AB^\dagger$. This means that we can write $|\psi\rangle\langle\psi|$ as a linear combination of the basis elements, that is, as $\sum_{Q\in T(n)} \alpha_Q Q$. It follows that $\mathtt{Tr}(|\psi\rangle\langle\psi| P) = \sum_{Q\in T(n)} \alpha_Q \mathtt{Tr}(QP) = \alpha_P \cdot 2^n$ since the trace of a Pauli operator is zero aside from I, in which case it is 2^n. Noting also that $1 = \langle\psi|\psi\rangle = \mathtt{Tr}(|\psi\rangle\langle\psi|)$, observe the following:

$$\begin{aligned}
\mathtt{Tr}(|\psi\rangle\langle\psi|) &= \mathtt{Tr}(|\psi\rangle\langle\psi|\,|\psi\rangle\langle\psi|) \\
&= \mathtt{Tr}\Big(\sum_{P\in T(n)} \alpha_P P\big(\sum_{Q\in T(n)} \alpha_Q Q\big)\Big) \\
&= \Big(\sum_{P\in T(n)} \alpha_P\big(\sum_{Q\in T(n)} \alpha_Q \mathtt{Tr}(PQ)\big)\Big) \\
&= \sum_{P\in T(n)} \alpha_P\big(\alpha_P \cdot 2^n\big) \\
&= \sum_{P\in T(n)} (\alpha_P \cdot 2^n)^2/2^n \\
&= \frac{1}{2^n}\sum_{P\in T(n)} \big(\mathtt{Tr}(|\psi\rangle\langle\psi| P)\big)^2
\end{aligned} \tag{4.5}$$

Since $\langle\psi|P|\psi\rangle$ is either 0 or ± 1 we can write $|\mathrm{Stab}\,|\psi\rangle|| = \sum_{P\in T(n)} |\langle\psi|P|\psi\rangle|^2$. Now,

since the trace is cyclic, $\mathtt{Tr}(|\psi\rangle\langle\psi| P) = \mathtt{Tr}(\langle\psi|P|\psi\rangle) = \langle\psi|P|\psi\rangle$ and therefore

$$1 = \mathtt{Tr}(|\psi\rangle\langle\psi|) = \frac{1}{2^n}\sum_{P\in T(n)} \left(\mathtt{Tr}(|\psi\rangle\langle\psi| P)\right)^2 = \frac{1}{2^n}\sum_{P\in T(n)} |\langle\psi|P|\psi\rangle|^2 = \frac{1}{2^n}|\mathrm{Stab}\,|\psi\rangle\,|.$$

Hence, $|\mathrm{Stab}\,|\psi\rangle\,| = 2^n$ and $|\psi\rangle$ is a stabilizer state. □

Proposition 4.3.22. *Let $|\psi\rangle$ be a state with entries in $\mathcal{R}_d$, let P be a Pauli observable such that measuring its $+1$ eigenvalue has probability $1/2$ and let $|\psi_+\rangle$ be the normalized result of that measurement. Then $\mu_2|\psi\rangle \geq \mu_2|\psi_+\rangle$, so μ_2 is non-increasing under Pauli measurements.*

Proof. We proceed by bounding the value of v_2 for some Pauli operator Q evaluated on the expectation $\langle\psi_+|Q|\psi_+\rangle$. Since the normalized state is just the post measurement state, and we know the probability of the $+1$ eigenvalue is $1/2$, we have that

$$|\psi_+\rangle = \frac{(I+P)|\psi\rangle}{2\sqrt{\langle\psi|P_{+1}|\psi\rangle}} = \frac{(I+P)|\psi\rangle}{2\sqrt{1/2}} = \frac{I+P}{\sqrt{2}}|\psi\rangle\,.$$

The expectation of Q is therefore equal to

$$\langle\psi_+|Q|\psi_+\rangle = \frac{\langle\psi|(I+P)Q(I+P)|\psi\rangle}{2}.$$

If P and Q anti-commute then

$$\begin{aligned}\langle\psi_+|Q|\psi_+\rangle &= \frac{\langle\psi|(IQ+PQ)(I+P)|\psi\rangle}{2}\\ &= \frac{\langle\psi|(Q+-QP)(I+P)|\psi\rangle}{2}\\ &= \frac{\langle\psi|Q(I+-P)(I+P)|\psi\rangle}{2}\\ &= 0.\end{aligned}$$

Thus the expectation does not contribute to the calculation of μ_2. Similarly, when P and Q commute,

$$\begin{aligned}\langle\psi_+|Q|\psi_+\rangle &= \frac{\langle\psi|Q(I+P)(I+P)|\psi\rangle}{2}\\ &= \frac{\langle\psi|Q(I+2P+P^2|\psi\rangle}{2}\\ &= \frac{\langle\psi|Q(2I+2P)|\psi\rangle}{2}\\ &= \langle\psi|Q|\psi\rangle + \langle\psi|PQ|\psi\rangle\,.\end{aligned}$$

Now we use the inequality from Proposition 4.3.17 to see that

$$v_2(\langle\psi|Q|\psi\rangle + \langle\psi|PQ|\psi\rangle) \geq \texttt{min}(\langle\psi|Q|\psi\rangle, \langle\psi|PQ|\psi\rangle) \geq -\mu_2 |\psi\rangle.$$

Now recall that $v_2(\langle\psi|Q|\psi\rangle + \langle\psi|PQ|\psi\rangle) = v_2(\langle\psi_+|Q|\psi_+\rangle)$ which is equal to -$\mu_2 |\psi_+\rangle$ given our choice of Q. So finally by multiplying by -1, we have the result: $\mu_2 |\psi\rangle \geq \mu_2 |\psi_+\rangle$ □

Chapter 5

Applications

5.1 The C^nZ gate

The C^nZ gate is a gate worth considering in detail since it is used in many important algorithms, like Grover's search algorithm. We start by computing the Pauli spectrum of $|C^nZ\rangle$. Lower bounds on the resources required for this gate follow after this proposition.

Proposition 5.1.1. *For all $n \geq 3$, the Pauli spectrum of the state $|C^nZ\rangle$ is:* $\{|1\ \ (1),\ 0\ \ (-1+2^n+2^{2n+1}),\ 1-2^{1-n}\ \ (2^{n+1}-1),\ 2^{1-n}\ \ (1-3\cdot 2^n+2^{2n+1})|\}$.

Proof. We have

$$|C^nZ\rangle = C^nZ\,|+\rangle^{\otimes n} = \tfrac{1}{\sqrt{2^m}} \sum_{b\in\{0,1\}^m} (-1)^{b_1\cdot b_2\cdots b_m}\,|b\rangle,$$

where $|C^nZ\rangle$ is an $m = n+1$ qubit gate. We want to compute the Pauli expectation $\langle C^nZ|X^xZ^z|C^nZ\rangle$ where x and z are bit strings. Note that we need not consider the Pauli matrix Y since $Y = iXZ$, and the phase will vanish once we take the absolute value as in the definition of the Pauli spectrum. For one-bit bit strings i and j, observe that $Z^i\,|j\rangle = |j\rangle$ if $i = j = 0$ or $i \neq j$, and $Z^i\,|j\rangle = -\,|j\rangle$ if $i = j = 1$. So in general $Z^z\,|b\rangle = (-1)^{z\cdot b}\,|b\rangle$. Furthermore, $X^i\,|j\rangle = |i\oplus j\rangle$, where $\oplus$ is addition modulo 2, so for arbitrary bit strings it follows that $X^x\,|b\rangle = |b\oplus x\rangle$, where $b\oplus x$ is extended component-wise. We can now directly calculate as follows:

$$\begin{aligned}
2^m\,\langle C^nZ|X^xZ^z|C^nZ\rangle &= \sum_{b,b'\in\{0,1\}^m} (-1)^{b_1\cdot b_2\cdots b_m}(-1)^{b'_1\cdot b'_2\cdots b'_m}\,\langle b'|X^xZ^z|b\rangle \\
&= \sum_{b,b'\in\{0,1\}^m} (-1)^{b_1\cdot b_2\cdots b_m}(-1)^{b'_1\cdot b'_2\cdots b'_m}(-1)^{z\cdot b}\,\langle b'|X^x|b\rangle \\
&= \sum_{b,b'\in\{0,1\}^m} (-1)^{b_1\cdot b_2\cdots b_m}(-1)^{b'_1\cdot b'_2\cdots b'_m}(-1)^{z\cdot b}\,\langle b'|b\oplus x\rangle \\
&= \sum_{b\in\{0,1\}^m} (-1)^{b_1\cdot b_2\cdots b_m}(-1)^{(b_1\oplus x_1)\cdot(b_2\oplus x_2)\cdots(b_m\oplus x_m)}(-1)^{z\cdot b}.
\end{aligned}$$

Note that we have the last line since $\langle b'|b \oplus x\rangle = 0$ when $b' \neq b \oplus x$, and so we can substitute $b'_i = b_i \oplus x_i$.

When x is the zero vector $\mathbf{0}$, we get

$$2^m \langle C^n Z|X^x Z^z|C^n Z\rangle = \sum_{b\in\{0,1\}^m} ((-1)^{b_1\cdot b_2\cdots b_m})^2 (-1)^{z\cdot b} = \sum_{b\in\{0,1\}^m} (-1)^{z\cdot b}.$$

This is 2^m for $z = \mathbf{0}$. For any other z half of the terms in the summation will be -1 and the other half 1, giving 0.

Now consider the case when $x \neq \mathbf{0}$. Denoting $\mathbf{1}$ as the all one vector, if $b = \mathbf{1}$ then $b_1 \cdot b_2 \cdots b_m = 1$ and $(b_1 + x_1) \cdot (b_2 + x_2) \cdots (b_m + x_m) = 0$. Similarly, if $b = \mathbf{1} + x$, then $b_1 \cdot b_2 \cdots b_m = 0$ and $(b_1 + x_1) \cdot (b_2 + x_2) \cdots (b_m + x_m) = 1$, and in either case we get:

$$(-1)^{b_1\cdot b_2\cdots b_m}(-1)^{(b_1+x_1)\cdot(b_2+x_2)\cdots(b_m+x_m)}(-1)^{z\cdot b} = (-1)(-1)^{z\cdot b}.$$

For any other b we have $b_1 \cdot b_2 \cdots b_m = 0$ and $(b_1 + x_1) \cdot (b_2 + x_2) \cdots (b_m + x_m) = 0$, giving us

$$(-1)^{b_1\cdot b_2\cdots b_m}(-1)^{(b_1+x_1)\cdot(b_2+x_2)\cdots(b_m+x_m)}(-1)^{z\cdot b} = (-1)^{z\cdot b}.$$

Thus the terms in the sum over b differ from $\sum_{b\in\{0,1\}^m}(-1)^{z\cdot b}$ only for $b = \mathbf{1}$ and $b = \mathbf{1} + x$. Therefore,

$$\begin{aligned}
2^m \langle C^n Z|X^x Z^z|C^n Z\rangle &= \sum_{b\in\{0,1\}^m} (-1)^{b_1\cdot b_2\cdots b_m}(-1)^{(b_1+x_1)\cdot(b_2+x_2)\cdots(b_m+x_m)}(-1)^{z\cdot b} \\
&= -(-1)^{z\cdot\mathbf{1}} - (-1)^{z\cdot(\mathbf{1}+x)} + \sum_{b\in\{0,1\}^m\setminus\{\mathbf{1},\mathbf{1}+x\}} (-1)^{z\cdot b} \\
&= -2(-1)^{z\cdot\mathbf{1}} - 2(-1)^{z\cdot(\mathbf{1}+x)} + \sum_{b\in\{0,1\}^m} (-1)^{z\cdot b}.
\end{aligned}$$

When $z = \mathbf{0}$, this is simply $2^m - 4$. When $z \neq \mathbf{0}$, it is $-2(-1)^{z\cdot\mathbf{1}} - 2(-1)^{z\cdot(\mathbf{1}+x)}$, and we have two more final cases. The first is when $x \cdot z$ is odd, where we get:

$$\begin{aligned}
-2(-1)^{z\cdot\mathbf{1}} - 2(-1)^{z\cdot(\mathbf{1}+x)} &= -2(-1)^{z\cdot\mathbf{1}} - 2(-1)^{z\cdot\mathbf{1}}(-1)^{z\cdot x} \\
&= -2(-1)^{z\cdot\mathbf{1}} - 2(-1)^{z\cdot\mathbf{1}}(-1)^{1} \\
&= -2(-1)^{z\cdot\mathbf{1}} + 2(-1)^{z\cdot\mathbf{1}} \\
&= 0
\end{aligned}$$

and if $x \cdot z$ is even, then we have $-2(-1)^{z\cdot\mathbf{1}} - 2(-1)^{z\cdot\mathbf{1}} = -4(-1)^{z\cdot\mathbf{1}}$ instead, which simply becomes 4 since the Pauli spectrum requires we take the absolute value. We

can now summarize:

$$|\langle C^n Z|X^x Z^z|C^n Z\rangle| = \begin{cases} 1 & \texttt{if } z = \mathbf{0} \texttt{ and } x = \mathbf{0}, \\ 1 - 2^{2-m} & \texttt{if } z = \mathbf{0} \texttt{ and } x \neq \mathbf{0}, \\ 0 & \texttt{if } z \neq \mathbf{0} \texttt{ and either } x = \mathbf{0} \texttt{ or } x \neq \mathbf{0} \\ & \quad \texttt{and } x \cdot z \texttt{ is odd} \\ 2^{2-m} & \texttt{if } z \neq \mathbf{0} \texttt{ and } x \neq \mathbf{0} \texttt{ and } x \cdot z \texttt{ is even} \end{cases}$$

We can count the number of each subset of binary vectors x and z to find multiplicities. When, $x = \mathbf{0}$ and $z = \mathbf{0}$, there is clearly only one possible choice for each x and z, thus we have a multiplicity of 1. When $z = \mathbf{0}$ and $x \neq \mathbf{0}$, we now have only 1 possibility for z and $2^m - 1$ possibilities for x, giving a multiplicity of $2^m - 1$ for this case. Similarly, when $x = \mathbf{0}$ and $z \neq \mathbf{0}$ we have $2^m - 1$ possibilities again. Also, observe that $x \cdot z$ takes an odd value for $(2^{2m} - 2^m)/2$ different possible combinations of x and z pairings. Adding these and simplifying gives the multiplicity of the third case: $2^{2m-1} - 2^{m-1} - 1$. Finally, there are overall 2^{2m} different combinations of x and z pairings, so we can simply subtract all the multiplicities above from this to get the multiplicity of the fourth case, which comes out to be $2^{2m-1} - 3 \cdot 2^{m-1} + 1$. Substituting $n + 1$ for m then gives the stated result. □

Corollary 5.1.2. *We have the following stabilizer nullity values:*

$$\nu(|T\rangle) = 1, \quad \nu(|CS\rangle) = 2, \quad \nu(|CCZ\rangle) = 3, \quad \textit{and} \quad \nu(|C^n Z\rangle) = n + 1.$$

Proof. The first three follow by direct calculation. For $\nu(|C^n Z\rangle) = n + 1$, recall that if $|\psi\rangle$ is an m-qubit state then $\nu(|\psi\rangle) = m - \log_2 |\mathrm{Stab}(|\psi\rangle)|$. By Proposition 5.1.1 we have $|\mathrm{Stab}(|C^n Z\rangle)| = 1$ since the size of the stabilizer of a state is the multiplicity of 1 in its Pauli spectrum. Hence $\nu(|C^n Z\rangle) = n + 1 - \log_2(1) = n + 1 - 0 = n + 1$. □

Proposition 5.1.3. *For $n \geq 2$, the $C^n Z$ gate cannot be implemented with Clifford gates and measurements using fewer than $n + 1$ T gates, or $(n + 1)/2$ CS gates, or $(n + 1)/3$ CCZ gates.*

Proof. First note that proving that a bound holds for the state $|C^n Z\rangle$ implies that it holds for the gate $C^n Z$. Indeed, if we can perform a task with k $C^n Z$ gates then we

can also perform it with k $|C^nZ\rangle$ states using the circuits from Section 3.4. Hence, any lower bound on the number of required states is a lower bound on the number of required gates. Now, $\nu(|T\rangle) = 1$ and $\nu(|C^nZ\rangle) = n+1$ by Corollary 5.1.2. Since ν is a monotone, it is non-increasing under Clifford operations and measurements. This implies that at least $n+1$ $|T\rangle$ states are required to implement the $|C^nZ\rangle$ state and hence the C^nZ gate. Similarly, since $\nu(|CS\rangle) = 2$ and $\nu(|CCZ\rangle) = 3$, we get that to implement the C^nZ gate, we need at least $(n+1)/2$ $|CS\rangle$ states or $(n+1)/3$ $|CCZ\rangle$ states. □

The above lower bound can be improved when measurements are restricted.

Corollary 5.1.4. *We have the following dyadic monotone values:* $\mu_2(|T\rangle) = 1/2$, $\mu_2(|CS\rangle) = 1$, $\mu_2(|CCZ\rangle) = 1$, *and* $\mu_2(|C^n(z)\rangle) = n-1$.

Proof. The first three follow from direct calculation. For the $|C^nZ\rangle$ state, Proposition 5.1.1 gives us all of its possible values for the Pauli spectrum. Thus to get the dyadic monotone we simply input them into the valuation function to get a set of values, which we then negate, to finally take the maximum to get $n-1$ as desired. □

Lemma 5.1.5. *For* $n \geq 2$, *the* C^nZ *gate cannot be implemented with Clifford gates and measurements with probability* $1/2$ *using fewer than* $2n-2$ T *gates, or* $n-1$ CS *gates, or* $n-1$ CCZ *gates.*

Proof. We reason as in the proof of Proposition 5.1.3 but using the dyadic monotone which is also non-increasing under Clifford operations, but with measurements of probability $1/2$, as seen in 4.3.22. This time the values in Corollary 5.1.4 are used. □

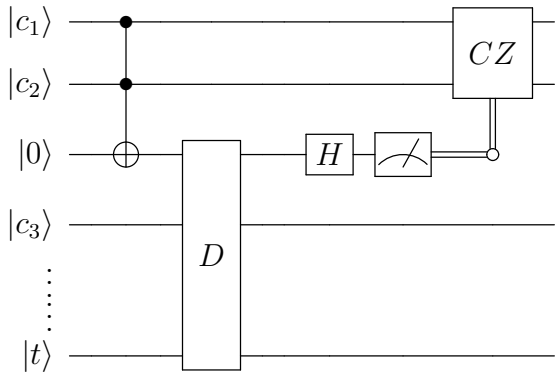
We now move on to upper bounds for the C^nZ gate. The next proposition provides reasoning as to why we do not need more than $n-1$ CCZ gates by showing a specific circuit construction.

Proposition 5.1.6. *Let* $n \in \mathbb{Z}_{\geq 2}$. *The* C^nZ *gate can be implemented using* $n-1$ CCZ *gates along with Clifford gates and measurements with probability* $1/2$.

Proof. In the proof, we use the CCZ and the CCX gates interchangeably because they are equivalent under a simple conjugation by a Hadamard gate. We reason by

induction on n. Consider the base case of $n = 2$. Then C^nZ is just the CCZ gate, so the result holds in this case.

Now for $n \geq 3$ assume we have a circuit D for $C^{n-1}Z$ which can be performed using $n-2$ CCZ gates. Then consider the following circuit:



Starting with the input state and tracking the state of this system step by step, we get the following:

$$
\begin{aligned}
& |c_1\rangle\,|c_2\rangle\,|0\rangle\,|c_3\rangle\cdots|c_{n-1}\rangle\,|t\rangle \\
\mapsto\ & |c_1\rangle\,|c_2\rangle\,|(c_1\cdot c_2)\rangle\,|c_3\rangle\cdots|c_{n-1}\rangle\,|t\rangle \\
\mapsto\ & |c_1\rangle\,|c_2\rangle\,|(c_1\cdot c_2)\rangle\,|c_3\rangle\cdots|c_{n-1}\rangle\,|t\oplus((c_1\cdot c_2)\cdot c_3\cdots c_{n-1})\rangle \\
=\ & |c_1\rangle\,|c_2\rangle\,|(c_1\cdot c_2)\rangle\,|c_3\rangle\cdots|c_{n-1}\rangle\,|t\oplus(c_1\cdots c_{n-1})\rangle.
\end{aligned}
$$

Now, before applying the Hadamard gate, write out the general states $|c_1\rangle$ and $|c_2\rangle$ as $\alpha_{c_1}|0\rangle + \beta_{c_1}|1\rangle$ and $\alpha_{c_2}|0\rangle + \beta_{c_2}|1\rangle$ respectively. Since we have already applied the D circuit, the only qubits left to consider are the first three, so we now ignore $|c_3\rangle\cdots|c_{n-1}\rangle\,|t\oplus(c_1\cdots c_{n-1})\rangle$ since it will remain unchanged. Thus, we now have:

$$
\begin{aligned}
& |c_1\rangle\,|c_2\rangle\,|(c_1\cdot c_2)\rangle \\
=\ & \alpha_{c_1}\alpha_{c_2}|000\rangle + \beta_{c_1}\alpha_{c_2}|100\rangle + \alpha_{c_2} + \alpha_{c_1}\beta_{c_2}|010\rangle + \beta_{c_1}\beta_{c_2}|111\rangle \\
\mapsto\ & \tfrac{1}{\sqrt{2}}(\alpha_{c_1}\alpha_{c_2}|000\rangle + \beta_{c_1}\alpha_{c_2}|100\rangle + \alpha_{c_1}\beta_{c_2}|010\rangle + \beta_{c_1}\beta_{c_2}|110\rangle) + \tfrac{1}{\sqrt{2}}(\alpha_{c_1}\alpha_{c_2}|001\rangle + \\
& \beta_{c_1}\alpha_{c_2}|101\rangle + \alpha_{c_1}\beta_{c_2}|011\rangle - \beta_{c_1}\beta_{c_2}|111\rangle) \\
\mapsto\ & \begin{cases} \big(\alpha_{c_1}\alpha_{c_2}|00\rangle + \beta_{c_1}\alpha_{c_2}|10\rangle + \alpha_{c_1}\beta_{c_2}|01\rangle + \beta_{c_1}\beta_{c_2}|11\rangle\big) & \text{if measurement is } |0\rangle, \\ \big(\alpha_{c_1}\alpha_{c_2}|00\rangle + \beta_{c_1}\alpha_{c_2}|10\rangle + \alpha_{c_1}\beta_{c_2}|01\rangle - \beta_{c_1}\beta_{c_2}|11\rangle\big) & \text{if measurement is } |1\rangle \end{cases}
\end{aligned}
$$

$\mapsto |c_1\rangle |c_2\rangle$.

Considering the rest of the qubits again, this gives us the output state of the system:

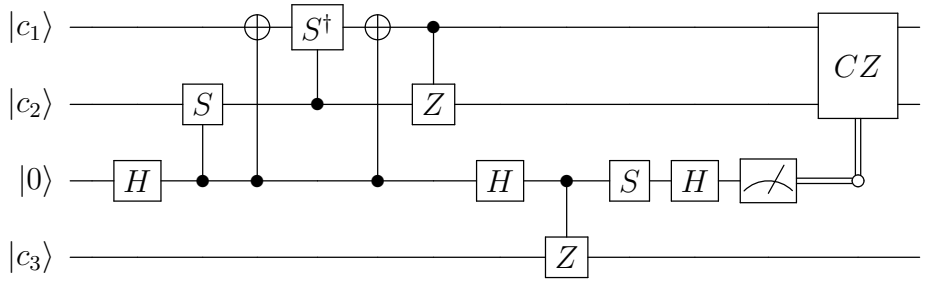
$$|c_1\rangle |c_2\rangle |c_3\rangle \cdots |c_{n-1}\rangle |t \oplus (c_1 \cdots c_{n-1})\rangle .$$

Hence, this circuit acts as the C^nZ gate. Note that the uncomputation of the added Toffoli gate follows from the circuit in Equation (2.1). □

We can also give upper-bounds similar to the ones in Proposition 5.1.6 for the CS and T gates.

Proposition 5.1.7. *The C^nZ gate can be implemented using exactly $2n-2$ CS gates along with Clifford gates and measurements with probability $1/2$.*

Proof. Simply put, we can implement the CCZ gate with a circuit using only two CS gates and then use this circuit to replace all the CCZ gates used in the circuit in proposition 5.1.6. The circuit for the CCZ gate using two CS gates is given below.

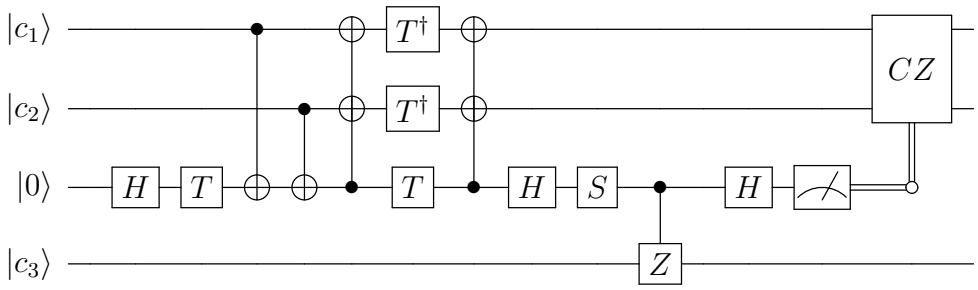


Thus, since we used $n-1$ CCZ gates in proposition 5.1.6, we can implement the $C^{n-1}Z$ gate with $2 \cdot (n-1)$ CS gates.

□

Proposition 5.1.8. *The C^nZ gate can be implemented using exactly $4n-4$ T gates along with Clifford gates and measurements with probability $1/2$.*

Proof. Simply put, we can write the CCZ gate with an equivalent circuit using four T gates and then use this circuit to replace all the CCZ gates used in the circuit in proposition 5.1.6. The circuit for the CCZ gate using four T gates is given below.



Again, since we used $n-1$ CCZ gates in proposition 5.1.6, we can implement the C^nZ gate with $4 \cdot (n-1)$ T gates.

□

5.2 The Modular Adder

In this final section, we provide lower bounds on circuits for the modular adder. The modular adder is an important part of many quantum algorithms.

Definition 5.2.1. A circuit A on 2^n qubits implements the modular adder if it acts on basis states as

$$A\,|i\rangle\,|j\rangle = |i\rangle\,|i+j\rangle$$

where $i+j$ is evaluated modulo 2^n.

Note that the adder defined in Definition 5.2.1 is an "in-place" adder: the result of the addition of the integers contained in the two input registers is stored in the second register. In order to establish bounds for the modular adder, we will rely on the so-called *Fourier states*. First, recall the definition of the Quantum Fourier Transform.

Definition 5.2.2. The *quantum Fourier transform* is an operator that maps the state $|a\rangle = \sum_{x=0}^{2^n-1} a_x\,|x\rangle$ to $|a'\rangle = \sum_{y=0}^{2^n-1} a'_y\,|y\rangle$ where $a'_y = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} a_x \omega_{2^n}^{xy}$ and $\omega_{2^n} = \exp(2\pi i/2^n)$.

Note that in Definition 5.2.2, we used ω_{2^n} for ζ_{2^n}, as is common in the quantum computing literature.

Definition 5.2.3. The quantum *Fourier state* is the quantum Fourier transform applied to a basis vector $|a\rangle$. This means that there is only one non-zero a_x, which we call a_ℓ. Hence, $a_\ell = 1$ necessarily, so that $|a\rangle = |\ell\rangle$. Thus we have the following:

$$|QFT_n^\ell\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} exp\Big[\frac{i2\pi\ell y}{2^n}\Big] |y\rangle \tag{5.1}$$

In fact, as explained in [13] we can rewrite this as:

$$|QFT_n^\ell\rangle = \otimes_{k=1}^n \frac{|0\rangle + e^{i2\pi\ell/2^k} |1\rangle}{\sqrt{2}},$$

which will be useful for the next Lemma.

Lemma 5.2.4. $\nu(|QFT_n^{-1}\rangle) = n - 2$.

Proof. We make use of the stabilizer nullity's additive property. Utilizing the above equality, we have that:

$$\begin{aligned}
\nu(|QFT_n^{-1}\rangle) &= \nu\left(\otimes_{k=1}^n \frac{|0\rangle + e^{-2\pi i/2^k} |1\rangle}{2^n} \right) \\
&= \sum_{k=1}^n \nu\left(\frac{|0\rangle + e^{-2\pi i/2^k} |1\rangle}{2^n} \right) \\
&= \nu\left(\frac{|0\rangle + e^{-\pi i} |1\rangle}{2^n} \right) + \nu\left(\frac{|0\rangle + e^{-2\pi i/4} |1\rangle}{2^n} \right) + \sum_{k=3}^n \nu\left(\frac{|0\rangle + e^{-2\pi i/2^k} |1\rangle}{2^n} \right) \\
&= \nu\left(\frac{|0\rangle + |1\rangle}{2^n} \right) + \nu\left(\frac{|0\rangle + (-i) |1\rangle}{2^n} \right) + \sum_{k=3}^n \nu\left(\frac{|0\rangle + e^{-2\pi i/2^k} |1\rangle}{2^n} \right)
\end{aligned}$$

Observe that both I and X stabilize $\frac{|0\rangle+|1\rangle}{2^n}$ and both I and $-Y$ stabilize $\frac{|0\rangle-i|1\rangle}{2^n}$, so the stabilizer nullity of both of these two terms is 0. Now consider $k \geq 3$. In this case, $e^{-2\pi i/2^k} \notin \mathbb{Q}[i]$. Because all entries of the Pauli matrices are in $\mathbb{Q}[i]$, it follows that $\frac{|0\rangle+e^{-2\pi i/2^k}|1\rangle}{2^n}$ has a trivial stabilizer, giving a stabilizer nullity value of 1. Thus $\nu\left(\frac{|0\rangle+e^{-2\pi i/2^k}|1\rangle}{2^n} \right) = 1$. Putting this all together we have $\nu(|QFT_n^{-1}\rangle) = \sum_{k=3}^n 1 = n - 2$. □

Proposition 5.2.5. *The modular adder cannot be implemented with Clifford gates and measurements using fewer than* $(n-2)\,|T\rangle$ *gates,* $(n-2)/2\,|CS\rangle$ *gates, or* $(n-2)/3\,|CCZ\rangle$ *gates.*

Proof. As in the previous section, we reason with states rather than with gates. Note that letting $\ell = 0$ in Definition 5.1, we get that $|QFT_n^0\rangle = |+\rangle^{\otimes n}$. Now consider applying the Adder circuit A to $|QFT_n^\ell\rangle\,|QFT_n^m\rangle$:

$$\begin{aligned} A\big(\,|QFT_n^\ell\rangle\,|QFT_n^m\rangle\,\big) &= A\Big(\sum_{y=0}^{2^n-1}\exp\Big[\frac{2\pi i(\ell y)}{2^n}\Big]\,|y\rangle\sum_{z=0}^{2^n-1}\exp\Big[\frac{2\pi i(mz)}{2^n}\Big]\,|z\rangle\,\Big) \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{z=0}^{2^n-1}\exp\Big[\frac{2\pi i(\ell y+mz)}{2^n}\Big]\,|y\rangle\,|z+y\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\exp\Big[\frac{2\pi i(\ell y+m(x-y))}{2^n}\Big]\,|y\rangle\,|x\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\exp\Big[\frac{2\pi i((\ell-m)y+mx)}{2^n}\Big]\,|y\rangle\,|x\rangle \\ &= |QFT_n^{\ell-m}\rangle\,|QFT_n^m\rangle \end{aligned} \tag{5.2}$$

By letting $\ell = 0$ we now have $A(|+\rangle^{\otimes n}\,|QFT_n^m\rangle) = |QFT_n^{-m}\rangle\,|QFT_n^m\rangle$. Now, suppose A is implemented with just Clifford gates, Pauli measurements, and some resource state $|\psi\rangle$. Then we can write $\nu(A(|+\rangle^{\otimes n}\,|QFT_n^m\rangle)) = \nu(|\psi\rangle\,|QFT_n^m\rangle)$, which implies that $\nu(|\psi\rangle\,|QFT_n^m\rangle) \geq \nu(|QFT_n^{-m}\rangle\,|QFT_n^m\rangle)$, and since the stabilizer nullity is additive over tensor products, we have that $\nu(|\psi\rangle) \geq \nu(|QFT_n^{-m}\rangle)$. Now letting $m = 1$ we can use Lemma 5.2.4 and Corollary 5.1.2 to get the lower bounds, reasoning as in Proposition 5.1.3. □

Finally, we give lower bounds using the dyadic monotone. To do this, we will need the dyadic monotone value of the Fourier state, given in the next Lemma.

Lemma 5.2.6. *Let a be an odd integer. Then $\mu_2\,|QFT_n^a\rangle = n - 3 + (1/2)^{n-2}$.*

Proof. Recall that from Example 4.2.8, the Pauli expectations of $(|0\rangle + e^{i2\pi a/2^k}\,|1\rangle)/\sqrt{2}$ are

$$\{0, \cos(2\pi a/2^k), \sin(2\pi a/2^k), 1\}.$$

Observe that $-v_2(0) = -\infty$ and $-v_2(1) = 0$, so for $k \geq 2$ we have:

$$\mu_2\big((|0\rangle + e^{i2\pi a/2^k}\,|1\rangle/\sqrt{2}\big) = -v_2\big(\sin(\pi a/2^{k-1})\big)$$

or

$$\mu_2\big((|0\rangle + e^{i2\pi a/2^k}|1\rangle/\sqrt{2}\big) = -v_2\big(\cos(\pi a/2^{k-1})\big)$$

Now, using the additive property of v_2, for odd a we can write

$$\begin{aligned} v_2\big(\sin(\pi a/2^{k-1})\big) &= v_2\big(2\sin(\pi a/2^{k-1})\big) + v_2(1/2) \\ &= v_2\big(\exp(i\pi a/2^{k-1}) - \exp(-i\pi a/2^{k-1})\big) - 1 \\ &= v_2\big(1 - \exp(i\pi a/2^{k-2})\big) - 1 \\ &= \frac{\bar{v}_2\big(N_{k-2}(1-\exp(i\pi a/2^{k-2}))\big)}{2^{k-2}} - 1 \\ &= \frac{\bar{v}_2(2)}{2^{k-2}} - 1 \\ &= 1/2^{k-2} - 1. \end{aligned}$$

Note we used the fact that $N_{k-2}(1-\exp(i\pi a/2^{k-2})) = 2$ which comes from Proposition 4.3.12. Furthermore, a similar calculation gives the same result for cosine, thus, using the multiplicative property of μ_2 we get:

$$\mu_2(|QFT_n^a\rangle) = \sum_{k=2}^{n} \big(1 - 1/2^{k-2}\big) = n - 3 + 1/2^{n-2}.$$

□

Proposition 5.2.7. *Let $n \geq 3$. The modular adder cannot be implemented with Clifford gates and measurements with probability $1/2$ using fewer than $(n-2)\,|CCZ\rangle$ gates.*

Proof. This proof follows similarly to the proof of Proposition 5.2.5, but with the dyadic monotone instead of the stabilizer nullity. Recall that if the adder circuit is implemented with Clifford gates, Pauli measurements, and some resource state $|\psi\rangle$, then we can write $\mu_2(|\psi\rangle\,|QFT_n^m\rangle) \geq \mu_2(|QFT_n^{-m}\rangle\,|QFT_n^m\rangle)$. Letting $m = 1$ and using the additive property of the dyadic monotone, we get that $\mu_2(|\psi\rangle) \geq \mu_2(|QFT_n^{-1}\rangle)$. Then by Lemma 5.2.6 $\mu_2(|\psi\rangle) \geq n - 3 + (1/2)^{n-2} \geq n - 2$. Finally, reasoning as in Proposition 5.1.3, the result follows by using the dyadic monotone value in Corollary 5.1.4.

□

Chapter 6

Conclusion

In this thesis, following the work of [4], we studied lower bounds on the number of non-Clifford gates in quantum circuits. The non-Clifford gates we focused on were the T gate, the CS gate, and the CCZ gate. After giving the fundamental tools required to define lower bounds, we explicitly demonstrated how to find lower bounds for certain protocols of interest. Moreover, upper bounds were also given to compare and contrast these lower bounds. The lower bounds discussed in this thesis required the use of monotonic functions: the stabilizer nullity and the dyadic monotone. The difference between these two approaches is apparent in the resulting lower bounds. Indeed, the stabilizer nullity yields looser bounds than the dyadic monotone. However, the stabilizer nullity is also subject to fewer restrictions in not needing measurement probabilities to be $1/2$ and is therefore more widely applicable.

There are many avenues for future work on this topic. Ideally for any circuit or gate, we would want the same lower bounds and upper bounds for the resource of interest, along with a circuit to represent such a bound. This would mean that we have the best circuit in terms of using the least amount of the expensive resources of interest. This is the case for the C^nZ gate, where the resource was the CCZ gate (and measurements are restricted to have probability $1/2$). It would be of great interest to have a construction matching the lower bound for other resources. It was recently shown in [5] that a $CCCZ$ gate can be implemented with less T gates than presented here, though this new construction does not yet match the lower bound. Another noteworthy question is deciding whether we can achieve the tighter lower bounds afforded by the dyadic monotone without the requirement of only using measurements with probability $1/2$.

Instead of lowering the upper bounds by providing improved circuit constructions, one could also try to improve the lower bounds. A possibility for doing this is considering another monotone. Since not all circuits or gates considered here had

the same lower and upper bounds, perhaps another monotone could result in tighter lower bounds so that we would know what the optimal number of required resources is. Of course, this is no trivial task, but one possible way to achieve this might be to make a slight modification to the definition of one of the monotones presented here. An example of this can be seen in [9], where the authors defined the stabilizer nullity on unitaries rather than states, calling it the unitary stabilizer nullity. Other monotones that are already known could also be explored, for example the stabilizer extent, introduced in [4].

Bibliography

[1] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70:052328, Nov 2004. Also available from `arXiv:quant-ph/0406196`.

[2] Matthew Amy and Michele Mosca. T-count optimization and Reed–Muller codes. *IEEE Transactions on Information Theory*, 65(8):4771–4784, Aug 2019. Also available from `arXiv:1601.07363`.

[3] Matthew Amy and Neil J. Ross. The phase/state duality in reversible circuit design. Available from `arXiv:2105.13410`, May 2021.

[4] Michael Beverland, Earl Campbell, Mark Howard, and Vadym Kliuchnikov. Lower bounds on the non-Clifford resources for quantum computations. *Quantum Science and Technology*, 5(3):035009, Jun 2020. Also available from `arXiv:1904.01124`.

[5] Craig Gidney and N. Cody Jones. A $CCCZ$ gate performed with 6 T gates. Available from `arXiv:2106.11513`, Jun 2021.

[6] Andrew N. Glaudell, Neil J. Ross, and Jacob M. Taylor. Optimal two-qubit circuits for universal fault-tolerant quantum computation. *npj Quantum Information*, 7:1–11, Jan 2020. Also available from `arXiv:2001.05997`.

[7] David Gosset, Vadym Kliuchnikov, Michele Mosca, and Vincent Russo. An algorithm for the T-count. *Quantum Information and Computation*, 14(15–16):1261–1276, November 2014. Also available from `arXiv:1308.4134`.

[8] Thomas Häner, Martin Roetteler, and Krysta M. Svore. Optimizing quantum circuits for arithmetic. Available from `arXiv:1805.12445`, May 2018.

[9] Jiaqing Jiang and Xin Wang. Lower bound the T-count via unitary stabilizer nullity. Available from `arXiv:2103.09999`, Mar 2021.

[10] Cody Jones. Low-overhead constructions for the fault-tolerant Toffoli gate. *Physical Review A*, 87(2):022328, Feb 2013. Also available from `arXiv:1212.5069`.

[11] Giulia Meuli, Mathias Soeken, Earl Campbell, Martin Roetteler, and Giovanni De Micheli. The role of multiplicative complexity in compiling low T-count oracle circuits. In *Proceedings of the International Conference on Computer-Aided Design, ICCAD 2019*, pages 1–8, Aug 2019. Also available from `arXiv:1908.01609`.

[12] G. Nebe, E. M. Rains, and N. J. A. Sloane. The invariants of the Clifford groups. *Designs, Codes and Cryptography*, 24, 2001. Also available from `arXiv:math/0001038`.

[13] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000.

[14] Neil J. Ross and Peter Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. *Quantum Information and Computation*, 16(11–12):901–953, 2016. Also available from `arXiv:1403.2975`.

[15] Peter Selinger. Efficient clifford+T approximation of single-qubit operators. *Quantum Information and Computation*, 15(1–2):159–180, January 2015. Also available from `arXiv:1212.6253`.

[16] Peter Selinger. Generators and relations for n-qubit Clifford operators. *Logical Methods in Computer Science*, 11(10):1–17, 2015. Also available from `arXiv:1310.6813`.

[17] Xin Wang, Mark M Wilde, and Yuan Su. Quantifying the magic of quantum channels. *New Journal of Physics*, 21(10):103002, Oct 2019. Also available from `arXiv:1903.04483`.