A Stabilizer Formalism for Infinitely Many Qubits

by

Xiangzhou Kong

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science (Quantum Information)

Waterloo, Ontario, Canada, 2023

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

Xiangzhou Kong was the sole author of this thesis, which was written under the supervision of Richard Cleve and were not written for publication.

Abstract

The study of infinite dimensional quantum systems has been an active area of discussion in quantum information theory, particularly in settings where certain properties are shown to be not attainable by any finite dimensional system (such as nonlocal correlations). Similarly, the notion of stabilizer states has yielded interesting developments in areas like error correction, efficient simulation of quantum systems and its relation to graph states. However, the commonly used model of tensor products of finite dimensional Hilbert spaces is not sufficiently general to capture infinite dimensional stabilizer states. A more general framework quantum mechanical systems using C*-algebras has been instrumental in studying systems with an infinite number of discrete systems in quantum statistical mechanics and quantum field theory. We propose a framework in the C*-algebra model (specifically, the CAR algebra) for the stabilizer formalism that extends to infinitely many qubits. Importantly, the stabilizer states on the CAR algebra form a class of states that can attain unbounded entanglement and yet has a simple characterization through the group structure of its stabilizer. In this framework, we develop a theory for the states, operations and measurements needed to study open questions in quantum information.

Acknowledgements

Firstly, I would like to express my deepest thanks to my supervisor, Richard Cleve for his guidance, his generous support, and above all else, his patience. I thank him for all the knowledge he imparted upon me, as well as all the counsel and advice. I thank him for always being available to answer my questions, and all his effort that made this thesis possible.

Throughout my time here, several friends have greatly enriched my time. I thank Hannah Wong, Karanbir Kamboj, Taaha Mahdi, Eugene Lu for all of the time we spent together, and all that you've done to make my university experience memorable. I thank my group members Vahid Asadi, Randy Lin, and Tony Lau for their support and companionship.

I thank my professors that I had the pleasure of studying under throughout my years at Waterloo, through undergraduate and my master's degrees. The knowledge given to me by these people greatly improved by ability as a researcher. In particular, I thank Vern Paulsen, John Watrous, Debbie Leung, and Roger Melko.

I would like to thank William Slofstra and Shalev Ben-David for being on my thesis committee, for their helpful comments and revisions.

Dedication

To my parents.

Table of Contents

Chapter 1

Introduction

In the field of quantum information theory (QIT), we have long recognized that quantum mechanical systems can be described by states which are vectors in a Hilbert space $\mathcal{H}$ and observables represented by an algebra of operators contained in $B(\mathcal{H})$. In QIT, where we mainly focus on discrete systems with finite dimension, this model has served very well. More recently however, it has been shown in various settings that there exists kinds of quantum correlations which are testable and cannot be attained by a system consisting of finitely many qubits or qudits[5, 14, 17]. Rather, an infinite dimensional system and some infinitary amount of entanglement is required to achieve it.

In infinite dimensional systems, the Hilbert space model of quantum information begins to break down. When we only have a finite number of systems, we can take the tensor product of the Hilbert spaces of each system to get a Hilbert space for the joint state on all the systems. When we have an infinite number of systems, the Hilbert space that contains the infinite tensor product of all the systems is difficult to work with mathematically. A simpler version of the infinite tensor product exists, but does not produce a large enough space to capture the states that are pertinent. A different framework is required.

The replacement, also inspired by von Neumann's work, lies in operator algebras. Operator algebras are already intrinsic to QIT, as the operators can all be expressed by some matrix algebra, but the framework that von Neumann developed is more general than finite matrices. The model focuses on the structure of the set of allowable operators on the system, and represents them using C*-algebras. The C*-algebra model was used extensively in quantum field theory and quantum statistical mechanics [1] in the 70s. More recently, the model has been applied to QIT to study non-locality of C*-algebra model systems as well [4].

We will discuss the C*-algebra model of quantum systems using the CAR algebra, which is essentially an algebra of operators on infinitely many qubit systems. This model gives access to many exotic states but we will focus on a restricted set of states which have been fruitful avenues of research in the past.

In the Hilbert space model, there is a set of states called Stabilizer states [9]. These states are fairly simple in the sense of the Gottesman-Knill theorem, which states that stabilizers and a restricted number of operations can even be efficiently simulated classically. Yet, these states have rich structure, and exhibit quantum nature. Notably, the Bell state is an example of a stabilizer state.

We introduce a formalism for states on the CAR algebra which have stabilizer structure. In Chapter 2, we give an overview of the general C*-algebra model with associated definitions and useful theorems. We give two constructions of the CAR algebra which each provide insight on the structure of the algebra, and prove theorems about the CAR algebra that will be used in the remainder of the thesis. In Chapter 3, we define stabilizers on the CAR algebra as well as the allowable operations needed to study quantum information theory, including Clifford operations and a definition of the partial trace. In Chapter 4 we define a related class of states, called graph states, and briefly discuss how their relationship to stabilizer states changes in the infinite dimensional system.

Chapter 2

The C*-Circuit Model

Inspired by classical circuits, the quantum circuit model of computation is a model of computation consisting of a collection of basic operations and states that are required for computation in quantum information theory.

2.1 The Conventional Circuit Model

First, we briefly review the typical model used in quantum information.

2.1.1 States and Registers

In this model, we have a notion of *registers* which hold information, akin to a register in a computer processor. Some collection of registers holds a quantum *state*, and finally we have a notion of the possible operations we can perform on such states.

A *register* is composed of either an alphabet Σ of symbols encoding the state set of the register, or it is a tuple of other registers (a compound register).

If the register is a tuple, then the register is called a compound register. The alphabet of a compound register is the Cartesian product of the alphabet of each component register, and the symbols are the string concatenations of the symbols from each register.

The classical state of a register is the symbol that the particular register holds. For example, the alphabet may be the alphabet of 32-bit strings, and the *classical states* are the symbols of that alphabet, in this case any 32-bit word.

In some models, the register is not necessarily deterministic, rather the actual classical state is random. This is simply called a classical probabilistic state, and the register holds a probability distribution p on the possible classical states (symbols) of a register rather than a single symbol. The probability that the register holds a classical state a is given by $p(a)$.

To each register, we can associate with it a vector space, equipped with a norm.

Definition 2.1.1. *An inner product space is a vector space V over a field $\mathbb{F}$, and an inner product map $\langle \cdot, \cdot \rangle$, where the inner product satisfies*

1. $\langle x, y \rangle = \overline{\langle x, y \rangle}$ *for all $x, y \in V$, where the $\overline{\alpha}$ denotes conjugation*
2. $\langle \alpha x, y \rangle = \alpha \langle x, y \rangle$, *for all $x, y \in V$, and $\alpha \in \mathbb{F}$*
3. $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$, *for all $x, y, z \in V$*

A vector space is called Euclidean if the norm used is the Euclidean norm, given by the inner product

$$||u|| = \sqrt{u \cdot u}$$

Given a norm, there is a natural distance function between vectors x, y in the vector space, given by $d(x, y) = ||u - v||$. If in addition to the properties of Definition 2.1.1 we have that the distance function is given as $d(x, y) = ||u - v||$, and every Cauchy sequence in V converges with respect to the norm, then the inner product space is also a Hilbert space.

For finite systems, it is sufficient to discuss Euclidean spaces, but is common and more general to consider a Hilbert space, also equipped with a Euclidean norm. Given a register X which has a finite alphabet Σ, the $\mathbb{C}^\Sigma$ denotes a complex vector space of dimension $|\Sigma|$. If the register $\mathsf{X} = (\mathsf{Y}_1, \mathsf{Y}_2, \dots)$ is compound, then the vector space associated with X is given by $\mathcal{X} = \mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \dots$, where each $\mathcal{Y}_i$ is the associated vector space for Y_i.

Whereas a classical state is represented by a simple probability distribution, a *quantum state* on a register is represented by a density operator. Given a Hilbert space or Euclidean space space $\mathcal{X}$, we can consider the bounded linear operators $B(\mathcal{X})$.

Definition 2.1.2. *Given two Hilbert spaces $\mathcal{X}$ and $\mathcal{Y}$, the norm $|| \cdot ||$ of a linear operator $T : \mathcal{X} \to \mathcal{Y}$ is given by*

$$||T|| = \sup\{||Tx||_{\mathcal{Y}} : x \in \mathcal{X}\}$$

Since T is linear, it is equivalent to restrict ourselves to $x \in \mathcal{X}, ||x||_{\mathcal{X}} = 1$.

Definition 2.1.3. *(Bounded Operators) Given a map $T : \mathcal{X} \to \mathcal{Y}$, T is called bounded if there exists M such that for all x, $||Tx|| \leq M||x||$. If $\mathcal{X}$ and $\mathcal{Y}$ are both finite dimensional vector spaces, then T is bounded if it is linear.*

Equivalently, T is bounded if $||T|| \leq \infty$

Definition 2.1.4. *(Trace) Let $\{e_i\}$ be an orthonormal basis for $\mathcal{X}$, then the trace of an operator $T : \mathcal{X} \to \mathcal{Y}$, denoted $tr(T)$, is given by*

$$tr(T) = \langle Te_i, e_i \rangle$$

Definition 2.1.5. *(Positive operators) An operator $T : \mathcal{X} \to \mathcal{X}$ is called positive if for all $x \in \mathcal{X}$, $\langle Tx|x \rangle \in \mathbb{R}$ and $\langle Tx|x \rangle \geq 0$. Positive operators are sometimes called positive-semidefinite or non-negative.*

Definition 2.1.6. *(Density operators) The density operators on $\mathcal{X}$ are the operators $\rho : \mathcal{X} \to \mathcal{X}$ which are positive semi-definite and have trace 1.*

The set of states on a conventional quantum register is the set of density operators on that register.

$D(\mathcal{X})$ is a convex set, so given some alphabet Γ, and a probability distribution $p(a)$ over $a \in \Gamma$, we can take a convex combination $\rho = \sum_a p(a)\rho_a$, and ρ is still a density operator. Previously, we mentioned that classical states are single symbols from the state set, or a probability distribution over the state set. A density operator can encode a single symbol when the density operator has only a single entry along the diagonal. A probabilistic mixture of such density operators represents a probabilistic classical state, which is given by a diagonal density matrix. Thus, the notion of a density matrix generalizes the notion of classical and probabilistic states on the register.

If the register X is a compound register, then the quantum states are density matrices from $D(\mathcal{Y}_1, \mathcal{Y}_2, \dots)$. It is not generally true that the states can be decomposed into the form $\rho = \rho_1 \otimes \rho_2 \otimes \dots$ where each $\rho_i \in \mathcal{Y}_i$, but in this special case, ρ is called a product state.

2.1.2 Dynamics

In the context of quantum information, we are interested in studying the dynamics of a quantum mechanical system, and leverage it to perform operations that will do computation. We need to have a model for the evolution of states, as well as the allowable operations.

The most general operations on quantum states are given by channels.

Definition 2.1.7. *(Completely Positive) A map $\Phi : B(\mathcal{X}) \to B(\mathcal{Y})$ is completely positive if for every Hilbert space $\mathcal{Z}$ the map $\Phi \otimes I : \mathcal{X} \otimes \mathcal{Z} \to \mathcal{Y}$, is positive.*

Definition 2.1.8. *(Quantum Channels) A linear map $\Phi : B(\mathcal{X}) \to B(\mathcal{Y})$ is called a quantum channel if it satisfies the following:*

1. *Φ is completely positive*

2. *Φ preserves the trace*

A specific example of channels we will focus on is given by the form $\Phi(\rho) = U\rho U^*$, where $U \in B(\mathcal{X})$ is unitary. These are sometimes called unitary channels, and represent the reversible operations on the register.

If the state set of the registers we work in are binary, then an operation is called *local* if it applies only to one particular bit position, and is identity on the remaining positions.

In 2 dimensions, each unitary is decomposable into a linear combination of the Pauli matrices, where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

In the circuit model, we typically only care about reversible operations and measurements.

Definition 2.1.9. *(Observables) An* observable *is a Hermitian operator O which represents a physical quantity that can be measured. The possible values that are measurement outcomes of O are its eigenvalues, with the state attaining a particular eigenvalue is the corresponding eigenvector.*

Each observable can be decomposed via the spectral decomposition into a linear combination of projectors that project an input onto one of the eigenvalues of the observable. We can view a state as being in an ensemble of the eigenvalues of a particular observable, where a measurement gives you a random outcome according to probabilities given by the ensemble. The notion of a POVM formalizes this notion.

Definition 2.1.10. *(POVMs) A positive operator valued measure (POVM) is a set of positive operators $\{P_i\}$ that sum to the identity operator. The operator P_i encapsulates the operation of measurement. Given a density matrix ρ, the probability of obtaining outcome i is given by $tr(P_i\rho)$.*

When every P_i is a projector (meaning $(P_i)^2 = P_i$) then this is also called a projector valued measure (PVM).

2.2 Limitations of the Conventional Model

The above definitions are sufficient for a discussion of many topics in quantum information, but it remains limited in some special cases. We can try to extend the typical notion of a register to hold one out of infinitely many states, that is, make the alphabet Σ a countably infinite set. This is possible if we choose an appropriate Hilbert space, but a finite dimensional space is no longer sufficient.

The trace operation is extended to infinite dimensional spaces. Given an orthonormal basis $\{e_k\}_{k\in\mathbb{N}}$, the trace of an operator A is defined as $\operatorname{tr} A = \sum_k \langle Ae_k | e_k \rangle$. Since the trace is a sum of non-negative real numbers, the trace is non-negative, or infinity. The operators with trace that does not diverge is called trace class. However, not every object we might want to represent is trace class.

For example, let $\Sigma = \mathbb{N}$, we can take $\mathcal{X} = \ell^2(\mathbb{N})$. The bounded operators on $\ell^2(\mathbb{N})$ are certainly not all trace class. Furthermore, it is necessarily the case that for a positive semi-definite operator to be trace class, the limit of the eigenvalues are vanishingly small. That is, for every ϵ there is an eigenvalue λ with $|\lambda| < \epsilon$. In the example of a diagonal density operator, the entries must tend to zero.

Currently, we assume that if X is a compound register, we expect that it is composed of finitely many other registers. We can extend this construction to allow compound registers formed from infinitely many registers, but we will see that we cannot include all the possible states that we might expect to have.

The state overall state on the joint spaces spanned by all of the systems is described by taking the Hilbert space tensor product of the Hilbert spaces of the individual systems. When we have a sequence Hilbert spaces, the construction of the infinite tensor product of all of the Hilbert spaces becomes fairly involved. The construction was studied fairly deeply by von Neumann [19], who actually showed that there are two kinds of infinite tensor products, the “complete” and “incomplete” tensor products[1]. The complete tensor product is non-separable and unwieldy so it rarely shows up in the literature. The incomplete tensor product is easy to work with, but does not capture states which are pertinent to a full discussion of quantum information theory.

Definition 2.2.1. *(Incomplete Tensor Product) Let $\mathcal{Y}_k, k \in \mathbb{N}$ be a family of finite dimensional Hilbert spaces. In each $\mathcal{Y}_k$ we choose a unit vector u_k. Let $(v_k)_{k\in\mathbb{N}}$ be a sequence of vectors where for all but finitely many k, we have $v_k = u_k$.*

We assign every such sequence to a basis vector $e_{(v_k)}$. We equip our space with the inner product $\langle e_{(v_k)}, e_{(w_k)}\rangle = \prod_k \langle v_k, w_k\rangle$ and the norm to be the Euclidean norm. The basis vectors form a vector space $\mathcal{V}$. Since all but finitely many indices k will have $\langle v_k, w_k\rangle = 1$, this norm is well defined.

The infinite tensor product of the Hilbert spaces,

$$\mathcal{X} = \bigotimes_{k}^{\infty} \mathcal{Y}_k$$

is given by the completion of $\mathcal{V}$ with respect to this norm.

It is not difficult to see that if we actually only have finitely many component registers, then this definition reduces to the usual definition of a tensor product of finitely many Hilbert spaces. For countably many registers this leads to a new construction, but typically, many interesting states will be missing.

For instance, if every $\mathcal{Y}_k$ is chosen to be $\mathbb{C}^2$, and for convenience, assume each u_k is the same vector, for example $u_k = |0\rangle$. We can then construct $\mathcal{H} = \bigotimes_k \mathcal{Y}_k$ using the above definition.

In this Hilbert space, we have vectors which are infinite tensor products of a sequence of vectors from $\mathbb{C}^2$. Since the basic vectors we start with only includes vectors in the linear span of sequences ending in $|0\rangle$, the only vectors we have are Cauchy sequences of vectors where all but finitely many positions are $|0\rangle$.

Roughly speaking, this means that the state in position k have to tend towards u_k in inner product. To illustrate what this means, suppose we have $|v\rangle = |v_1\rangle \otimes |v_2\rangle \otimes |v_3\rangle \otimes \dots$ where each v_k is a pure state in $\mathbb{C}^2$. This is the form of a general product state. We are

[1] The *incomplete* term is a bit of a misnomer. Both types are complete with respect to the norm, and the name incomplete instead refers to the fact that not every sequence of vectors from the Hilbert spaces is included in the incomplete space.

interested in what conditions we need to impose to be able to claim that $|v\rangle$ is really in the Hilbert space.

Suppose we take the sequence of vectors where the n-th term is

$$|x_n\rangle \equiv |v_1\rangle \otimes |v_2\rangle \dots |v_n\rangle \otimes |0\rangle \otimes \dots$$

as in we truncate all but the first n factors in the tensor product, and the remaining ones are just $|0\rangle$. Clearly this sequence converges to $|v\rangle$, and each $|x_n\rangle$ a basic vector before we take the completion. Thus, $|v\rangle$ is in the Hilbert space if and only if this sequence is Cauchy with respect to the inner product. If we compute the distances $|x_n - x_m|$, we obtain the following:

$$\begin{aligned} |x_n - x_m| &= \left| |v_1\rangle \otimes \dots \otimes |v_n\rangle \otimes (|v_{n+1}\rangle \otimes |v_{n+2}\rangle \otimes \dots \otimes |v_m\rangle - |0\rangle^{\otimes(m-n)}) \otimes |0\rangle \otimes \dots \right| \\ &= \left| |v_{n+1}\rangle \otimes |v_{n+2}\rangle \otimes \dots \otimes |v_m\rangle - |0\rangle^{\otimes(m-n)} \right| \\ &= 1 + 1 - \prod_{i=n+1}^{m} \langle 0|v_k\rangle - \prod_{i=n+1}^{m} \langle v_k|0\rangle \end{aligned}$$

We must be able to make the distance $|x_n - x_m|$ arbitrarily small only by increasing n, m, so the two products should both approach 1. This implies that the terms in the individual terms $|\langle 0, v_k\rangle|$ should not be too far from 1. Specifically, the condition is

$$\sum_i |\langle v_i|0\rangle - 1| < \infty$$

We can make a similar argument for non product states, as well as mixed states. In those cases, we obtain a similar condition where essentially the state must tend towards $|0\rangle$.

This means that a state such as $|1\rangle^{\otimes\infty}$ where the state at position i clearly does not tend towards $|0\rangle$ cannot be in this Hilbert space, since it is not the limit of any Cauchy sequence.

Still, this presents some useful ideas that we can use. We will see in the next section how these are addressed.

2.3 C*-Circuit Model

In the C*-circuit model, we represent quantum registers by making use of different mathematical object than the Hilbert space. This allows us to represent registers with structure that we like to exploit. Specifically, we use C*-algebras.

Definition 2.3.1. *(C*-Algebras) Let A be an associative algebra with an operation $* : A \to A$. Suppose that the $*$ operation satisfies the following conditions for all $x, y \in A$, $\lambda \in \mathbb{C}$*

1. $x^{**} = (x^*)^* = x$
2. $(x + y)* = x^* + y^*$
3. $(xy)^* = y^* x^*$
4. $(\lambda x)* = \bar{\lambda} x^*$

These conditions make A a $*$-algebra. In addition, if A is equipped with a norm $|| \cdot ||$ satisfying

1. *A is complete with respect to the metric induced by $|| \cdot ||$.*
2. *$||xy|| = ||x|| \cdot ||y||$ for all $x, y \in A$.*
3. *$||x^* x|| = ||x|| \cdot ||x^*||$ or equivalently, $||xx^*|| = ||x||^2$.*

then A is a $C*$-algebra. A $*$-algebra with the first two of the above conditions makes A a Banach algebra, and with all three, make it a C-algebra. The last condition is also known as the C*-condition.*

The above definition gives a characterization of a C*-algebra. Any abstract algebra that satisfies those conditions is a C*-algebra, but we can also have explicit constructions of C*-algebras of operators, typically bounded operators acting on a concrete Hilbert space.

Definition 2.3.2. *Given a C*-algebra $\mathcal{A}$ and some Hilbert space $\mathcal{H}$, a $*$-homomorphism $\pi : \mathcal{A} \to B(\mathcal{H})$ is called a representation.*

A linear, multiplicative map $\pi : \mathcal{A} \to B(\mathcal{H})$ from the algebra to bounded operators on some Hilbert space is called a *representation* of $\mathcal{A}$. Although representations can be fairly arbitrary, a representation is called *faithful* if its kernel is trivial.

The Gelfand Naimark Segal construction[16] says that every C*-algebra has at least one faithful representation as bounded operators on a Hilbert space. Thus, it is common to say that a particular algebra is a C*-subalgebra of $B(\mathcal{H})$, for some Hilbert space $\mathcal{H}$, even if the C*-algebra itself is defined with abstract elements.

Definition 2.3.3. *Given a C*-algebra $\mathcal{A}$, $\mathcal{A}$ is called* unital *if it contains a multiplicative identity I.*

2.3.1 States on a C*-algebra

In its abstract form, the C*-circuit model doesn't require us to define a classical state set. Nor do we need to choose a particular basis for the states on our register. In the case of a C*-algebra model, we have *abstract* states which are linear functionals mapping elements of the C*-algebra to the complex numbers, that are positive and unital.

In this subsection, we will develop the necessary results to define quantum states on the C*-circuit model.

States on a C*-algebra are represented by functionals, which are maps that take elements of the algebra to the base field, in this case $\mathbb{C}$. The physical intuition here is that Hermitian elements of the algebra represent all the observables, and states represent the measurement outcomes of the observables.

A functional is positive if it maps positive operators to real, positive numbers.

Let $s(A)$ be a positive functional on the C*-algebra $\mathcal{A}$, $s : \mathcal{A} \to \mathbb{C}$.

Then $s^*(A) = \overline{s(A^*)}$ denotes its adjoint. s is Hermitian if $s = s^*$. For a (bounded) Hermitian linear functional, we have the following equivalent definition of norm, which is equivalent to the operator norm

$$||s|| = \sup\{s(H) : H = H^*, ||H|| \leq 1\}$$

That is, although the operator norm is the supremum over operators on the C*-algebra, taking the supremum over only the self-adjoint operators of the C*-algebra is sufficient.

As above, if a positive linear functional is a state if it is, in addition, unital. That is, if $s(I) = 1$. A positive linear functional is Hermitian (one can show this by considering $||A|| \cdot I \pm A$)

In the following, $\mathcal{A}$ is a unital C*-algebra.

Lemma 2.3.4. *Let s be a positive linear functional on $\mathcal{A}$, then*

$$|s(B^*A)|^2 \leq s(A^*A)s(B^*B)$$

Lemma 2.3.5. *Let $\mathcal{A}$ be a unital C*-algebra, and let $A \in \mathcal{A}, andsaastateonA.Thefollowingaretrue$*

If $\forall s, s(A) = 0$, then $A = 0$.

If $\forall s, s(A)$ is real, then $A = A^*$.

If $\forall s$, $s(A) \geq 0$, then $A \geq 0$.

If A is normal, then there exists s such that $|s(A)| = ||A||$.

Hermitian states are a lot like Hermitian operators, in the sense of the following lemma

Lemma 2.3.6. *Every bounded Hermitian functional can be expressed in the form of $s^+ - s^-$, where s^+, s^- are both positive linear functionals. Furthermore, $||s|| = ||s^+|| + ||s^-||$.*

As mentioned before, functionals essentially encode the measurement information of observables on the algebra. If we know the outcome of certain observables, we can uniquely determine the state.

In the last section of this chapter, we will look at a specific algebra that includes a basis for a countable number of qubits.

2.3.2 Reversible Dynamics on the C*-circuit model

We also need a model for the "gates" of the circuit. In the conventional model, we looked at channels as the basic operations on quantum states. In a circuit, the reversible operations are unitary channels. Mappings of the form:

$$\phi(\rho) = U\rho U^*$$

where U is a unitary operator is the form of all unitary operations. In infinite dimensions, requiring that all operations be unitary may be too restrictive. For instance, there are operations O and O^* such that $OO^* = I$, but $O^*O \neq I$. Such operations partially satisfy the unitary condition, but are not unitary themselves.

Definition 2.3.7. *A $*$-automorphism on a C*-algebra $\mathcal{A}$ is a map $u : \mathcal{A} \to \mathcal{A}$ such that*

1. *u is linear.*
2. *u is multiplicative, $u(a)u(b) = u(ab)$.*
3. *u preserves the $*$-operation, $u(a)^* = u(a^*)$.*
4. *u is a bijection.*

If the map is not bijective, then u is called an endomorphism. If the codomain is some other algebra, then u is an isomorphism. If the map is not bijective and the domain and codomain are not equal, then the map is called a homomorphism.

Since automorphisms are bijective, they are reversible.

We call an automorphism $\alpha : \mathcal{A} \to \mathcal{A}$ *inner* if it is of the form $\alpha(a) \mapsto UaU^*$, where U is a unitary element of $\mathcal{A}$. However, the set of *inner* automorphisms on $\mathcal{A}$ is usually not the same as the set of automorphisms on $\mathcal{A}$. For arbitrary Hilbert spaces, every $*$-automorphism from $B(\mathcal{H})$ to itself is inner[2] (see [16] for a proof), but this is not true for C*-algebras in general.

Thus, the reversible operations that we permit is the entire automorphism group of $\mathcal{A}$.

Given an automorphism α, the state s on the C*-algebra remain the same, but the operators evolve. The outcome of measuring a state after with an element $A \in \mathcal{A}$ after an automorphism is applied is given by measuring the evolved operator $\alpha(A)$ on the original state.

Equivalently, we can say that $s \mapsto s'$, where s' is defined as

$$s'(A) = s(\alpha(A))$$

[2] Technically, if the base field is $\mathbb{C}$, there is a simple $*$-automorphism that is not inner, which is the map $\varphi_\theta(A) \mapsto e^{i\theta}A$. However, since in quantum information, the global phase is not relevant, we can simply say that every $*$-automorphism on a seperable Hilbert space is some inner automorphism composed with the phase automorphism.

By the fact that the automorphism preserves multiplication, it must also map the identity to itself, so s' is unital. Automorphisms also preserve positivity, so s' is also positive, thus s' is a well defined state.

2.3.3 Tensor Products of C*-algebras

In the conventional model, we allowed ourselves to compose two registers X and Y by taking all the possible concatenations xy for $x \in \mathsf{X}$ and $y \in \mathsf{Y}$. The density matrices on the composition are the density matrices on the Hilbert space $\mathcal{X} \otimes \mathcal{Y}$.

We can do the same thing in the C*-algebra model. The tensor product of C*-algebras $\mathcal{A}$ and $\mathcal{B}$ is made up of tensor products of pairs of elements $A \in \mathcal{A}$ and $B \in \mathcal{B}$.

Definition 2.3.8. *(Algebraic Tensor Product) Given two C*-algebras $\mathcal{A}$ and $\mathcal{B}$, the algebraic tensor product of $\mathcal{A}$ and $\mathcal{B}$ is a vector space $\mathcal{A} \odot \mathcal{B}$, with a bilinear map $A \times B \to A \odot B$.*

Being bilinear, the map $\odot$ satisfies

1. $(a_1 + a_2) \odot b = a_1 \odot b + a_2 \odot b$ *for all* $a_1, a_2 \in \mathcal{A}, b \in \mathcal{B}$
2. $\lambda(a \odot b) = (\lambda a) \odot b = a \odot (\lambda b)$ *for all* $a \in \mathcal{A}$, $b \in \mathcal{B}$, $\lambda \in \mathbb{C}$

The algebraic tensor product is essentially equivalent to taking the concatenation of its factors A and B. The resulting algebra is not necessarily complete with respect to any norm satisfying the C*-property.

This definition is similar to the setting when $\mathcal{A}$ and $\mathcal{B}$ are Hilbert spaces. In that case, resulting vector space is also not generally complete. For Hilbert spaces, we choose a norm based on the inner product $\langle a \otimes b, c \otimes d \rangle_{\mathcal{A} \odot \mathcal{B}} = \langle a, c \rangle_{\mathcal{A}} \langle b, d \rangle_{\mathcal{B}}$, and take the completion with respect to this norm.

When $\mathcal{A}$ and $\mathcal{B}$ are C*-algebras, $\mathcal{A} \odot \mathcal{B}$ is a $*$-algebra we also need to choose a norm, and take the completion. However, there is usually more than one norm satisfying the C*-condition, which could be a good choice of norm. The following is a very natural candidate for a C*-norm on $A \odot B$. Given representations $\pi_1 : \mathcal{A} \to B(\mathcal{H}_1)$, and $\pi_2 : \mathcal{B} \to B(\mathcal{H}_2)$, we can choose the norm on $\mathcal{A} \odot \mathcal{B}$ to be

$$\left|\left| \sum_i A_i \odot B_i \right|\right| = \left|\left| \sum_i \pi_1(A_i) \otimes \pi_2(B_i) \right|\right|_{B(\mathcal{H}_1 \otimes \mathcal{H}_2)} \tag{2.1}$$

Where the norm is defined by mapping the algebra elements to operators on Hilbert spaces, then using the usual norm on the Hilbert space tensor product. This means that given a representation of the $*$-algebra as operators on a Hilbert space, the Hilbert space norm induces a norm on the $*$-algebra. One can still choose a number of representations π_1 and π_2, so we can choose the norm to be the largest norm given by any representation.

$$\left|\left|\sum_i A_i \odot B_i\right|\right| = \sup_{\pi_1,\pi_2}\left\{\left|\left|\sum_i \pi_1(A_i)\otimes\pi_2(B_i)\right|\right|_{B(\mathcal{H}_1\otimes\mathcal{H}_2)}\right\} \tag{2.2}$$

However, this is also not the only norm that is natural to consider. The norm in Equation 2.3 implies a spatial decomposition of operators, that every simple tensor $A_i \odot B_i$ has a representation as a tensor product $\pi_1(A)\otimes\pi_2(B)$. Another possible norm is to simply consider all possible representations of $\mathcal{A}\odot\mathcal{B}$ itself, and take the largest norm.

$$\left|\left|\sum_i A_i \odot B_i\right|\right| = \sup_{\pi}\left\{\left|\left|\sum_i \pi(A_i \odot B_i)\right|\right|_{B(\mathcal{H}_1\otimes\mathcal{H}_2)}\right\} \tag{2.3}$$

These two norms are called the *min* and *max* norm respectively, and they are the most relevant norms since these are the two norms that we know best how to describe. As implied by the name, every C* norm on $A\odot B$ has a value somewhere between the min and max norms. Since the norms are different in general, taking the completion with respect to the min and max norms will give different C*-algebras. The C*-algebra generated by taking the max norm completion of $A\odot B$ gives the max tensor product, denoted $\otimes_{max}$, and respectively, $\otimes_{min}$ for the min norm.

The specifics of the differences between the min and max tensor products of C*-algebras are out of the scope of this thesis. Instead, we will focus on special cases of algebras where the min and max tensor products are the same.

Definition 2.3.9. *A C*-algebra $\mathcal{A}$ is called* nuclear*, if for all C*-algebras $\mathcal{B}$, $\mathcal{A}\otimes_{min}\mathcal{B} = \mathcal{A}\otimes_{max}\mathcal{B}$.*

Specifically, any full matrix algebra is nuclear, because $M_n \otimes \mathcal{B}$ is related by a $*$-isomorphism to $M_n(\mathcal{A})$ (the matrix algebra of $n\times n$ size matrices which entries are elements of $\mathcal{A}$) which is a C*-algebra. Since any finite C*-algebra is a direct sum of full matrix algebras[3], any finite C*-algebra is also nuclear.

[3] This well known, but is actually a fairly deep theorem to prove. See [13]

2.4 The CAR Algebra Model

The CAR algebra is named by the acronym for Canonical Anticommutation Relations, which is a notion that comes from quantum mechanics. A fermionic quantum field has creation and annhilation operators that anticommute with each other, whereas bosonic fields have operators that commute. The CAR algebra is an abstract algebra representation of these relationships.

In the first part of this chapter, we highlighted some limitations of the ability of the conventional model to represent some states that would be useful to consider. One example was that in the Hilbert space of an infinite tensor products qubit Hilbert spaces, many states are “missing”. Once the representative vector from each qubit Hilbert space is fixed, you cannot take a infinite tensor product of arbitrary vectors from each component Hilbert space.

We will introduce an algebra that allows us to encode these states and more.

The CAR algebra has two equivalent definitions. One is significantly simpler to understand, and more intuitive to work with. The other is somewhat more abstract, but allows us to tease out some important properties of the algebra. In this section we will introduce both.

Taking the completion with respect to this norm yields a C*-algebra which is the CAR algebra.

2.4.1 CAR Algebra Construction

In this section, we will give two equivalent definitions of the CAR algebra. Both are useful to see in order to understand some of the properties of the CAR algebra.

Algebra Generated by CAR Relations

Let $\mathcal{H}$ be a Hilbert space, and α be a linear map $\alpha : \mathcal{H} \to B(\mathcal{H})$, mapping each vector in the Hilbert space to an operator. If it holds that for all $f, g \in \mathcal{H}$

$$\alpha(f)\alpha(g) + \alpha(g)\alpha(f) = 0 \tag{2.4}$$

$$\alpha(f)^*\alpha(g) + \alpha(g)\alpha(f)^* = \langle f, g \rangle I \tag{2.5}$$

$$\tag{2.6}$$

then α encodes an anticommutating relationship. The C*-algebra generated by the set $\{\alpha(f) : f \in \mathbb{H}\}$ is the CAR algebra.

We follow [6] for this section. To understand this definition a bit, first consider f and g are unit vectors, and let $f = g$. Then we have that $\alpha(f)^2 = 0$ and $\alpha(f)^*\alpha(f) + \alpha(f)\alpha(f)^* = I$. The second implies that

$$(\alpha(f)^*\alpha(f))^2 = \alpha(f)^*\alpha(f)$$

This implies that $\alpha(f)$ is a partial isometry. The operator $E(f) := \alpha(f)^*\alpha(f)$ is a projection, and $E^{\perp}(f) = \alpha(f)\alpha(f)^*$ The $E(f)$ and $E^{\perp}(f)$ defines the domain and range of $\alpha(f)$. We claim the following

Proposition 2.4.1. *The C*-algebra generated by the operator $C^*(\alpha(f))$ is isometric to M_2.*

Proof. This fact is made obvious if we make the association $E_{11} = E(f)$, $E_{12} = \alpha(f)^*$, $E_{21} = \alpha(f)$, and $E_{22} = E^{\perp}(f)$

It may be checked now that each multiplication $E_{ij}E_{kl}$ satisfies the relationships between 2×2 matrix elements $e_{ij}e_{kl}$. Here are some example calculations:

$$\begin{aligned} E_{11}E_{11} &= (E(f))^2 = E(f) \\ E_{11}E_{12} &= E(f)\alpha(f)^* \\ &= \alpha(f)^*\alpha(f)\alpha(f)^* \\ &= \alpha(f)^* = E_{12} \end{aligned}$$

□

Now consider $f \neq g$ and $\langle f, g \rangle = 0$. Note that $\alpha(f)$ and $\alpha(g)$ must anticommute. Computing the commutator $[\alpha(g), E(f)]$, we have

$$\begin{aligned} [\alpha(g), E(f)] &= \alpha(g)\alpha(f)^*\alpha(f) - \alpha(f)^*\alpha(f)\alpha(g) \\ &= \alpha(g)\alpha(f)^*\alpha(f) + \alpha(f)^*\alpha(g)\alpha(f) \\ &= (\alpha(g)\alpha(f)^* + \alpha(f)^*\alpha(g))\alpha(f) \\ &= \langle g, f \rangle \alpha(f) = 0 \end{aligned}$$

Via an extension of this calculation it is shown that $[E(g), E(f)] = 0$ as well.

Define the reflection $V_1 = I - 2E(f)$. Now let

$$E_{11}^{(2)} = E(g), E_{22}^{(2)} = E^{\perp}(g), E_{12}^{(2)} = V_1\alpha(g)^*, E_{21}^{(2)} = V_1\alpha(g)$$

We can again check that $E_{ij}^{(2)}$ satisfies the matrix element relationships. In addition, using the fact that $V_1\alpha(g)$ commutes with everything in $C^*(\alpha(f))$, we have that every $E_{ij}^{(2)}$ commutes with every E_{kl}, which we will henceforth denote as $E^{(1)}$. Thus, $C^*(V_1\alpha(g)) \cong M_2$, and $C^*(\alpha(f), V_1\alpha(g)) \cong M_4$.

If we fix an orthonormal basis $\{f_n : n = 1, 2, \dots\}$, and set

$$V_n = \prod_{i}^{n-1}(I - 2E(f_i))$$

and $V_0 = I$, we can define

$$E_{11}^{(n)} = E(f_n), E_{21}^{(n)} = V_n\alpha(f_n), E_{12}^{(n)} = V_n\alpha(f_n)^*, E_{22}^{(n)} = E^{\perp}(f_n)$$

It follows that the algebra $\mathcal{A}_n = C^*(\{\alpha(f_i) : 1 \leq i \leq n\})$ contains n of copies of M_2, and so its isomorphic to M_{2^n}. The full CAR algebra contains each $\mathcal{A}_n$ for all finite n, and it is clear that $\mathcal{A}$ the closed union of all $\mathcal{A}_n$.

$$\mathcal{A} = \overline{\bigcup_n \mathcal{A}_n}$$

This fact gives us a few notable properties of the CAR algebra. First, any algebra which is the closed union of a union of finite dimensional subalgbras is called Approximately Finite. Moreover, if we have that the sequence of $\mathcal{A}_{k_n}$ are all isomorphic to full matrix algebras, then the algebra is called Uniformly Hyperfinite (UHF).

In a sense, the CAR algebra is the closed union of the C*-algebra of operators on k qubits for all finite k. The following section will make this view more clear.

CAR algebra as a group C*-algebra

Another way think about the CAR algebra is as a C*-algebra generated by a group.

We start by considering the C*-algebra of a single qubit. If we consider a single qubit, the set of operators is simply the linear maps on the Hilbert space $\mathbb{C}^2$.

We can build the C*-algebra of operators for a qubit fairly easily, since the full matrix algebra M_2 is already a C*-algebra. However, we can generate the entire $M_2(\mathbb{C})$ using the Pauli operators X, Y and Z. The Pauli operators can also be defined (up to change in basis) by their commutation relationships and Hermiticity alone. Instead of defining the Pauli operators by their matrix representation, we can abstractly define the Pauli matrices as abstract mathematical objects, satisfying

$$X = X^*, Z = Z^*, Y = -iXZ$$

and

$$X^2 = Z^2 = Y^2 = I$$

The group generated by these elements includes X, Y, Z, but also $-I$ and iI. We can construct the group algebra by taking complex vectors indexed by X, Y, Z, representing linear combinations of X, Y, Z. The group element $-X$ is associated with the scalar multiple of X and (-1), i.e. $-X \equiv (-1) \cdot X$. If we take the norm of a linear combination to be the operator norm of the matrix with X, Y, Z taking their usual matrix definitions, this norm is a C*-norm. This algebra is already complete, and is equivalent to the matrix algebra $M_2(\mathbb{C})$.

At this point we introduce some notation.

Definition 2.4.2. *Let M be some 2×2 matrix, and a be a bit string (possibly countably infinite length). Let $a[i]$ denote the bit in the i-th position. The notation M^a denotes*

$$M^a \equiv \bigotimes_i M^{a[i]}$$

When i is an integer, M_i denotes

$$M_i \equiv \underbrace{I \otimes I \otimes I \otimes \ldots}_{i-1 \text{ times}} \otimes M \otimes I \otimes I \otimes \ldots$$

Suppose we are given 2 qubits instead, the algebra of operators is now generated by the matrices $R \otimes R$, where each $R \in \{I, X, Z, Y\}$. Moreover, we can encode R into two bits, where the first bit a is the exponent on X^a, the second is the exponent on Z^b, and associating $-Y = XZ$. For two qubits, we can enlarge a and b to be 2-bit strings, where $a = 01$ is understood to be $X^0 \otimes X^1$ for example. We can then generalize to n qubits, we can have a and b be n bit strings.

We can generalize further by letting the $*$-algebra be indexed by infinite sequences of Paulis, that ends in $I \otimes I \otimes \dots$. If we disregard the coefficients (since they will be done by scalar multiplication anyway) and associate $XZ = Y$, we can simply define the set $S = \{X^a Z^b : a, b \in \{0,1\}^*\}$. The $*$-algebra is the algebra of linear combinations of finitely many such sequences. The norm that we will use is similar to the single qubit case. If we have finitely many combinations, the terms must have all finite number of tensor factors which are not identity. Thus, the result is of the form $M \otimes I \otimes I \dots$, where M is an arbitrary 2^n dimensional matrix.

At this point, we should make the notation $I \otimes I \otimes \dots$ more formal. We can define the notation $\bar{I} \equiv I \otimes I \otimes \dots$. The operations associated with $\bar{I}$ can be defined with the following axioms:

Definition 2.4.3. *The notation $\bar{I}$ is used to denote $I \otimes I \otimes \dots$. In the CAR algebra, $\bar{I}$ itself is the identity element, but also it acts as a tensor component of some operators. IF A and B are 2^n-dimensional square matrices, and $\bar{I}$ follows the following rules*

1. $I \otimes \bar{I} = \bar{I}$
2. $(A \otimes \bar{I})(B \otimes \bar{I}) = (AB) \otimes \bar{I}$
3. $(\alpha A \otimes \bar{I}) + (\beta B \otimes \bar{I}) = (\alpha A + \beta B) \otimes \bar{I}$

When A and B are not the same dimension (1) may be combined with the other rules to pad one operator to the size of the larger operator.

Using these rules, we can formalize the operations on $\mathbb{C}G$.

It remains to choose a norm satisfying the C* condition. Since each operator in $\mathbb{C}G$ is a finite linear combination of operators where only finitely many components are non-identity. Operators in $\mathbb{C}G$ are of the form of $M \otimes I \otimes I \dots$, where M is some finite dimensional operator. Thus, we can define a norm using the norm of M, and $||M \otimes I \otimes I \dots|| = ||M||$. The C* condition is satisfied, since the spectral norm satisfies the C* condition.

The completion with respect to this norm gives us the CAR algebra.

2.4.2 States on the CAR Algebra

As a special case of the C*-algebra model, the states on the CAR algebra are the positive, unital, linear functionals as usual. Nevertheless, there are a few important classes of states which will be discussed in more detail. The CAR algebra allows us to define quantum states that we encounter in a typical discussion of quantum information. But more than that, we can generalize the states to infinite dimensions.

In this section, we will develop a framework that we will use to define states specifically on the CAR algebra.

A state is defined by its action on elements of the CAR algebra. Certain CAR algebra elements correspond to values with physical interpretations. For example, given a state s, $s(X_1)$ corresponds to measuring in the Pauli X in the 1 position.

To try to define a state, we start by considering states on the underlying $*$-algebra, which is the algebra of finite linear combinations of Pauli operators discussed in the previous section. The definition of a state is a positive, unital, linear functional, but the $*$-algebra does not come with a definition of positive, so we have to define one.

Definition 2.4.4. *($*$-closed subalgebra) Let $\mathcal{V}$ be a subalgebra of a C*-algebra, then $\mathcal{V}$ is called* $*$-closed *if the $*$ applied to every element in $\mathcal{V}$ is another element in $\mathcal{V}$*

Definition 2.4.5. *Let $\mathcal{A}$ be a C*-algebra, and $\mathcal{V}$ be a $*$-closed subalgebra. Let $\mathcal{A}^+$ denote the positive elements of the C*-algebra, the positive elements of $\mathcal{V}$ are the elements $\mathcal{V} \cap \mathcal{A}^+$.*

The $*$-algebra is clearly $*$-closed, and is a subalgebra, so the elements of the $*$-algebra which are positive are exactly the ones which are also positive in the C*-algebra.

Definition 2.4.6. *Given $\mathcal{V}$ a $*$-algebra with positivity, a state on $\mathcal{V}$ is a unital linear functional that maps positive elements to positive real numbers.*

We can define a linear functional on the $*$-algebra by defining its action on every tensor product of Paulis, and extending linearly. The elements $Z^a X^b$, where a and b are infinite binary strings each with finitely many 1s, forms a basis for the $*$-algebra, and so every element of the $*$-algebra is a finite linear combination of said operators.

It still remains to show that such a linear functional is positive, i.e. that it maps positive elements of the $*$-algebra to positive real numbers. To ensure that our linear functional is a state, we will scale every linear functional to be unital, so $s(I) = 1$. We also will show that a positive, linear functional on the $*$-algebra can be extended to a positive linear functional on the C*-completion of that $*$-algebra.

Lemma 2.4.7. *Let $\mathcal{A}$ be a C*-algebra, and $V \subseteq \mathcal{A}$ be a subspace closed under the $*$ operation. Let s be a linear functional on V, then s is positive if and only if $|s| = s(1)$. Specifically when s is also unital, s is positive when $|s| = 1$.*

Proof. The proof of this is adapted from a proof given in [13]

For the forward direction, let s be a positive linear functional, and A be an arbitrary element in the C*-algebra. We can choose a complex unit scalar α, so that $s(\alpha A) \geq 0$ is real and positive.

Let H be the real part of αA, then we have $||H|| \leq ||A||$, and also $H \leq ||H||I \leq ||A||I$. Thus, $s(||H||I - H) = ||A||s(I) - s(H) \geq 0$. Also, $|s(A)| = s(\alpha A)$.

Since s is positive, it is also Hermitian, so $s(\alpha A) = \overline{s(\alpha A)} = s(\alpha^* A^*)$. So $s(H) = s(\text{Re}(\alpha A)) = s((\alpha A + \alpha^* A^*)/2)$. Combined with the fact that $s(H) \leq ||H||s(I)$, we have $|s(A)| \leq ||H||s(I) \leq ||A||s(I)$. Which implies $||s|| \leq s(I)$.

For the backwards direction, assume that $|s| = s(I)$. Without loss of generality, we can assume that $s(I) = 1$ by normalizing.

Suppose A is positive, and $s(A) = a + bi$. It suffices to show that a is positive, and $b = 0$.

The spectrum of A is real and positive, so if we fix a small positive number s, we can make the spectrum of $(I - sA)$ to be normalized, $\text{sp}(I - sA) \subseteq [0, 1]$, and so that $||I - sA|| \leq 1$.

Since $1 \geq |s(I - sA)| = |1 - s(a + bi)| \geq 1 - sa$, and s is positive, this implies that a must be positive.

Let B_n be a family of operators with $B_n = A - (a - inb)I$. We have $||B_n||^2 = ||B_n^* B_n|| \leq ||A - aI||^2 + n^2 b^2$. On the other hand, $|s(B_n)|^2 = |s(A - aI + inbI)|^2 = |bi + inb|^2 = b^2(n^2 + 2n + 1)$. Using the fact that $|s(B_n)|^2 = ||B_n||^2$, we have $b^2(n^2 + 2n + 1) \leq ||A - aI||^2 + n^2 b^2$, which is only possible if $b = 0$. □

This lemma is a very useful characterization of positive functionals, which will be used in a few ways. From this lemma, each state lies on the surface of the unit ball of the space of bounded linear functionals. The set of all states is also a convex set. One other immediate consequence of the forward direction is the following lemma.

Lemma 2.4.8. *Let s be a linear functional that is positive and unital on a $*$-algebra, then s may be extended uniquely to its C*-completion.*

Proof. To show that s can be extended to the completion, we need to show that for every Cauchy sequence (A_i), the sequence $s(A_i)$ is also Cauchy.

Let (A_i) be a sequence in the $*$-algebra converging to A in the C*-completion of the $*$-algebra (for us, the CAR algebra). Then for every A_i, A_j in the sequence, we have that $|s(A_i) - s(A_j)| = |s(A_i - A_j)| \leq |A_i - A_j|$ by Lemma 2.4.7. For every ϵ, there exists an N such that for all $i, j > N$, we have $|A_i - A_j| < \epsilon$, and so we also have $|s(A_i) - s(A_j)| < \epsilon$. Thus, the sequence $(s(A_i))$ is Cauchy.

For every A in the completion of the $*$-algebra, we can choose a Cauchy sequence (A_i) with $\lim_{i\to\infty} A_i = A$, and define $s(A) = \lim_{i\to\infty} s(A_i)$. □

Using these lemmas, we can define a state by defining it on the Pauli basis, and then use Lemma 2.4.7 to determine if it is positive, and use Lemma 2.4.8 to extend it to a state on the entire CAR algebra. We will see some examples.

2.4.3 $*$-Automorphisms on the CAR Algebra

Once again, let $\mathcal{P}$ denote the set of infinite Pauli sequences, and $\mathbb{C}\mathcal{P}$ denote the $*$-algebra of finite linear combinations of $\mathcal{P}$ with complex coefficients. Recall also that $\mathbb{C}\mathcal{P}$ is made up of elements of the form of $M \otimes \bar{I}$, where M is some finite square matrix which has dimension power of 2. The completion of $\mathbb{C}\mathcal{P}$ with respect to the norm $|M \otimes \bar{I}| = |M|$ gives the CAR algebra.

The following theorem gives an important fact about $*$-automorphisms on $\mathbb{C}\mathcal{P}$ and the CAR algebra.

Theorem 2.4.9. *Let $\varphi : \mathbb{C}\mathcal{P} \to \mathbb{C}\mathcal{P}$ be a $*$-automorphism. There exists a unique extension $\tilde{\varphi} : CAR \to CAR$, which is a $*$-automorphism.*

Proof. We will show that the unique extension is the map $\tilde{\varphi}(A) = \lim_n \varphi(a_n)$, where $(a_n)_{n\in\mathbb{N}} \in \mathbb{C}\mathcal{P}$ is a sequence in the $*$-algebra converging to A.

Claim 1: If φ is a $*$-automorphism, then φ is uniformly continuous.

Proof of claim 1. We will prove this claim in 2 parts. First, we show that since φ is a $*$-automorphism, then $|\varphi(A)| \leq |A|$. Suppose for some scalar λ, $A + \lambda\bar{I}$ is invertible, then let B be its inverse.

$$\varphi(A+\lambda\bar{I}) = \varphi(A)+\lambda\varphi(\bar{I}) \tag{2.7}$$
$$= \varphi(A)+\lambda\bar{I} \tag{2.8}$$

We can then show that $\varphi(A)+\lambda\bar{I}$ is invertible, where its inverse is $\varphi(B)$.

$$(\varphi(A)+\lambda\bar{I})\varphi(B) = \varphi(A+\lambda\bar{I})\varphi(B) \tag{2.9}$$
$$= \varphi((A+\lambda\bar{I})B) \tag{2.10}$$
$$= \varphi(\bar{I}) \tag{2.11}$$
$$= \bar{I} \tag{2.12}$$

And respectively for the left inverse.

We have shown that if $A+\lambda\bar{I}$ is invertible, then so is $\varphi(A)+\lambda\bar{I}$. Conversely, if $\varphi(A)+\lambda\bar{I}$ is not invertible, then neither is $A+\lambda\bar{I}$, and so if λ is in the spectrum of $\varphi(A)$, then it is also in the spectrum of A. In other words, the spectrum of $\varphi(A)$ is a subset of the spectrum of A, so $|\varphi(A)| \leq |A|$.

Since φ is invertible, and its inverse is also a $*$-automorphism, then we can make the same argument and show that $|A| \leq |\varphi(A)|$, so we have $|\varphi(A)| = |A|$.

Let ϵ be an arbitrary positive real number, and let A, B be arbitrary elements of $\mathbb{C}\mathcal{P}$ with $|A-B| \leq \epsilon$. Then $|\varphi(A)-\varphi(B)| = |\varphi(A-B)| = |A-B| \leq \epsilon$. Thus, there exists a constant $\delta = \epsilon$ such that for arbitrary A, B, whenever $|\varphi(A)-\varphi(B)| \leq \epsilon$, then $|A-B| \leq \delta$. Thus, $\varphi(A)$ is uniformly continuous.

This concludes claim 1. □

Claim 2: $\tilde{\varphi}$ is well defined.

Proof of claim 2. By the definition of the CAR algebra, every $A \in$ CAR, there is a Cauchy sequence $(a_n)_{n\in\mathbb{N}}$ that converges to A and each A_i is in $\mathbb{C}\mathcal{P}$.

Since φ is uniformly bounded, it can be shown that if (a_n) is a Cauchy sequence, then $(\varphi(a_n))$ is also a Cauchy sequence.

Let $(A_i)_{i\in\mathbb{N}}$ be a Cauchy sequence, we want to show that the sequence $(\varphi(a_i))$ is also Cauchy. We need to show that for every ϵ, there exits some N such that for all $n, m > N$, we have $|\varphi(a_n) - \varphi(a_m)| \leq \epsilon$. However, we know that φ is uniformly continuous, so for every ϵ, there exists some δ such that for any i, j, whenever $|a_i - a_j| \leq \delta$ we have that $|\varphi(a_i) - \varphi(a_j)| \leq \epsilon$ also. Since (a_i) is Cauchy, given δ (which was obtained for fix ϵ), there exists N such that for all $i, j > N$, we have $|\varphi(a_i) - \varphi(a_j)| \leq \delta$, as required.

Thus, $\varphi(a_n)$ is a Cauchy sequence, and $\tilde{\varphi}(A) = \lim_n \varphi(a_n)$ converges to an element in the CAR algebra, so $\tilde{\varphi}$ is well defined. □

Claim 3: $\tilde{\varphi}$ is an extension, and $\tilde{\varphi}$ is unique

Proof of claim 3. $\tilde{\varphi}$ is an extension, because whenever $a \in \mathbb{C}\mathcal{P}$, we can take the constant sequence $a_n = a$, and clearly $a_n \to a$ and $\varphi(a_n) \to \varphi(A)$.

Whenever $\mathcal{X} \subseteq \mathcal{Y}$ is a dense subset, the extension of a linear map from $\mathcal{X}$ to $\mathcal{Y}$ is unique. □

Claim 4: $\tilde{\varphi}$ is a $*$-automorphism

Proof of claim 4. A $*$-automorphism has the following properties. Let $A, B \in \text{CAR}$, $\lambda \in \mathbb{C}$

1. $\tilde{\varphi}(A^*) = \tilde{\varphi}(A)^*$
2. $\tilde{\varphi}(\lambda_1 A + \lambda_2 B) = \lambda_1 \tilde{\varphi}(A) + \lambda_2 \tilde{\varphi}(B)$
3. $\tilde{\varphi}(AB) = \tilde{\varphi}(A)\tilde{\varphi}(B)$
4. $\tilde{\varphi}$ is bijective

For the first condition, using the fact that $a_n^* \to A^*$ if $a_n \to A$,

$$\begin{aligned}\tilde{\varphi}(A^*) &= \lim_n \varphi(a_n^*) \\ &= \lim_n \varphi(a_n)^* \\ &= (\lim_n \varphi(a_n))^* \\ &= \tilde{\varphi}(A)^*\end{aligned}$$

By linearity and multiplicativity of limits, the second and third condition is met.

Finally, $\tilde{\varphi}$ is bijective, since we can define a unique inverse $\tilde{\varphi}^{-1}(A) = \lim_n \varphi^{-1}(a_n)$

This proves that $\tilde{\varphi}$ is a $*$-automorphism. □

This ends the proof. □

Using the above theorem, it is sufficient to define the action of maps on Pauli elements, and extend linearly to the $*$-algebra. If the map is a automorphism on the $*$-algebra, then it is uniquely extendable to the CAR algebra. This will is particularly useful when defining stabilizers, since the majority of operations will happen on Pauli group elements.

2.4.4 Hyperfinite Property of the CAR Algebra

Recall from earlier that every finite algebra is of the form of a direct sum of full matrix algebras.

Let $\mathcal{A}_i$ be a family of finite dimensional C*-algebras where each $\mathcal{A}_i = M_{n_i}(\mathbb{C})$, a complex matrix algebra, and the family is connected via inclusions, that is $A_i \subseteq A_{i+1}$. The union of the the family of C*-algebras is a C*-algebra itself, upon taking the completion.

Definition 2.4.10. *If a C*-algebra $\mathcal{A}$ is unital and there exists a chain of unital C*-algebras $\mathcal{A}_0, \mathcal{A}_1, \ldots$ satisfying*

1. $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \cdots \subseteq \mathcal{A}$
2. *each $\mathcal{A}_k$ is isomorphic to $M_{n_k}(\mathbb{C})$ for some integer n_k*
3. $\mathcal{A} = \overline{\bigcup_{i \in \mathbb{N}} \mathcal{A}_i}$

then $\mathcal{A}$ is a uniformly hyperfinite algebra (UHF)

Specifically, by the construction of the CAR algebra in Section 2.4.1, one can see that the CAR algebra contains the matrix algebras $M_2(\mathbb{C})$, $M_4(\mathbb{C})$, and every $M_n(\mathbb{C})$ where n is a power of 2. Thus, the CAR algebra is a UHF algebra, and is commonly seen as the prototypical UHF algebra.

It is only a slight abuse of notation to view the CAR algebra as M_{2^∞}, the matrix algebra of infinite tensor products of $M_2(\mathbb{C})$.

Due to a line of work culminating in [2], UHFs are described as a special case of the more general class of nuclear C*-algebras. Being a UHF algebra, the CAR algebra in particular is nuclear, so we can take tensor products of the CAR algebra with any other C*-algebra $\mathcal{B}$, and referring to the completion of CAR$\otimes\mathcal{B}$ is unambiguous.

Since the CAR algebra is UHF, we also have CAR $\cong$ CAR $\otimes M_n(\mathbb{C})$ for any n which is a power of 2. Moreover, we have that CAR $\otimes$ CAR $\cong$ CAR. The easiest way to see this isomorphism is that the CAR algebra, being UHF, is a direct limit of matrix algebras M_n where n is a power of 2. Each matrix algebra M_n is a tensor product of $\log n$ tensor factors of M_2. We can instead associate the first $\log n$ tensor factors with the algebra M_n, and the first factor of the CAR algebra with the $(\log n) + 1$ tensor factor in the chain.

Similarly the algebra CAR $\otimes$ CAR can be viewed as associating the even position tensor factors with the first copy of the CAR algebra, and the odd with the second. Together forming a single copy of the CAR algebra once again.

Chapter 3

Stabilizer States

3.1 Review of the Stabilizer Formalism

In the conventional model, stabilizer states[9] are a class of states which are important in the theory of error correcting codes, and by the Gottesman-Knill theorem, is important to the study of classical simulation of quantum computing. We will study in this chapter an extension of conventional stabilizer groups into the CAR algebra.

Definition 3.1.1. *(Stabilizer Groups) The stabilizer group is a commuting subgroup of the Pauli group not containing $-I$.*

The stabilizer group $\mathcal{G}$ "stabilizes" a particular state $|\psi\rangle$ if for every $M \in \mathcal{G}$ we have $M|\psi\rangle = |\psi\rangle$. This leads to the following definition.

Definition 3.1.2. *(Stabilizer States) A stabilizer state is a state $|\psi\rangle$ for which there exists a stabilizer group $\mathcal{G}$ such that for all $M \in \mathcal{G}$, $M|\psi\rangle = |\psi\rangle$.*

For every such $\mathcal{G}$, $|\psi\rangle$ is said to be stabilized by $\mathcal{G}$

Next, we will define what is called the Clifford group. To do so, consider the Pauli group on n qubits, we denote this group $\mathcal{P}_n$.

The Clifford group of $\mathcal{P}_n$ can be defined in a few ways. Often, the Clifford group CL_n is defined to be the unitary normalizer of $\mathcal{P}_n$, i.e. viewing the Pauli group as a subset of $2^n \times 2^n$ matrices, the Clifford group are the $2^n \times 2^n$ unitary matrices that map Pauli group elements to other Pauli group elements.

$$\mathrm{CL}_n = \{u \in U_{2^n} | u\mathcal{P}_n u^* = \mathcal{P}_n\}$$

However, the Clifford group as defined is too large. For one, the center of this group are the elements of the form $U(1) \cdot I$, which is mathematically uninteresting because $U(1)$ represents a phase in the operators that always cancels out. Moreover, defining the Clifford group in this way gives an infinite group since $U(1)$ is already infinite.

A common resolution is to factor out the unphysical phase, and define the quotient group $\mathrm{CL}_n/U(1)$. This group is equivalent to the group generated by the operators H, S and CNOT, which are called the *Clifford gates.* From here on, we amend the definition of the Clifford group so that CL_n refers to the group with finite center.

Definition 3.1.3. *(The Clifford Group) The Clifford group, denoted CL_n, is the quotient group $\{u \in U_{2^n} | u\mathcal{P}_n u^* = \mathcal{P}_n\}/U(1)$, or equivalently, the group generated by the gates H, S and CNOT on n qubits.*

The Clifford Gates are these particular generators of the Clifford group. A Clifford Circuit is a circuit consisting of only clifford gates, aka an element of the Clifford Group.

Defined by its generators, it is clear that the group is finite, since the gates all square to the identity. With these definitions, we can give an alternate characterization of stabilizer states, starting with the following lemma.

Lemma 3.1.4. *Clifford circuits map commuting Paulis to commuting Paulis.*

Proof. Let A and B be tensor products of Paulis, and $[A, B] = 0$, and let $C \in \mathrm{CL}_n$ be a Clifford circuit. Then

$$\begin{aligned}
[CAC^*, CBC^*] &= CAC^*CBC^* - CBC^*CAC^* && (3.1)\\
&= CABC^* - CBAC^* && (3.2)\\
&= C[A, B]C^* && (3.3)\\
&= 0 && (3.4)
\end{aligned}$$

□

If $\mathcal{G}$ is an abelian subgroup of the Pauli group (for example, a stabilizer group), then the action of a Clifford circuit C is that the group $C\mathcal{G}C^*$ is also a stabilizer group. Suppose that $|\psi\rangle$ is a stabilizer state, we claim that $C|\psi\rangle$ is a stabilizer state, and if $\mathcal{G}$ stabilizes $|\psi\rangle$, then $C\mathcal{G}C^*$ stabilizes $C|\psi\rangle$.

Lemma 3.1.5. *Let $|\psi\rangle$ be a stabilizer state and $\mathcal{G}$ be a group that stabilizes it, and let $C \in CL_n$ be a Clifford circuit. Then $C\mathcal{G}C^*$ is the stabilizer subgroup of $C|\psi\rangle$.*

Proof. From the above lemma, we know that the group $C\mathcal{G}C^*$ is in the Pauli group, and it is abelian. It remains to show that for every $M \in \mathcal{G}$, CMC^* has a $+1$ eigenvalue which is $|\psi\rangle$.

Let $|\psi'\rangle = C|\psi\rangle$.

$$\begin{aligned} CMC^*|\psi'\rangle &= CMC^*C|\psi\rangle && (3.5)\\ &= CM|\psi\rangle && (3.6)\\ &= C|\psi\rangle && (3.7)\\ &= |\psi'\rangle && (3.8) \end{aligned}$$

As required. □

As a consequence of this lemma, we have a second, equivalent definition of stabilizer. Every state in Definition 3.1.2 can be obtained by applying a Clifford circuit to the state $|0\rangle^{\otimes n}$, and every Clifford circuit applied to the all 0 state has a stabilizer group obtained by conjugating the stabilizer group with the Clifford circuit.

So far, we have defined the states which have stabilizers, and the stabilizer group itself. We have not yet addressed the uniqueness of stabilizer groups. In the terms we have defined so far, if $\mathcal{G}$ is a group that stabilizes $|\psi\rangle$, then clearly any subgroup of $\mathcal{G}$ stabilizes $|\psi\rangle$. On the other hand, if $|\psi\rangle$ is stabilized by $\mathcal{G}_1$, and $|\phi\rangle$ is stabilized by $\mathcal{G}_2$, then both states are simultaneously stabilized by $\mathcal{G}_1 \cap \mathcal{G}_2$. In other words, it is not generally the case that a state $|\psi\rangle$ is stabilized by a unique subgroup $\mathcal{G}$, and it is also not the case that $\mathcal{G}$ only stabilizes one state. Still, we are interested in the case when this is true.

Definition 3.1.6. *Let $|\psi\rangle$ be a stabilizer state, and $\mathcal{G}$ be a stabilizer for $|\psi\rangle$. $\mathcal{G}$ is called maximal if every stabilizer of $|\psi\rangle$ is a subset of $\mathcal{G}$.*

Theorem 3.1.7. *The maximal stabilizer of a stabilizer state is unique.*

Proof. Suppose for contradiction that $\mathcal{G}_1$ and $\mathcal{G}_2$ are both maximal stabilizers of $|\psi\rangle$. Since they are maximal, they are not subsets of each other, so there exists $M_1 \in \mathbb{G}_1$ and $M_1 \notin \mathbb{G}_2$. But for every $M_2 \in \mathbb{G}_2$, we have $M_1M_2|\psi\rangle = M_2M_1|\psi\rangle = |\psi\rangle$, so M_1 commutes with everything in $\mathbb{G}_2$, so $\mathbb{G}_2$ cannot be maximal. □

Theorem 3.1.8. *If $\mathcal{G}$ is maximal, then the state that it stabilizes is unique.*

Finally, a common way of analyzing stabilizers is to encode them into binary form. The elements of the Pauli group can be uniquely decomposed into a pair of Pauli matrices with only X factors and another Z factors, since $X \cdot Z = Y$, up to a phase. We can encode any n-qubit Pauli into 2 n-bit strings and one coefficient for the phase, which is one of $\pm 1, \pm i$.

For example, consider the following generators on 4 qubits (omitting the $\otimes$ symbol).

$$\begin{matrix} X & I & I & I \\ I & X & I & I \\ I & I & X & X \\ I & I & Z & Z \end{matrix}$$

These can be encoded into the matrices

$$X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

The above encoding does not take into account the phases associated with each operator.

Since the stabilizer is a subgroup of a finite group, it must be finite, and so it must be generated by a finite number of Pauli elements. An entire stabilizer can be encoded via its generators, which can themselves be put into binary form. We can describe a stabilizer using a pair of matrices (X, Z) where each row is a pair of binary strings (s_x, s_y) which encodes two Pauli operators.

Furthermore, the elementwise addition of the vectors corresponds to group multiplication of Pauli group elements. The rows which are vectors in a binary linear space $\mathbb{F}_2^{2n}$, and the vector space structure encodes the group structure of the stabilizer. Specifically, if we have a group $\mathcal{G}$ with n generators encoded into vectors, then a Pauli operator M is in the group $\mathbb{G}$ if it is in the linear span of the binary representation of the generators. The binary vector encoding of the generators forms a basis for the binary vectors of all the group elements. This allows us to show some properties of stabilizers is given in the following lemmas.

Lemma 3.1.9. *If $A = (s_x, s_y)$ and $B = (s'_x, s'_z)$ are pairs of bit strings that represent two Pauli operators, then A and B commute if and only if $s_x \cdot s'_z + s_z \cdot s'_x = 0$, where $u \cdot v$ is the dot product in the space $\mathbb{F}_2^n$.*

Lemma 3.1.10. *In finite dimensions, a stabilizer group on n qubits is not extendable if it has n independent generators.*

In other words, the pair of matrices representing a stabilizer are both square. When the stabilizer is not extendable, the state that exists as the joint +1 eigenvector of every Pauli in the stabilizer is unique.

When we extend this logic to infinite stabilizers, we aim to show that some infinite analogue of the pair of matrices (X, Z) encodes an infinite stabilizer, which defines a particular state on the CAR algebra. In order for each row of the matrices to encode one Pauli operator in the CAR algebra, we allow the binary strings that forms each row to be infinite so that we have infinite width matrices $X = x_{ij}$.

3.2 Stabilizer States in the CAR algebra

In this section, we aim to bring the stabilizer formalism to the CAR algebra, and establish stabilizer states on infinitely many qubits.

First, we need to translate the components of the stabilizer formalism to the language of the CAR algebra. To do so, we have to make a few adjustments. The group structure of the stabilizer is simple to define in the CAR algebra. All the Pauli elements M can be mapped to an operator of the form $M \otimes \bar{I}$. In fact, through the map $M \mapsto M \otimes \bar{I}$, every n-qubit Pauli group is embeddable into the CAR algebra, so any stabilizer group can be embedded into the CAR algebra.

In the CAR algebra formalism, the definition of a stabilizer remains the same, a stabilizer on the CAR algebra is a subgroup of the infinite Pauli group. This definition is not novel, see [8] for example.

Still there are a few caveats. A stabilizer with finitely many generators is always extendable in the CAR algebra. The intuition is, to stabilize a unique state in conventional model, the stabilizer group is generated by n Paulis. In the infinite case, you cannot stabilize a unique state with finitely many generators.

Lemma 3.2.1. *A stabilizer group in the CAR algebra is extendable if it contains finitely many generators*

Proof. Using the matrix form to encode the generators, we obtain the tuple of matrices (X, Z) which have n rows and infinitely many columns. Since each row has finitely many 1's, we can choose some integer k which is the position of the last 1 in all the rows. A Pauli element which is padded with k 0's on both sides will be linearly independent and commuting with all other generators. □

This implies that even though stabilizers on n qubits for any n has an analogue in the CAR algebra, these are not all the stabilizer states possible. This is a direct consequence of the fact that a maximal stabilizer exists in the CAR algebra, given by the following generators.

$$\begin{array}{cccc} Z & I & I & I\dots \\ I & Z & I & I\dots \\ I & I & Z & I\dots \\ & & & \ddots \end{array}$$

These generate X^a where a is any finite weight binary string. The stabilizer above stabilizes the state $|0\rangle^{\otimes\infty}$.

In addition, even with infinitely many generators, there is still a distinction between maximal infinitely generated stabilizers and extendable infinitely generated stabilizers. A simple way to see this is to take any maximal stabilizer and remove any subset of the generators. The result is no longer maximal, but you may still be left with an infinite number of generators.

Even if we are given a maximal stabilizer on the CAR algebra, we still have the issue of defining the stabilizer *state*. The algebra elements themselves are not operators acting on a Hilbert space, and do not have eigenvalues, so while the stabilizer is well defined, so the definition of a stabilizer state cannot be directly extended to the CAR algebra. What is much more interesting than the stabilizer group itself is to consider the class of CAR algebra states which are stabilizer states.

Theorem 3.2.2. *Given a stabilizer group $\mathcal{G}$, define the following functional s.*

1. *If P is an element of the Pauli group, and $P \in \mathcal{G}$, then $s(P) = 1$.*

2. *If P is an element of the Pauli group and $-P \in \mathcal{G}$, then $s(P) = -1$.*

3. *For all other Pauli group elements, $s(P) = 0$*

Extend to the entire CAR algebra linearly.

Then s is a state on the CAR algebra.

Proof. Since the Pauli group elements form a basis for the $*$-algebra, the above defines a functional from the $*$-algebra to the complex numbers. We will argue first that s is a state on the $*$-algebra in the sense of Definition 2.4.6, and then argue that its extension to the C*-completion is also a state using Lemma 2.4.8.

Claim 1: s defined on the $*$-algebra is a state.

Proof of claim 1. Note that s is unital by definition, since I is always in the stabilizer, and $s(I) = 1$. Also by definition, s is linear. It remains to show that s is positive.

Lemma 2.4.7 states that s, defined on the $*$-algebra, is a state if and only if we have $|s| = s(I)$. Since s is unital, it suffices to show that $|s| = 1$.

The norm $|s|$ is given by

$$|s| = \sup\{|s(H)| : ||H|| = 1, \text{ is Hermitian }\}.$$

Where H is a Hermitian element of the $*$-algebra. We already have that $|s(I)| = 1$, so the norm is at least 1. We only need to show that $|s| \leq 1$, we will prove that $|s(H)|/||H|| \leq 1$. Since $|s(H)| = |\sum_i c_i s(P_i)|$ and $|s(P_i)| \leq 1$, we have $|s(H)| \leq |\sum_i c_i|$. It then suffices to show that $||H|| \geq |\sum_i c_i|$.

We can decompose H into a finite linear combination of Paulis, $H = \sum_i c_i P_i$, where each c_i is a real number since H is Hermitian. Since s is linear, we can equivalently take the supremum over all non-zero H, and divide $|s(H)|$ by the norm of H and maximize the value $|s(H)|/||H||$ instead. Note that, we can assume that in the linear combination, whenever $s(P_i) = 0$, then $c_i = 0$. By removing these terms, $|s(H)|$ does not change but $||H||$ decreases, so this only increases $|s(H)|/||H||$ and we take the supremum.

Therefore, without loss of generality, H is a linear combination of commuting Pauli operators. Next, we prove that whenever the P_i's pairwise commute, then the norm $||\sum_i c_i P_i|| \geq ||\sum_i c_i||$.

Every P_i must be of the form $p_i \otimes \bar{I}$ where $p_i \in \mathcal{P}_n$ is a finite Pauli operator for some n. Moreover, $||P_i|| = ||p_i \otimes \bar{I}|| = ||p_i||$, for the purposes of computing $||H||$ we can treat H as a linear combination of Paulis on finitely many qubits. We can compute $||H||$ by computing the operator norm of a finite matrix.

From the finite theory of stabilizers, the operators generate a stabilizer on n qubits, and there exists a state $|\psi\rangle$ which is the joint $+1$ eigenvector of every p_i, satisfying $p_i|\psi\rangle = |\psi\rangle$. Therefore, $\sum_i c_i p_i$ has an eigenvector $|\psi\rangle$ with eigenvalue $\sum_i c_i$. This proves that $||H|| \geq |\sum_i c_i p_i| = |\sum_i c_i|$.

Combined with the above fact that $|s(H)| \leq |\sum_i c_i|$ for all H, we have that $|s(H)|/||H|| \leq 1$, where equality is attained when $H = 1$, for example.

This proves that $|s| = 1$, and with the fact that s is linear and unital, proves that s is a state on the $*$-algebra.

□

Claim 2: The extension of 2 onto the CAR algebra is a state

Proof of claim 2. Lemma 2.4.8 gives us that s has a unique extension $\tilde{s}$ to the CAR algebra, given by $\tilde{s}(A) = \lim_{n\to\infty} s(a_n)$, where a_n is some Cauchy sequence in the $*$-algebra converging to A.

By definition s remains linear. Note that the sequence $(s(a_n))_{n\in\mathbb{N}}$ is Cauchy, so a Cauchy sequence of non-negative real numbers cannot converge to a negative number, so whenever A is positive, $\tilde{s}(A)$ is a positive real number. Finally, $\tilde{s}(I) = 1$, since $\tilde{s}$ agrees with $s(I)$ for elements in the $*$-algebra. □

Thus, s is a state on the CAR algebra. □

Definition 3.2.3. *A computational basis state is a state corresponding to the infinite bit string b, and represents the state $|b[1]\rangle|b[2]\rangle\ldots$, where $b[i]$ is the i-th bit of b. The state s_b is defined to be the state where $s_b(Z_i) = (-1)^{b[i]}$, and $s_b(X_i) = 0$ for all i, extended linearly.*

In addition, we can define states in the X basis ($|+\rangle, |-\rangle$ basis) in a similar way.

3.3 Mixed States

In the previous section, we showed that stabilizers give well defined states on the CAR algebra. In the conventional model we have states that exist on compound registers which are composed of multiple registers. It is sometimes necessary to consider what the state on one of those registers would be. In the conventional model, it is done using the partial trace. In this section, we will develop a framework for studying the partial trace in the CAR algebra.

In the conventional model, extendable stabilizer groups show up in areas such as error correction, where we are interested in stabilizing a *subspace* of the set of states, rather than one unique state. An extendable stabilizer group can be used instead to encode a mixture of multiple states.

From the definition of stabilizer state, we have for a Pauli operator P,

$$s = \begin{cases} s(P) = 1 & : P \in \mathcal{G} \\ s(P) = -1 & : -P \in \mathcal{G} \\ s(P) = 0 & : P \notin \mathcal{G} \end{cases}$$

This definition has an operational meaning as well.

We will give an example in the finite dimensional case. Suppose we have a stabilizer group that is extendable $\mathcal{G}$, and let $\mathcal{G}$ be generated by XX only. We can find all the pure states that are stabilized by XX, by imagining all the possible ways to extend $\mathcal{G}$ to a maximal stabilizer. After enumerating the finitely many extensions of $\mathcal{G}$, one can see that $\pm XI$ and $\pm ZZ$ generates the 4 unique states which has XX as one of its stabilizers.

If we choose XI, then the state is $|+\rangle|+\rangle$, and if the generator is $-XI$ the state is $|-\rangle|-\rangle$. If we choose ZZ, then the state is $(|00\rangle + |11\rangle)/\sqrt{2}$, and we get $(|01\rangle + |10\rangle)/\sqrt{2}$ if the generator is $-ZZ$.

The definition tells us that $s(\pm XI) = s(\pm ZZ) = 0$, but we can obtain an intuitive meaning from this. Suppose we choose an extension, say XI. It remains to decide what the sign of XI would be, either $+1$ or -1. Once we choose, the state becomes a pure state, and we should have $s(XI) = 1$, or -1. However, we can also take the probabilistic ensemble of the two, with probability $1/2$ assign $+1$ sign, and -1 otherwise.

If we assigned a $+$, we can call the state s_+, and s_- otherwise. With this definition, the overall state is $s = \frac{1}{2}s_+ + \frac{1}{2}s_-$, since the value of the state should be like the expected outcome. This gives us $s(XI) = s_+(XI) + s_-(XI) = 1 + (-1) = 0$, and $s(-XI) = s_+(-XI) + s_-(-XI) = -1 + 1 = 0$ as required. In addition, we also have $s(ZZ) = s(-ZZ) = 0$, since they are in neither the stabilizer group nor the extended stabilizer.

In finite dimensions, this analogy makes sense, since the state is just the expectation value of measuring an observable, we can take the mixture of $|+\rangle|+\rangle$ and $|-\rangle|-\rangle$ and compute the expectation values. The mixed state is $s(A) = \operatorname{tr} \rho A$, where we can choose $\rho = \frac{1}{2}(| + +\rangle\langle + + |) + \frac{1}{2}(| - -\rangle\langle - - |)$. Suppose we measure $s(XI)$, the first term gives us

$1/2$, but the second terms us $-1/2$, so this is as expected. If we instead measure $s(ZZ)$, both terms give us 0.

It should be noted that for any extension M of $\mathcal{G}$, we can define ρ as $\rho = \rho_+ + \rho_-$, where ρ_+ is the state stabilized by $\mathcal{G} \cup M$, and ρ_- is the state stabilized by $\mathcal{G} \cup -$. In the above example, we defined ρ by choosing $M = XI$, but ρ could equivalently be defined as $\rho = \frac{1}{4}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|) + \frac{1}{4}(|00\rangle - |11\rangle)(\langle 00| - \langle 11|)$. Expanding, we see that this is equivalent to the definition above.

Moreover, this analogy can be generalized to mixtures of more than 2 states. Suppose we need n extensions to make $\mathcal{G}$ maximal. We can choose any extension with n new generators, and randomly assign signs + or − to each one with probability 1/2 each.

We can also extend this analogy to the CAR algebra. If there are only a finite number n of generators required to make the stabilizer maximal, then we simply randomly assign a sign to each, and s is an equal mixture of all the 2^n possible resulting states. However, in the CAR algebra, we have the possibility of more exotic mixtures. For example, it could happen that we can add infinitely many operators to extend $\mathcal{G}$. Suppose the generators are

$$\begin{array}{cccccccc}
Z & I & I & I & I & I & I & I\ldots \\
I & I & Z & I & I & I & I & I\ldots \\
I & I & I & I & Z & I & I & I\ldots \\
I & I & I & I & I & I & Z & I\ldots \\
 & & & & & & & \ddots
\end{array}$$

Here, every even position is left open. We can extend this in a simple way, for example, with generators

$$\begin{array}{cccccccc}
I & Z & I & I & I & I & I & I\ldots \\
I & I & I & Z & I & I & I & I\ldots \\
I & I & I & I & I & Z & I & I\ldots \\
I & I & I & I & I & I & I & Z\ldots \\
 & & & & & & & \ddots
\end{array}$$

However, there are now infinitely many ways to choose the sign for each new generator. We now have a uniform probability density of states.

Another example is when we have no generators at all. If $\mathcal{G}$ is the trivial group, then $s(P) = 0$ except $s(I) = 1$, which amounts to the maximally mixed state. To see that, note that each Z_i is a possible extension to $\mathcal{G}$, and they all pairwise commute. Taking Z_i for all $i \in \mathbb{N}$ as the extensions, and randomly assigning the sign, we essentially randomly fix the bit i in each position, so s is the equal mixture over all infinite bit strings.

3.4 Partial Trace

If we are allowed mixed states, we can begin to define a partial trace.

Definition 3.4.1. *Given a stabilizer $\mathcal{G}$ and index set $F \subset \mathbb{N}$. Let $\mathcal{G}'$ be the set of all elements of S which are identity on all positions in $\mathcal{I}$. We then trim the elements of $\mathcal{G}'$, by taking each element and removing the factors of identity on the positions in F.*

The partial trace of the stabilizer state is defined as $\operatorname{tr}_{\mathcal{I}}(s) = s'$, where s' is the state of $\mathcal{G}'$.

Suppose we have the state $|0\rangle^{\otimes\infty}$ which has generators

$$\begin{array}{cccccccl}
Z & I & I & I & I & I & I & I\ldots \\
I & Z & I & I & I & I & I & I\ldots \\
I & I & Z & I & I & I & I & I\ldots \\
I & I & I & Z & I & I & I & I\ldots \\
I & I & I & I & Z & I & I & I\ldots \\
 & & & & & & & \ddots
\end{array}$$

If we trace out every even position, we need to first find the subgroup of the stabilizer group which has identity as all the tensor factors on the positions we want to trace out. Clearly, the elements in the group which are identity in the even positions are reachable by products of the above generators with Z's in only odd positions. The remaining group is generated by

$$\begin{array}{cccccccl}
Z & I & I & I & I & I & I & I\ldots \\
I & I & Z & I & I & I & I & I\ldots \\
I & I & I & I & Z & I & I & I\ldots \\
I & I & I & I & I & I & Z & I\ldots \\
 & & & & & & & \ddots
\end{array}$$

However, after trimming all the even positions (which contain identity only), we obtain once again.

$$\begin{array}{cccccccc}
Z & I & I & I & I & I & I & I\dots \\
I & Z & I & I & I & I & I & I\dots \\
I & I & Z & I & I & I & I & I\dots \\
I & I & I & Z & I & I & I & I\dots \\
I & I & I & I & Z & I & I & I\dots \\
 & & & & & & & \ddots
\end{array}$$

Which is a pure state, and is the state $|0\rangle^{\otimes\infty}$ which is what we expect.

Note that in general, $\mathcal{G}'$ is not going to be maximal, even if we disregard the positions of the index set. Not all states will be in a product state with respect to our partition. For example, consider $(|00\rangle + |11\rangle)/\sqrt{2} \otimes |0\rangle^{\otimes\infty}$, and trace out the second qubit. The stabilizer of this state can be defined by the generators

$$\begin{array}{cccccccc}
X & X & I & I & I & I & I & I\dots \\
Z & Z & I & I & I & I & I & I\dots \\
I & I & Z & I & I & I & I & I\dots \\
I & I & I & Z & I & I & I & I\dots \\
I & I & I & I & Z & I & I & I\dots \\
 & & & & & & & \ddots
\end{array}$$

The group of elements which are identity in the second position is generated by all the above generators, except the first two. The resulting group after trimming is generated by

$$\begin{array}{cccccccc}
I & Z & I & I & I & I & I & I\dots \\
I & I & Z & I & I & I & I & I\dots \\
I & I & I & Z & I & I & I & I\dots \\
I & I & I & I & Z & I & I & I\dots \\
 & & & & & & & \ddots
\end{array}$$

This state is now mixed, and can be extended, for example by $\pm ZII\dots$. So the result is a maximally mixed state in the first positions, and $|0\rangle$ in all other positions.

We can also take the partial traces where we trace out infinitely many positions. For example, consider a similar example where the state is an infinite tensor product of Bell pairs. Its generators can be the following:

$$\begin{array}{cccccccc}
X & X & I & I & I & I & I & I\ldots \\
Z & Z & I & I & I & I & I & I\ldots \\
I & I & X & X & I & I & I & I\ldots \\
I & I & Z & Z & X & X & I & I\ldots \\
I & I & I & I & Z & Z & I & I\ldots \\
 & & & & & & & \ddots
\end{array}$$

If one traces out every even position, you would obtain a maximally mixed state.

3.5 Operations on Stabilizer States

In the CAR algebra model, we are allowed to perform operations on states to transform them and use them for computation. In Section 3.1, we introduced Clifford gates, which are a set of quantum gates in the conventional gate model that transforms stabilizer states to other stabilizer states. We will define Clifford operations in the CAR algebra model.

In the CAR algebra model, allowable operations are $*$-automorphisms. If φ is a $*$-automorphism on the CAR algebra, then it transforms a state $s(A)$ into $s(\varphi(A))$. Following the spirit of the Clifford operations in the conventional model, we are interested in $*$-automorphisms φ where $s(\varphi(A))$ is a stabilizer state whenever $s(A)$ is a stabilizer state.

Specifically, φ applied to a Pauli group element should map it to another Pauli element.

Definition 3.5.1. *Let $\mathcal{P}$ denote the Pauli group of the CAR algebra. A $*$-automorphism $\varphi : CAR \to CAR$ with the property $\varphi(\mathcal{P}) = \mathcal{P}$ is a Clifford map.*

A remark is that given a group automorphism on the Pauli group, we can extend linearly to the $*$-algebra, and consequently we can give an extension into the CAR algebra through Theorem 2.4.9. A Clifford operation can be then defined as a $*$-automorphism on the Pauli group. Similarly, the restriction of a Clifford operation to the Pauli group is a $*$-automorphism.

Similar to the finite dimensional case in the conventional model, a Clifford operation φ maps commuting elements to commuting elements. This fact is true for all $*$-automorphisms, not just Clifford.

Lemma 3.5.2. *Let $\varphi : CAR \to CAR$ be a $*$-automorphism, and $A, B \in \mathcal{P}$ with $[A, B] = 0$, then $[\varphi(A), \varphi(B)] = 0$*

Proof.

$$\begin{aligned}
[\varphi(A), \varphi(B)] &= \varphi(A)\varphi(B) - \varphi(B)\varphi(A) \tag{3.9}\\
&= \varphi(AB - BA) \tag{3.10}\\
&= \varphi([A, B]) \tag{3.11}\\
&= \varphi(0) \tag{3.12}\\
&= 0. \tag{3.13}
\end{aligned}$$

□

If we have a stabilizer group $\mathcal{G}$, then a Clifford operation φ maps $\varphi(\mathcal{G})$ to a commuting subgroup of the Pauli group.

Every finite Clifford group CL_n can be embedded into the CAR algebra as a $*$-automorphism, specically an inner automorphism. Each element of CL_n for every n is a subset of the finite matrix algebra $M_{2^n}(\mathbb{C})$, which are all in the CAR algebra through the inclusion map $M \in M_{2^n}(\mathbb{C}) \mapsto M \otimes \bar{I}$. The elements $C \in \mathrm{CL}_n$ for all integers n forms a simple class of Clifford operations on stabilizers. Each element C is unitary, so the map $\varphi(A) = CAC^*$ is an inner automorphism on the CAR algebra.

These inner automorphisms form the basic building blocks of Clifford circuits.

In the CAR algebra, we can have outer automorphisms which are automorphisms that are not conjugation by a unitary from the CAR algebra. Clifford automorphisms can be outer automorphisms as well. For example, the map that takes an element X^a which is a tensor product of X's and I's only, and maps it to Z^a which is a tensor product with Z's to the same position cannot be inner. To see why this is the case, consider the following operators.

$$\begin{array}{cccccccc}
X & I & I & I & I & I & I & I\ldots \\
X & X & I & I & I & I & I & I\ldots \\
X & X & X & I & I & I & I & I\ldots \\
 & & & & & & & \ddots
\end{array}$$

We can map each of the elements in the sequence to Z's by conjugating by $H \otimes H \otimes H \otimes \ldots$. However this is not an element of the CAR algebra, so there is no inner automorphism that maps each of these elements to the following.

$$\begin{array}{cccccccc}
Z & I & I & I & I & I & I & I\ldots \\
I & Z & I & I & I & I & I & I\ldots \\
I & I & Z & I & I & I & I & I\ldots \\
 & & & & & & & \ddots
\end{array}$$

This automorphism turns out to still be a valid $*$-automorphism (see Chapter 5), but not an inner automorphism.

Aside from Clifford operations, we are also allowed to measure the value of any of the positions. Measurements can be done in the framework of PVMs from Definition 2.1.10, where the only allowable projectors are operators from the Pauli group.

Definition 3.5.3. *Given a stabilizer state with stabilizer $\mathcal{G}$ and a Pauli element M, the outcome of measuring M is the following:*

- *If $M \in \mathcal{G}$, then the result is deterministically $+1$, or -1 if $-M \in \mathcal{G}$*

- *Otherwise, the outcome is random with equal probability.*

After the measurement, we modify the stabilizer group $\mathcal{G}$ to a new stabilizer $\mathcal{G}'$ reprenting the remaining state after the measurement. If the outcome of the measurement is $+1$, we remove every element in $\mathcal{G}$ that does not commute with M (if any), and add M to the set of generators of $\mathcal{G}'$. Respectively, we add $-M$ if the outcome was -1.

Chapter 4

States and Graph States

In this section, we will dicuss a few frameworks in the C* circuit model that will allow us to perform computations.

4.1 Inner Automorphisms

Recall that $*$-automorphisms may be categorized as inner and outer. An inner automorphism is a map φ of the form $\varphi(A) = UAU^*$, where U is a unitary element of the CAR algebra. Immediately, this gives us some useful gates to use by creating a unitary map φ_U for any unitary element of the CAR algebra.

The CAR algebra includes elements of the form of tensor products of Pauli matrices and identity maps. For example, X_i denotes $i-1$ copies of identity, tensor a single Pauli X operation.

$$X_i \equiv \underbrace{I \otimes I \otimes I \otimes \ldots}_{i-1 \text{ times}} \otimes X \otimes I \otimes I \otimes \ldots$$

Similarly, we define Z_i and Y_i in the same way. More generally, if s is a infinite binary string with finitely many 1s, and M is a 2×2 matrix then M^s denotes a tensor product of the form

$$\bigotimes_i M_{s[i]}$$

Where $s[i]$ is the i-th bit of the string.

We can also make other operations acting on single positions, such as Hadamard operations. The Hadamard operator is a unitary element in the CAR algebra and is constructed as a linear combination $\frac{1}{\sqrt{2}}(X_i + Z_i)$. Other gates from the conventional model, such as the phase gate, T gate, can be replicated in the CAR algebra as inner automorphisms by making them from linear combinations of the Paulis.

In fact, since the $*$-algebra generated by n-fold tensor products of Pauli matrices generates the full matrix algebra M_{2^n}, we every n-qubit unitary gate from the conventional model can be constructed from finite linear combinations of CAR algebra elements. Moreover, all of these are inner automorphisms.

Through linear combinations, we can show that matrix elements are in the CAR algebra as well. We can the CNOT gate by building the unitary operator using matrix elements on 2 positions.

Let $E_{ij}^{(n)}$ denote a 2×2 matrix entry on the n-th position, with ij ranging between 1 and 2. For example, on any position i, $(\bar{I} + Z_i)/2 = E_{11}^{(i)}$, and $(\bar{I} - Z_i)/2 = E_{22}^{(i)}$. We can construct the CNOT gate by taking linear combinations of the form

$$E_{11}^{(i)} E_{11}^{(j)} + E_{22}^{(i)} E_{11}^{(j)} + E_{12}^{(i)} E_{22}^{(j)} + E_{21}^{(i)} E_{22}^{(j)}$$

Since these above gates form a universal gate set [15], we can perform universal quantum computation with this model with inner automorphisms alone.

4.2 Outer Automorphisms

An Outer Automorphism is one that cannot be made into the form of $\varphi(A) = UAU^*$, but is still an automorphism nonetheless. A basic example of such an automorphism is one where $\varphi(A) = e^{i\phi}A$. This example is not very interesting, since it is not physically significant to consider the global phase. Another example is the following.

Consider the family of automorphisms on the CAR algebra, $\varphi_{H_i}(A) = H_i A H_i$. Each of these are an inner automorphism. Suppose instead, we iteratively apply maps in a chain

$$A \xrightarrow{\varphi_{H_1}} A_1 \xrightarrow{\varphi_{H_2}} A_2 \xrightarrow{\varphi_{H_3}} A_3 \xrightarrow{\varphi_{H_4}} \dots$$

Clearly, the map that takes A to A_n for each finite n is a valid inner automorphism because any composition of finitely many automorphisms is itself an automorphism. We can show this to be inner by constructing the unitary element that gives the inner automorphism, which is $U_n = H_1 H_2 H_3 \dots H_n$. For all elements A of the CAR algebra, the map $A \mapsto A_n$ can be implemented by $U_n A U_n$

However, it is clear that $\prod_{i=0}^{\infty} H_i$ is not an element of the CAR algebra since $\lim_{n\to\infty} \prod_{i=0}^{n} H_i$ does not converge in the CAR algebra norm. It is also not immediately obvious that the result of applying H to every position, $\lim_{n\to\infty} A_n$, is well defined. But in fact, any sequence of single qubit operations applied to the positions is a $*$-automorphism.

To show it, we use the fact that $*$-automorphism on $\mathbb{C}P$ extends to a $*$-automorphism on the CAR algebra.

Theorem 4.2.1. *Let (M_i) be a sequence of 2×2 unitary operators acting on the i-th position. The sequence of maps*

$$\begin{tikzcd} A \arrow[r, "\varphi_{M_1}"] & A_1 \arrow[r, "\varphi_{M_2}"] & A_2 \arrow[r, "\varphi_{M_3}"] & A_3 \arrow[r, "\varphi_{H_4}"] & \dots \end{tikzcd}$$

converges for every element in the CAR algebra.

Proof. It suffices to show that it converges for every element in the $*$-algebra $\mathbb{C}P$, then using Theorem 2.4.9, extend the map to the entire CAR algebra.

Note that every element in the $*$-algebra is of the form $M \otimes \bar{I}$, where M is a finite dimensional matrix. There exist some positive integer k where the element is only "active" on the first k positions. Thus, for some k, every map M_i with $i > k$ has no effect on the input state and acts as the identity map.

For a fixed element in the $*$-algebra, the sequence of the maps converges to applying only the first k elements.

This map is linear and multiplicative, since for A and B in the $*$-algebra, we can find the max of the dimensions of the non-trivial part. We can then truncate the sequence to a finite sequence of $*$-automorphisms, which has the linearity and multiplicative properties we want. □

We refer to these maps as a "layer" of single qubit maps, since all of these maps can be applied in parallel to each other.

Definition 4.2.2. *(Locality of Automorphisms) An inner $*$-automorphism φ is called* local *if there exists a set $C \subset \mathbb{N}$ such that for all $i \notin C$, $\varphi(M_i) = M_i$ for all 2×2 matrices M. If $|C| = 1$, then φ is also called* single-qubit *or* qubit-local.

If φ_1 is local to C, and φ_2 is local to C' with $C \cap C' = \emptyset$ then φ_1 and φ_2 are sometimes called disjoint *$*$-automorphisms.*

It is not actually important that each map in the chain is a single qubit operation. All we really require is that the operation is inner, and also that the position(s) it acts on is disjoint from all the positions of the previous maps.

Corollary 4.2.3. *Let φ_i be a family of inner $*$-automorphisms which are all local to a finite set of positions that are pairwise disjoint, then the chain*

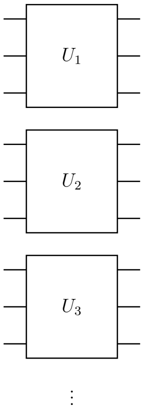
$$A \xrightarrow{\varphi_1} A_1 \xrightarrow{\varphi_2} A_2 \xrightarrow{\varphi_3} A_3 \xrightarrow{\varphi_4} \dots$$

Is a $*$-automorphism.

Proof. This follows the same argument as the proof of Theorem 4.2.1.

Given a $*$-algebra element $M \otimes \bar{I}$, where M has dimension 2^k, we can find the last element in the chain which is not disjoint from all positions $1 \dots k$ and truncate the chain there. Such an element must exist, because since all the maps are pairwise disjoint, there are only finitely many maps which are not also disjoint with the k positions. □

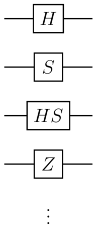
Schematically, this corresponds to taking a series of unitary operations affecting groups of qubits, where each group is disjoint from one another. For every element in the $*$-algebra, its active area only interacts with a finite number of maps in the chain, therefore the entire chain of map is well defined for every element in the $*$-algebra. As a circuit, the following chain of inner automorphisms (represented by their unitaries) forms an outer automorphism.



These can be done in one "layer" in a single step. One particular type of layer of this form is the qubit-local Clifford operation.

Definition 4.2.4. *(Qubit-Local Cliffords) A* qubit-local Clifford *operation is an operation where a single-qubit Clifford gate is applied to each qubit*

Pictorially, this amounts to something like



Another example of a $*$-automorphism is given by a special case of operations where the unitaries in the chain are not pairwise disjoint, but all commute. In this case the result is also a $*$-automorphism.

Lemma 4.2.5. *Let φ_i be a family of inner $*$-automorphisms which are all local to a finite set of positions and the operations pairwise commute, then the chain*

$$A \xrightarrow{\varphi_1} A_1 \xrightarrow{\varphi_2} A_2 \xrightarrow{\varphi_3} A_3 \xrightarrow{\varphi_4} \dots$$

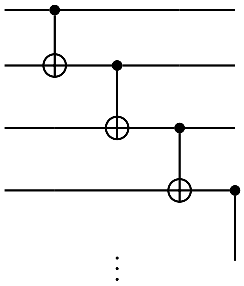
is a $*$-automorphism as long as each position i is acted on by a finite number of maps in the chain.

Proof. First as an illustrative example, consider the case of two commuting operations φ_0 and φ_1. Suppose that for a fixed $*$-algebra element $M \otimes \bar{I}$, φ_0 acts on the active region of M, but φ_1 does not. The result is that φ_0 can increase the size of the active region, in which case φ_1 may end up acting on a part that is now no longer identity.

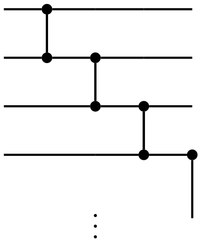
However, since φ_1 and φ_0 commute, we can apply φ_1 first, obtaining $M \otimes \bar{I}$ again, then apply φ_0. The conclusion is that we can still truncate the chain, by applying the non-interacting operations first.

Suppose now we have a sequence of maps φ_i. Since M is active on a finite region, we only need to apply the maps that intersect this position. That number is finite in the chain, since each position only intersects a finite number of maps in the chain, and there are finitely many positions. Thus the $*$-automorphism is well defined on the $*$-algebra. □

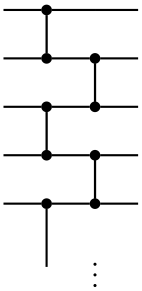
Consider the map given by the circuit



Clearly, this map is not allowed since the unitaries are not disjoint, and also are not pairwise commuting. However, the map given by the same circuit where the CNOT gates are replaced by controlled-Zs



Is in fact a valid infinite circuit, by lemma 4.2.5. The map is also equivalent to



Which is simply a composition of 2 outer $*$-automorphisms.

4.3 Graph States on the CAR Algebra

Definition 4.3.1. *Given an undirected graph $G(V, E)$ with no self-loops or duplicate loops, a graph state is the state produced by applying a Hadamard on every qubit of $|0\rangle^{\otimes|V|}$, and then applying a controlled-Z gate according to the edges of the graph. Specifically, for every edge $(i, j) \in E$, we apply C-Z_{ij}.*

Note that the C-Z gate is symmetric in that the action of gate is the same regardless of which one is the control and which position is the target. Thus, the graph should be undirected. Each C-Z commutes with the C-Z gate on any position, so there is no necessary ordering of the edges, and the graph itself encodes all necessary information of the graph state. The pair of edges (i, j) and (j, i) are considered duplicates. Unless noted, graphs in this section will be undirected with no self-loops or duplicate edges.

The notion of graph states can be replicated with states on the CAR algebra in a straightforward way. If the graph G is finite, and the state associated with G is denoted $|G\rangle$, then there is a corresponding state in the CAR algebra. Let s_0 denote the analogue of the all $|0\rangle$ state. Then for every finite graph, the graph state $|G\rangle$, $|G\rangle \otimes |0\rangle^{\otimes\infty}$ is in the CAR algebra.

Lemma 4.3.2. *Given an undirected graph $G(V, E)$ with $|V| \leq \infty$, then $|G\rangle \otimes |0\rangle^{\otimes\infty}$ is in the CAR algebra.*

Proof. Let $|0\rangle^{\otimes\infty}$ be the state corresponding to $|000\ldots\rangle$. Note that $|0\rangle^{\otimes\infty} = |0\rangle^{\otimes|V|} \otimes |0\rangle^{\otimes\infty}$. The Hadamard layer $H_1 H_2 \ldots H_{|V|}$ and the C-Z layer are valid $*$-automorphisms on the CAR algebra as finite sequences of inner automorphisms, therefore we can apply these operations to $|0\rangle^{\otimes\infty}$ and obtain $|G\rangle \otimes |0\rangle^{\otimes\infty}$ □

Graph states with finite graphs are interesting for many reasons, but can be implemented nicely on a conventional circuit model. The purpose of using a CAR algebra model is to consider more interesting graph states. One natural way to extend the notion of graph states is to consider infinite graphs.

Definition 4.3.3. *(Locally Finite Graphs) Let V be an countable index set (typically $\mathbb{N}$), and E be a subset of $V \times V$. The graph $G(V, E)$ is called locally finite if for every $i \in V$, the* $\deg(i)$ *is finite.*

It can be shown that for any locally finite graphs G, a corresponding state exists on the CAR algebra.

Definition 4.3.4. *Given an infinite, locally finite graph G, the state $|G\rangle$ is the state constructed by applying a layer of H gates, followed by a controlled-Z layer where c-Z_{ij} is applied for every edge (i, j)*

This is well defined, since each position only has a finite number of controlled-Z gates incident upon it, so the layer is a valid $*$-automorphism via Lemma 4.2.5,

The above definition would no longer hold for infinite graphs if we allowed vertices to have infinitely many neighbours, since we may need to apply an infinite sequence of automorphisms where the limit may not be well defined for all inputs. Within the proof of the Lemma 4.2.5, the fact that the c-Z gate is used and that the c-Z gate commutes with itself regardless of the positions it acts on is key. If the proof were replaced the CNOT gate for example, it would not hold.

In the case where the operators do not commute, it would not hold even if the graph has bounded degree. For example, applying CNOT_{12} to the element X_1 results in X_1X_2. The chain of CNOT gates $\text{CNOT}_{12}\text{CNOT}_{23}\text{CNOT}_{34}\dots$ would result in an element $X_1X_2X_3\dots$ which is not in the CAR algebra, so applying this infinite sequence of maps does not yield a valid $*$-automorphism on the $*$-algebra.

4.4 Relationship Between Graph States and Stabilizers

In the conventional model, the notion of a graph state and a stabilizer state holds a special relationship. We describe this relationship, and try to extend to the infinite dimensional case in the CAR algebra.

Recall that the Clifford group is generated by the gates $\{H, S, \text{CNOT}\}$. The subgroup generated by the single qubit gates $\{H, S\}$ gives us a group of operations which are local to each single qubit, which we will call local Clifford operations.

Definition 4.4.1. *Given two finite dimensional stabilizer states $|\psi_1\rangle$ and $|\psi_2\rangle$ are said to be local Clifford (LC) equivalent if there exists an element of the form*

$$\mathcal{K} = \bigotimes_{i}^{n} K_i$$

Where each K_i is a single qubit element of the Clifford Group CL_1

It is known in the conventional model that every graph state is a stabilizer.

Theorem 4.4.2. *Given a finite graph G, the graph state $|G\rangle$ is a stabilizer state, where the stabilizer (encoded into binary matrices) is of the form*

$$X = I, Z = A$$

Where I is the infinite identity matrix, and Z is the infinite adjacency matrix of G. That is, for each vertex i in G, there is a stabilizer of the form $X_i \prod_{j:(i,j)\in E} Z_j$.

Proof. Since the Hadamard layer and the controlled-Z layer are both Clifford $*$-automorphisms, then clearly $|G\rangle$ as defined is a stabilizer state. It remains to show that the given generators generate a stabilizer for $|G\rangle$.

Claim 1: These operators generate a maximal stabilizer.

Proof of claim 1. Note that it has n generators which are distinct. They are clearly independent, since the position of the X factors are all different, so one cannot generate the i-th stabilizer as a product of any of the other generators.

They also all commute pairwise. Let i and j be vertices in the graph, the corresponding stabilizers are $X_i \prod_{k:(i,k)\in E} Z_k$ and $X_j \prod_{k:(i,k)\in E} Z_k$. Each component of the stabilizers commute, unless $k = j$ or $k = i$, and $(i,j) \in E$. In this case, the stabilizer corresponding to i has the factor $X_i Z_j$, and $X_j Z_i$ for the stabilizer on j, which commutes.

This shows that the stabilizer is not extendable. □

Claim 2: The stabilizer stabilizes $|G\rangle$.

Proof of claim 2. We prove this claim by an induction on the edges for each vertex. Let M_i denote the stabilizer corresponding to the ith vertex, and U_{ij} denote the controlled-Z applied to i and j.

For the base case, note that if G n vertices and has no edges, then $|G\rangle = |+\rangle^{\otimes\infty}$. The stabilizers are of the form $M_i = X_i$, which together stabilizes $|G\rangle$.

Suppose $|G\rangle$ is a graph state corresponding to G, and we we add an edge (i,j) to G. The state transforms into $|G' = U_{ij}|G\rangle$, and the stabilizers M_i and M_j each gain a factor of Z, the others remaining unchanged. Since U_{ij} commutes with every Z gate, it commutes with every stabilizer $M_k = M'_k$ for $k \neq i, k \neq j$, which all do not have factors of X in positions i or j. We have,

$$
\begin{aligned}
M_k|G'\rangle &= M_k U_{ij}|G\rangle && (4.1)\\
&= U_{ij} M_k|G\rangle && (4.2)\\
&= U_{ij}|G\rangle && (4.3)\\
&= |G'\rangle && (4.4)
\end{aligned}
$$

so M_k is a stabilizer.

For M_i and M_j, we have that $U_{ij}M_iU_{ij}^* = Z_jM_i$, and $U_{ij}M_jU_{ij}^* = Z_iM_j$. A similar calculation then shows us that the new operator indeed is a stabilizer. □

This shows that the stabilizer we constructed is a maximal stabilizer, and the elements in the stabilizer all stabilizes $|G\rangle$. □

In *finite* dimensions, graph states are representative for the set of stabilizer states, in the sense of the following theorem.

Theorem 4.4.3. *Each stabilizer state $|\psi\rangle$ LC equivalent to a graph state for some G.*

By the above theorem, we can view graph states as a sort of standard form for stabilizer states.

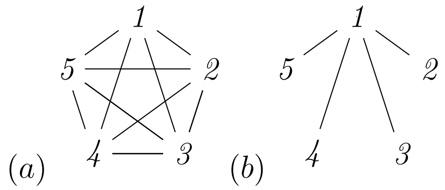
In the infinite dimensional case, we are interested in studying which theorems still hold. It can be shown that for a locally finite graph G, the graph state on the CAR algebra has a stabilizer which is maximal. Whether every maximal stabilizer is a graph state is still an open problem.

On a graph state, the edge connections essentially gives you the entanglement structure of the state. For example, the graph state for the connected graph consisting of two vertices connected by a single edge is LC equivalent to the Bell pair.

There are other LC operations that do change the underlying graph structure. In [18], Van den Nest et al. showed that there is essentially one graph operation that generates all graphs that are LC equivalent to one graph. The operation has a clear action on the graph.

Definition 4.4.4. *(Local Complementation) Given a graph $G(V, E)$, and a vertex $v \in V$, the local complement operation on the graph, applied at vertex v, takes the subgraph of the neighbours of v and complements it.*

Example 4.4.5. *Local complementation on the complete graph K_5*



(a) maps to (b) via the local complementation operation applied to vertex 1. The subgraph of the neighbours of 1 is the complete graph of vertices $2, 3, 4, 5$, so in the final graph, $2, 3, 4, 5$ have no edges with each other.

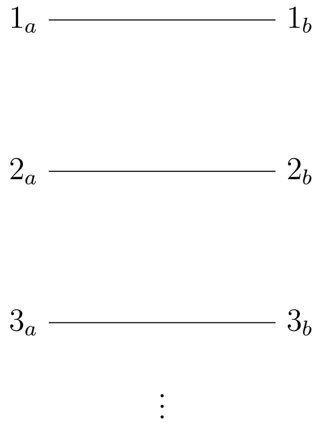
If we are allowed more than local Clifford operations, we can make more transformations between graphs. Suppose instead we had a bipartite state, where one set of qubits were local to Alice, and the remaining are local to Bob. Specifically, suppose we have some index set $\mathcal{I}$, and the state is bipartite on locations $\mathcal{I}$ and $\mathbb{N} \setminus \mathcal{I}$. Alice is only allowed to apply operations to her own qubits, and respectively Bob to his qubits. Alice and Bob can jointly perform any single qubit Clifford operations, and Alice and Bob can also apply multi-qubit Clifford operations to their own set of qubits, such as the controlled-Z.

In the finite dimensional case, the kind of entanglement we can achieve is simple. The state can always be transformed into one which is a product state composed of only Bell pairs and $|0\rangle$ states. This essentially amounts to transforming the graph into a union of K_2 and K_1 graphs, where K_n denotes the complete graph on n vertices.

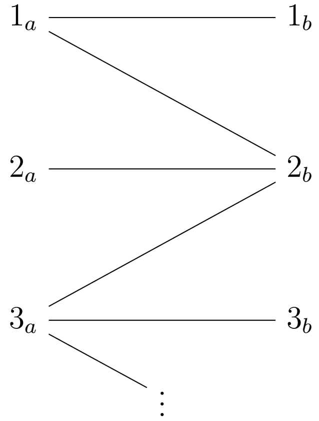
Lemma 4.4.6. *Let $|G\rangle$ be a finite dimensional graph state with graph G, with a partition on the vertices such that Alice holds the vertices $A \subset V$, and Bob holds $B = VA$. Up to operations local to Alice's and Bob's qubits, the state $|G\rangle$ is equivalent to a tensor product of Bell pairs and $|0\rangle$ states.*

In the CAR algebra case, whether this holds remains open.

We can construct examples of graph states which are equivalent to the maximally entangled state. Consider the following graph where the vertices on the left are held by Alice and the ones on the right are held by Bob.



This is the graph representing the infinite tensor product of Bell states. Suppose we have the state represented by the following graph.



We can actually convert the above graph to the top graph through a sequence of operations. First, we perform a controlled-Z on qubits 1_b and 2_b, then do a local complement on 1_b. This removes the edge $(1_a, 2_b)$. We then perform another controlled-Z to remove the edge $(1_b, 2_b)$.

Let $j = i + 1$, we remove each edge (i_a, j_b) by doing a controlled-Z on the pair (i_b, j_b), then a local complement on i_b, followed by a controlled-Z on (i_b, j_b) again. Note that these operations do not affect any other edges. Next, we turn our attention to the diagonal edges in the other direction, (j_a, i_b). We perform a similar sequence of operations, controlled-Z on (i_a, j_a), local complement on i_a, then controlled-Z on (i_a, j_a) again.

The local complement does not commute with the controlled-Z, so an arbitrary infinite sequence of operations is not necessarily valid. However, the operation that removes the edges (i_a, j_b) commute with each other, since the neighbourhoods of i_a and $(i+2)_a$ are disjoint. The infinite sequence of commuting $*$-automorphisms is itself a $*$-automorphism, so we can remove all the edges (i_a, j_b) at once, then remove the edges (j_a, i_b) afterwards.

However, it is not known if this can be done with all graph states.

Chapter 5

Related Work and Open Questions

5.1 Related Work

In this work, identified some of the limitations of the Hilbert space model of quantum information, and propose a novel formalism for stabilizer states on infinitely many qubits. There have been works similar to ours. In [8], Forney introduces a variant of stabilizers on infinite qubits to introduce quantum convolutional codes. In that setting, the states are from the *incomplete*[1] Hilbert space model, but the encoded state can assumed to be non-trivial on a finite number of indices since in practical terms one only wants to transmit a finite amount of information.

In the incomplete Hilbert space, we can have all k-qubit states for any finite k (where everything else is assumed to be padded with $|0\rangle$). In the CAR algebra model, we can really have an infinite dimensional state. It is an important distinction between arbitrary infinite dimensional states and arbitrary dimensional states padded with infinitely many $|0\rangle$. In the case of convolutional codes both models are interchangeable, but the quantum correlations achievable in the Hilbert space model is provably different from the correlations achievable in our model.

The fact that our model captures the types of states that we are interested in is not unique to the C*-algebra model, one can always come up with a Hilbert space model that also has the same states. In fact, it is a property of our construction that there exists at least one such Hilbert space by virtue of the GNS construction. The *complete* Hilbert space introduced by von Neumann should suffice, although it is not clear that there is a

[1] This refers to the smaller Hilbert space given by an infinite tensor product of Hilbert spaces.

faithful representation of the CAR algebra on the complete tensor product of infinitely many copies of $\mathbb{C}^2$. However, working in the Hilbert space model becomes fairly involved. A Hilbert space containing at least as many states as our model would be non-separable. Our model implicitly has a rich tensor product structure, as it contains all finitely many tensor products of $\mathbb{C}^2$, but also tensor products of the CAR algebra with other algebras is simple to construct by the fact that the CAR algebra is nuclear.

5.2 Open Questions

The main motivation for introducing this model is to try to describe exotic classes of entangled states. Many problems remain open in this area.

The first question is whether or not graph states are LC equivalent to stabilizer states in the infinite qubit model as they are in the finite dimensional model. It is shown in our work that graph states have a stabilizer in the CAR algebra model, but it is not known that every stabilizer has a graph state representation. Showing that they are equivalent would give allow us to use graphical techniques to study infinite stabilizer states.

In finite dimensions, the bipartite entanglement structure is extremely simple. Any bipartite state can be transformed into tensor products Bell states by operations local to each partition.

For infinite graphs it is not known if one can always transform the graph state into the tensor product of Bell states.

One can give examples of states that can be transformed into any finite number of Bell states, but it is not known if there is a $*$-automorphism that transforms it to the maximally entangled state. This leads to the question of whether graph states can achieve highly entangled states which are much harder to describe than in the finite dimensional case.

References

[1] Ola Bratteli and Derek W. Robinson. *Operator algebras and Quantum Statistical Mechanics*. Springer, 2002.

[2] Man-Duen Choi and Edward G. Effros. Nuclear c*-algebras and the approximation property. *American Journal of Mathematics*, 100(1):61–79, 1978.

[3] Richard Cleve, Benoit Collins, Li Liu, and Vern Paulsen. Constant gap between conventional strategies and those based on c$* - dynamicsforself - embezzlement.Quantum, 6 : 755, jul2022$.

[4] Richard Cleve, Li Liu, and Vern I. Paulsen. Perfect embezzlement of entanglement. *Journal of Mathematical Physics*, 58(1):012204, jan 2017.

[5] Andrea Coladangelo and Jalex Stark. An inherently infinite-dimensional quantum correlation. *Nature Communications*, 11(1), 2020.

[6] Kenneth Davidson. *C^*-algebras by example*. Amer Mathematical Society, 1996.

[7] David Fattal, Toby S. Cubitt, Yoshihisa Yamamoto, Sergey Bravyi, and Isaac L. Chuang. Entanglement in the stabilizer formalism, 2004.

[8] G. David Forney, Markus Grassl, and Saikat Guha. Convolutional and tail-biting quantum error-correcting codes. *IEEE Transactions on Information Theory*, 53(3):865–880, mar 2007.

[9] Daniel Gottesman. Stabilizer codes and quantum error correction, 1997.

[10] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel. Entanglement in graph states and its applications, 2006.

[11] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Physical Review A*, 69(6), jun 2004.

[12] Zhengfeng Ji, Jianxin Chen, Zhaohui Wei, and Mingsheng Ying. The lu-lc conjecture is false. *Quantum Info. Comput.*, 10(1):97–108, jan 2010.

[13] R V Kadison and John R Ringrose. *Fundamentals of the theory of operator algebras.* Springer, New York, NY, September 2011.

[14] Debbie Leung, Ben Toner, and John Watrous. Coherent state exchange in multi-prover quantum interactive proof systems, 2008.

[15] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2010.

[16] G K Pedersen. *C-Algebras and Their Automorphism Groups.* London Mathematical Society Monographs. Academic Press, San Diego, CA, September 1979.

[17] Wim van Dam and Patrick Hayden. Universal entanglement transformations without communication. *Physical Review A*, 67(6), jun 2003.

[18] Maarten Van den Nest, Jeroen Dehaene, and Bart De Moor. Graphical description of the action of local clifford transformations on graph states. *Phys. Rev. A*, 69:022316, Feb 2004.

[19] John von Neumann. On infinite direct products. *Compositio Mathematica*, 6:1–77, 1939.