HARVARD UNIVERSITY
Graduate School of Arts and Sciences

DISSERTATION ACCEPTANCE CERTIFICATE

The undersigned, appointed by the

Department of Physics

have examined a dissertation entitled

Finding and building algebraic structures in finite-dimensional Hilbert spaces for quantum computation and quantum information

presented by Robert Henry Lin

candidate for the degree of Doctor of Philosophy and hereby certify that it is worthy of acceptance.

Signature Arthur Jaffe

Typed name: Professor Arthur Jaffe, Chair

Signature Eric Heller

Typed name: Professor Eric Heller

Signature ______________________

Typed name: Professor Mikhail Lukin

Signature ______________________

Typed name: Professor Peter Shor (MIT)

Date: April 26, 2023

Finding and building algebraic structures in finite-dimensional Hilbert spaces for quantum computation and quantum information

A DISSERTATION PRESENTED
BY
ROBERT HENRY LIN
TO
THE DEPARTMENT OF PHYSICS

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
IN THE SUBJECT OF
PHYSICS

HARVARD UNIVERSITY
CAMBRIDGE, MASSACHUSETTS
APRIL 2023

Dissertation Advisor: Professor Arthur Jaffe Robert Henry Lin

Finding and building algebraic structures in finite-dimensional Hilbert spaces for quantum computation and quantum information

Abstract

In this dissertation, we investigate algebraic structures in finite-dimensional Hilbert spaces, as concerns quantum computation and quantum information, as well as these structures' applications to lattices.

On the quantum computation side, we develop an algebraic framework of axioms which abstracts various high-level properties of multi-qudit representations of generalized Clifford algebras. We further construct an explicit model and prove that it satisfies these axioms. Subsequently, we develop a graphical calculus for multi-qudit computations with generalized Clifford algebras, using the algebraic framework developed. We build our graphical calculus out of a fixed set of graphical primitives defined by algebraic expressions constructed out of elements of a given generalized Clifford algebra, a graphical primitive corresponding to the ground state, and also graphical primitives corresponding to projections onto the ground state of each qudit. We establish many algebraic identities, including a novel algebraic proof of a Yang-Baxter equation. We also derive a new identity for the braid elements, which is key to our proofs. We then use the Yang-Baxter equation proof to resolve an open question of Cobanera and Ortiz [4]. We demonstrate that in many cases, the verification of involved vector identities can be reduced to the combinatorial application of two basic vector identities. In addition, we show how to explicitly compute various vector states in an efficient manner using algebraic methods.

On the quantum information side, we introduce a new decomposition of quantum channels acting on group algebras, which we term Kraus-like operator decompositions (Kraus-like decompositions for short). An important motivation for this new decomposition is a general nonexistence result that we show for Kraus operator decompositions for quantum channels in this setting. We show that the notion of *convex* Kraus-like operator decompositions (in which the coefficients in the sum decomposition are nonnegative and satisfy a sum rule) that are induced by the irreducible characters of a finite group is equivalent to the notion of a conditionally negative-definite length when the length is a class function. For a general finite group G, we prove a stability condition which shows that if the semigroup associated with a length has a convex Kraus-like operator decomposition for all $t > 0$ small enough, then it has a convex Kraus-like operator decomposition for all time $t > 0$. Using the stability condition, we show that for a general finite group, conditional negativity of the length function is equivalent to a set of semidefinite linear constraints on the length function. By a result of [38], our result implies that in the group algebra setting, a semigroup P_t induced by a length function which is a class function is a *quantum channel* for all $t \geq 0$ if and only if it possesses a convex Kraus-like operator decomposition for all $t > 0$.

Finally, motivated by the importance of lattice problems in quantum cryptography, we extend the algebraic framework for multi-qudit representations of generalized Clifford algebras to lattices in $\mathbb{Z}_p^d$. We show that under suitable number-theoretic conditions, the subalgebra induced by a lattice has trivial center. Under the trivial center constraint, we construct for pairs of lattice vectors satisfying an algebraic constraint a unitary operator based on the product of generalized Clifford algebra generators associated to each lattice vector.

Contents

Dedicated to the teachers who have made me a better scientist and person.

Acknowledgments

When I first came to Harvard as a PhD student in Chemical Physics, little did I expect that, over seven years later, I would be graduating with a PhD in Physics, with my subfield being mathematical physics and quantum computation/information. Needless to say, there have been many hurdles along the way in getting to this point.

I wish to thank foremost my parents for supporting me throughout my graduate studies, and always believing in me.

I thank my advisor, Professor Arthur Jaffe, for creating a research environment which has allowed me to prosper and follow my intuition, physical and mathematical, in fruitful directions. Arthur has taught me not to focus on what is known, but always to work on new things.

I am grateful to Professor Howard Georgi for teaching me how to think, read, and write like a physicist, during a research and reading course I took with him in my G3 year, and the research that continued into the summer.

I am especially grateful to Professor Martin Karplus, who first welcomed me into his group when I was a G1, and has believed in and helped me throughout my graduate career.

I owe my heartfelt thanks to Professor Peter Shor, for his generous feedback on several of my projects, which helped me at important junctures when I was stuck.

I wish to thank Professor Eric Heller for helping to bring me into the physics department, and for teaching me to think in terms of pictures during my time in his group, as well as for patiently teaching me how to give a good presentation.

I want to thank Professor Misha Lukin for helpful feedback on my research. From a broader standpoint, I have benefited from taking his course in atomic and molecular optics, which illuminated for me the tightly constrained relationship between physical concepts, as formulated *quantitatively*, and mathematical derivations.

I also want to express my deep thanks to Professor Zhengwei Liu, now of Tsinghua University, for his foundational work on quon and parafermions with my advisor, without which none of my later work in Chapters 2, 3, and 5 would be possible. In my overlap with his stay as a postdoctoral fellow in the Jaffe group, I benefited greatly from listening to his informal talks, and he has always been kind and responsive to my queries.

Circling back to the beginning, I wish to express gratitude to Professor Richard Hamilton, of the mathematics department at Columbia University, who, as my undergraduate mathematics thesis advisor, gave me many valuable lessons on how to think and work in mathematics. I owe my gratitude to Professor Shlomo Sternberg, now retired, of the Harvard mathematics department, for mentoring me in my G1 year and for taking me on for a research rotation with him. Sitting in on his course on functional analysis, namely, the rigorous mathematical theory for quantum mechanics, planted the seeds, years later, to start working in a completely new field for me, that of mathematical physics. I have also benefited from mentorship from Professor Shing-Tung Yau, now emeritus of the Harvard mathematics department, during a brief spell in my G3 year. I would like to thank many important figures in my graduate studies in the physics department, namely, Professor Masahiro Morii, Professor Tim Kaxiras, Professor David Nelson, Professor Vinny Manoharan, Professor Doug Finkbeiner, Professor Bob Westervelt, Professor Chris Stubbs, Professor Mara Prentiss, the late Professor Roy Glauber, Barbara

Drauschke, Crystal Stillman, Professor Bert Halperin, Dr. Greg Kestin, Dr. Jacob Barandes, and Lisa Cacciabaudo, as well as Professor Jim Moran of the Harvard-Smithsonian Center for Astrophysics, and Professor Dan Stinebring of Oberlin College. I further want to thank Dr. Radhakrishnan Balu of the Army Research Office for his advice and guidance. I am grateful for the support from ARO Grant W911NF-20-1-0082 through the MURI project “Toward Mathematical Intelligence and Certifiable Automated Reasoning: From Theoretical Foundations to Experimental Realization.” Thanks to my long-time collaborator, Jon Boretsky (we did it!).

1

Introduction

This dissertation gives an account of my original work at the intersection of mathematical physics and quantum computation and quantum information. While the topics may seem to be disparate, there are technical reasons for this selection of problems and their resolution by the dissertation author. In each investigation undertaken,

1. The system is discrete, rather than continuous. Hence, no measure theory is required; there are no derivatives either.

2. The system is finite. Thus, the physical realm of interest is quantum mechanics, rather

than quantum field theory.

When one confines oneself to quantum mechanical systems of finite size, it is commonly understood that one is working with matrices. This is not true, although indeed most investigations into finite quantum-mechanical systems have dealt with this case. In Chapter 4, a deep investigation into the nature of quantum channels on finite group algebras (which can be described by direct sums of matrix representations) is presented.

In the field of quantum computation, many different graphical methods of representation have been proposed for quantum states and quantum operations, with their own particular advantages (a popular one for *qubit* representations is the ZX-calculus by [5][6]). One particular graphical representation for *qudit* representations (where the dimension of the single-particle Hilbert space is $d \geq 2$ instead of $d = 2$ for qubits) was introduced by Jaffe and Liu [15], based on ideas in operator algebras, planar algebras (in particular, the Temperley-Lieb algebra [41]), and reflection positivity. This graphical representation depicts vector states by linear superpositions of several caps, and operators as superposition of charged strings. Reflecting the structure of the underlying generalized Clifford algebra (GCA), the charges on each string can be moved vertically, and when two charges on different strings are moved past each other, the operator is the same provided one adds a phase factor.

In studying this graphical representation, the dissertation author realized that the advantages of pictorial intuition accrued by this graphical representation would be greatly multiplied if one could carry out the topological manipulations described in [15] on a computer algebra system (such as Mathematica). However, from a mathematical perspective, the existing theory was insufficient to accomplish this practical goal. Thus, Chapters 2 and 3 present the dissertation author's new algebraic axiomatization and graphical *reformulation* of multi-qudit representations of generalized Clifford algebras. These two chapters solve in large part the difficulties of transporting the topological manipulations into algebraic manipulations.

From the perspective of quantum computation, as one generalizes Clifford algebras to generalized Clifford algebras (mod p instead of binary), one goes from multi-qubit systems to multi-qudit systems. It is inevitable that richer and more exotic algebraic structures arise in these multi-qudit systems. The approach pioneered in this dissertation is to **build** algebraic structures from a distinguished ground state satisfying particular symmetry properties. The success of my approach in the particular case of the algebraic reconstruction of the graphical representation in [15] shows that one can encode particular structural properties at the level of the ground state, and under the action of an appropriate algebra, develop a complete calculus from the properties of the ground state alone.

Given this success, it becomes natural to consider whether for certain problems of interest in the quantum information science community, the same approach can work to *identify* and *isolate* the important structural features at an algebraic level. In Chapter 5, this approach is applied to understand the lattices appearing in quantum cryptography. The motivation here is to provide a new algebraic approach for tackling the problem of devising secure publicly-verifiable quantum lattice money [21], which is an important open problem in the field of quantum cryptography.

2

A new algebraic framework for quantum computation with generalized Clifford algebras

It is often desirable to formulate a theory as simply as possible, but no simpler. There are two constraints one would like to impose on a theory of graphical representation of the generalized Clifford algebras, which arise in the study of multi-qudit vector spaces in quantum computation. The first is the constraint of being physically reasonable, i.e. that the axioms of the theory be well-motivated from a physics standpoint. The second is the constraint of being correct and rigorous. An elementary set of axioms is presented by the dissertation author, which solves both these constraints, at one stroke.

In devising axioms for a theory, it is not sufficient from the perspective of mathematical completeness to merely propose axioms. One should also construct an explicit example of a mathematical object which satisfies these axioms. Thus, the bulk of the chapter is devoted to constructing an explicit representation of the generators of the generalized Clifford algebra that satisfies the axioms proposed, and proving that this representation indeed satisfies these axioms.[1]

2.1 The Algebraic Framework

Fix N a positive integer greater than 1, n a positive integer at least 1, and consider the **generalized Clifford algebra** $\mathcal{C}_{2n}^{(N)}$ generated by $c_1, c_2, c_3, \ldots, c_{2n}$, under multiplication and addition, equipped with scalar multiplication by the complex numbers $\mathbb{C}$. The generators c_k are subject to the relations $c_i c_j = q c_j c_i$ if $i < j$, and $c_i^N = 1$ for all i. Here, $q = \exp(2\pi i/N)$ is a primitive Nth root of unity. When $N = 2$, one recovers the Clifford algebra with $2n$ generators.

Whereas previous authors [15] have considered fairly elaborate frameworks for working with the generalized Clifford algebras in diagrammatic fashion, in this chapter, the following axiomatization is presented, which gives rise to a very straightforward algebraic framework for a graphical calculus for the generalized Clifford algebras.

Axiom 1: Let $\mathcal{V}^{N^n}(\mathbb{C})$ be a complex vector space upon which the generalized Clifford alge-

[1] This chapter is an expanded version of the arXiv preprint [24] by the dissertation author.

bra is realized as unitary N^n by N^n matrix operators. Assume that there exists a state (which we call the ground state) which is a tensor of states $|\Omega\rangle$, $|\Omega\rangle^{\otimes n}$, that satisfies the following algebraic identity:

$$c_{2k-1}\,|\Omega\rangle^{\otimes n} = \zeta\, c_{2k}\,|\Omega\rangle^{\otimes n} \tag{2.1.1}$$

for all $k = 1, 2, \ldots, n$, where ζ is a square root of q such that $\zeta^{N^2} = 1$.

In addition, for each qudit, the projector E_k onto the kth qudit's ground state $|\Omega\rangle$ is assumed to satisfy

$$c_{2k-1}E_k = \zeta\, c_{2k}E_k. \tag{2.1.2}$$

Axiom 2: Scalar product: The set $\{c_2^{a_1}c_4^{a_2}\ldots c_{2n}^{a_n}\,|\Omega\rangle^{\otimes n} \;:\; a_i \;=\; 0, 1, \ldots, N-1\}$ is an orthonormal basis for $\mathcal{V}^{N^n}(\mathbb{C})$.

The choice of these two axioms is motivated by the desire to solve at once the duality problem of representation, in which caps are transformed into cups via graphical manipulations, as well as the motion of charges around a cup or cap, both of which were discovered in [15]. While the representation of generalized Clifford algebras has been well-known as being unique up to equivalence, e.g., see [23], via bosonization of the GCA generators in terms of generalized Pauli operators (also known as the Jordan-Wigner transformation), the imposition of axiom 1 is state-dependent, and hence imposes a physical constraint, namely the existence of a distinguished ground state and the requirement of unitarity of the generators. Thus, it is important to show that this physical constraint is satisfied. Meanwhile, axiom 2 is a description of an inner product structure, and so *its* imposition ensures that that axiom 1 is compatible with an inner product structure.

We will show that these two axioms can be simultaneously satisfied by giving an explicit construction and verifying that this construction verifies all the properties and assumptions given in the axioms. In other words, the axiomatic framework is not a vacuous one. This is important since it implies that all results derived *from* the axioms are true in at least one explicit model.

The easiest way to construct a unitary representation of the generalized Clifford algebra satisfying the above axioms is to work backward from the assumption that the axioms hold, and to calculate the action of the generalized Clifford algebra on the basis states given by $\{c_2^{a_1} c_4^{a_2} \ldots c_{2n}^{a_n} \left|\Omega\right\rangle^{\otimes n} \,:\, a_i \,=\, 0, 1, \ldots, N-1\}$. For convenience, we label these basis states by the tuples $\left|a_1, a_2, \ldots, a_n\right\rangle$. Then

$$\begin{aligned} c_{2k} \left|a_1, a_2, \ldots, a_n\right\rangle &= c_{2k} c_2^{a_1} c_4^{a_2} \ldots c_{2n}^{a_n} \left|\Omega\right\rangle^{\otimes n} \\ &= q^{-\sum_{i<k} a_i} c_2^{a_1} c_4^{a_2} \cdots c_{2k}^{a_k+1} \cdots c_{2n}^{a_n} \left|\Omega\right\rangle^{\otimes n} \\ &= q^{-\sum_{i<k} a_i} \left|a_1, a_2, \ldots, a_k+1, \ldots, a_n\right\rangle . \end{aligned}$$

Thus, we now **define** c_{2k} as a matrix operator on the basis $\left|a_1, a_2, \ldots, a_n\right\rangle$ via

$$c_{2k} \left|a_1, a_2, \ldots, a_n\right\rangle := q^{-\sum_{i<k} a_i} \left|a_1, a_2, \ldots, a_k+1, \ldots, a_n\right\rangle \tag{2.1.3}$$

for $a_i = 0, 1, \ldots, N-1$.

Now, let's calculate the action of c_{2k-1} on this same basis. We first need to find ζ such that $\zeta^2 = q$ and $\zeta^{N^2} = 1$.

Lemma 2.1.1. *Let $q = \exp(2\pi i/N)$. If N is odd, $\zeta = -\exp(\pi i/N)$ is the only square root of q satisfying $\zeta^{N^2} = 1$. If N is even, setting ζ to be either square root of q will satisfy $\zeta^{N^2} = 1$.*

Proof. $q = e^{i\frac{2\pi}{2N+1}}$, $\zeta = \pm e^{i\frac{\pi}{2N+1}}$ for odd case yields $\zeta^{(2N+1)^2} = \pm\exp(i\pi(2N+1)) = (\pm 1)(-1) = \mp 1$, so one chooses the $-$ sign. For even case, $N = 2M$, $q = e^{i\frac{2\pi}{2M}} = e^{i\pi/M}$, then $\zeta = \pm e^{i\pi/2M} \rightarrow \zeta^{(2M)^2} = \zeta^{4M^2} = (\pm e^{i\pi/2M})^{4M^2} = e^{i\pi(2M)} = 1$. □

Thus, we choose ζ according to the lemma 2.1.1. Now using the axioms and applying c_{2k-1}

to the basis elements yields

$$\begin{aligned} c_{2k-1}\left|a_1,a_2,\ldots,a_n\right\rangle &= c_{2k-1}\,c_2^{a_1}c_4^{a_2}\ldots c_{2n}^{a_n}\left|\Omega\right\rangle^{\otimes n} \\ &= \zeta q^{a_k-\sum_{i<k}a_i}c_2^{a_1}c_4^{a_2}\cdots c_{2k}^{a_k+1}\ldots c_{2n}^{a_n}\left|\Omega\right\rangle^{\otimes n}, \end{aligned}$$

which then gives $\zeta\, q^{a_k-\sum_{i<k}a_i}\left|a_1,a_2,\ldots,a_k+1\ldots,a_n\right\rangle$. So we **define**

$$c_{2k-1}\left|a_1,a_2,\ldots,a_n\right\rangle := \zeta\, q^{a_k}q^{-\sum_{i<k}a_i}\left|a_1,a_2,\ldots,a_k+1,\ldots,a_n\right\rangle. \tag{2.1.4}$$

2.2 An Explicit Representation satisfying the Axioms

We are now in a position to state the following theorem.

Theorem 2.2.1. *Consider an orthonormal basis of the complex vector space $\mathcal{V}^{N^n}(\mathbb{C})$ labeled by the tuples $(a_1,a_2,\ldots,a_n)$, for $a_i=0,1,\ldots,N-1$, i.e. the states are given by $\left|a_1,a_2,\ldots,a_n\right\rangle$. We can identify this complex vector space with a tensor of n N-dimensional complex vector spaces such that $\left|a_1,a_2,\ldots,a_n\right\rangle = \left|a_1\right\rangle\otimes\cdots\otimes\left|a_n\right\rangle$.*

Define the matrix operators c_{2k-1}, c_{2k} by their action on the orthonormal basis $\left|a_1,a_2,\ldots,a_n\right\rangle$ via

$$c_{2k}\left|a_1,a_2,\ldots,a_n\right\rangle := q^{-\sum_{i<k}a_i}\left|a_1,a_2,\ldots,(a_k+1)(mod\,N),\ldots,a_n\right\rangle \tag{2.2.1}$$

and

$$c_{2k-1}\left|a_1,a_2,\ldots,a_n\right\rangle := \zeta\, q^{a_k}q^{-\sum_{i<k}a_i}\left|a_1,a_2,\ldots,(a_k+1)(mod\,N),\ldots,a_n\right\rangle \tag{2.2.2}$$

for all $k=1,2,\ldots,n$, where ζ is chosen according to the lemma 2.1.1.[2]

[2] For convenience, we will omit all the mod N qualifiers, and simply identify states with the same indices mod

Define the matrix operators E_k, for $k = 1, 2, \ldots, n$ by the linear extension of their action on the orthonormal basis via

$$E_k |a_1, a_2, \ldots, a_k, \ldots, a_n\rangle = \delta_{a_k,0} |a_1, a_2, \ldots, 0, \ldots, a_n\rangle \qquad (2.2.3)$$

for all $a_i = 0, 1, \cdots, N-1$, $i = 1, 2, \cdots, n$.

Define the ground state

$$|\Omega\rangle := |0\rangle \qquad (2.2.4)$$

so that

$$|\Omega\rangle^{\otimes n} := |0, 0, \cdots, 0\rangle \qquad (2.2.5)$$

Then the matrix operators c_{2k-1}, c_{2k}, E_k and the ground state $|\Omega\rangle$ satisfy axioms 1 and 2.

Proof. First, we need to show that c_{2k-1}, c_{2k} are unitary, and that $c_{2k-1}^N = 1$, $c_{2k}^N = 1$, as well as $c_i c_j = q c_j c_i$ for $i < j$.

Unitarity can be shown by showing that $c_{2k}^\dagger c_{2k} = c_{2k} c_{2k}^\dagger = 1$. Note that the dagger operation is just the usual conjugate transpose operation in the orthonormal basis setting.

$$c_{2k} = \sum_{a_j=0,1,\ldots,N-1} q^{-\sum_{i<k} a_i} |a_1, a_2, \ldots, a_k + 1, \ldots, a_n\rangle \langle a_1, a_2, \ldots, a_n|$$

implies

$$c_{2k}^\dagger = \sum_{a_j=0,1,\ldots,N-1} q^{\sum_{i<k} a_i} |a_1, a_2, \ldots, a_n\rangle \langle a_1, a_2, \ldots, a_k + 1, \ldots, a_n|$$

so clearly the outcome is

$$c_{2k} c_{2k}^\dagger = \sum_{a_j=0,1,\ldots,N-1} |a_1, a_2, \ldots, a_k + 1, \ldots, a_n\rangle \langle a_1, a_2, \ldots, a_k + 1, \ldots, a_n| = 1$$

N. This identification is justified since the coefficients of q to some power are invariant under shifts of the indices mod N.

and that

$$c_{2k}^{\dagger}c_{2k} = \sum_{a_j=0,1,\dots,N-1} \left|a_1,a_2,\dots,a_k,\dots,a_n\right\rangle \left\langle a_1,a_2,\dots,a_k,\dots,a_n\right| = 1.$$

Similarly, for c_{2k-1}, we have that

$$c_{2k-1} = \sum_{a_j=0,1,\dots,N-1} \zeta\, q^{a_k} q^{-\sum_{i<k} a_i} \left|a_1,a_2,\dots,a_k+1,\dots,a_n\right\rangle \left\langle a_1,a_2,\dots,a_n\right|$$

and

$$c_{2k-1}^{\dagger} = \sum_{a_j=0,1,\dots,N-1} \zeta^{-1}\, q^{-a_k} q^{\sum_{i<k} a_i} \left|a_1,a_2,\dots,a_n\right\rangle \left\langle a_1,a_2,\dots,a_k+1,\dots,a_n\right|$$

implying that

$$c_{2k-1}\, c_{2k-1}^{\dagger} = \sum_{a_j=0,1,\dots,N-1} \left|a_1,a_2,\dots,a_k+1,\dots,a_n\right\rangle \left\langle a_1,a_2,\dots,a_k+1,\dots,a_n\right| = 1.$$

And also that

$$c_{2k-1}^{\dagger}c_{2k-1} = \sum_{a_j=0,1,\dots,N-1} \left|a_1,a_2,\dots,a_k,\dots,a_n\right\rangle \left\langle a_1,a_2,\dots,a_k,\dots,a_n\right| = 1$$

This concludes the check for **unitarity**.

For the relations satisfied by c_{2k}, and c_{2k-1}, we have that since

$$c_{2k}\left|a_1,a_2,\dots,a_n\right\rangle = q^{-\sum_{i<k} a_i} \left|a_1,a_2,\dots,a_k+1,\dots,a_n\right\rangle$$

implies that

$$c_{2k}^{N}\left|a_1,a_2,\dots,a_n\right\rangle = q^{-N\sum_{i<k} a_i} \left|a_1,a_2,\dots,a_k+N,\dots,a_n\right\rangle = \left|a_1,a_2,\dots,a_k,\dots,a_n\right\rangle,$$

it follows by unique linear extension that $c_{2k}^N = 1$.

The statement for c_{2k-1} is a bit more involved to show. Starting from $c_{2k-1}\,|a_1, a_2, \ldots, a_n\rangle = \zeta\, q^{a_k} q^{-\sum_{i<k} a_i}\,|a_1, a_2, \ldots, a_k + 1, \ldots, a_n\rangle$, we obtain that

$$c_{2k-1}^2\,|a_1, a_2, \ldots, a_n\rangle = \zeta^2\, q^{a_k+(a_k+1)} q^{-2\sum_{i<k} a_i}\,|a_1, a_2, \ldots, a_k + 2, \ldots, a_n\rangle\,,$$

so that $c_{2k-1}^3\,|a_1, a_2, \ldots, a_n\rangle = \zeta^3\, q^{a_k+(a_k+1)+(a_k+2)} q^{-3\sum_{i<k} a_i}\,|a_1, a_2, \ldots, a_k + 3, \ldots, a_n\rangle$, and inductively, one obtains that

$$c_{2k-1}^m\,|a_1, a_2, \ldots, a_n\rangle = \zeta^m\, q^{m\,a_k+(0+1+\cdots+(m-1))} q^{-m\sum_{i<k} a_i}\,|a_1, a_2, \ldots, a_k + m, \ldots, a_n\rangle\,.$$

Plugging in $m = N$, we get that

$$\begin{aligned} c_{2k-1}^N\,|a_1, a_2, \ldots, a_n\rangle &:= \zeta^N\, q^{N\,a_k+N(N-1)/2} q^{-N\sum_{i<k} a_i}\,|a_1, a_2, \ldots, a_k, \ldots, a_n\rangle \\ &= \zeta^N\, q^{(N^2-N)/2}\,|a_1, a_2, \ldots, a_k, \ldots, a_n\rangle\,. \end{aligned}$$

Now things get interesting. If N is even, $\zeta = \pm q^{1/2}$ implies that $\zeta^N = q^{N/2}$, in which case $q^{N/2} q^{(N^2-N)/2} = q^{N^2/2} = 1$. If N is odd, $\zeta = -q^{1/2}$ implies that $\zeta^N = -q^{N/2}$, in which case $-q^{N/2} q^{(N^2-N)/2} = -q^{N^2/2} = -e^{(2\pi i/N)\cdot(N^2/2)} = -e^{N\pi i} = -(-1)^N = -(-1) = 1$! So we have shown that $c_{2k-1}^N = 1$.

To show $c_i c_j = q c_j c_i$ for all $i < j$, observe that

$$c_{2k}\,|a_1, a_2, \ldots, a_n\rangle = q^{-\sum_{i<k} a_i}\,|a_1, a_2, \ldots, a_k + 1, \ldots, a_n\rangle$$

yields

$$c_{2l} c_{2k}\,|a_1, a_2, \ldots, a_n\rangle = q^{-\sum_{i<l} a_i} q^{-\sum_{i<k} a_i}\,|a_1, a_2, \ldots, a_l + 1, \ldots, a_k + 1, \ldots, a_n\rangle$$

if $l < k$. Meanwhile, $c_{2l} \left|a_1, a_2, \ldots, a_n\right\rangle = q^{-\sum_{i<l} a_i} \left|a_1, a_2, \ldots, a_l + 1, \ldots, a_n\right\rangle$ yields

$$c_{2k}c_{2l} \left|a_1, a_2, \ldots, a_n\right\rangle = q^{-(\sum_{i<k} a_i)-1} q^{-\sum_{i<l} a_i} \left|a_1, a_2, \ldots, a_l + 1, \ldots, a_k + 1, \ldots, a_n\right\rangle .$$

So $c_{2k}c_{2l} = q^{-1}c_{2l}c_{2k}$, i.e.

$$c_{2l}c_{2k} = q\, c_{2k}c_{2l}$$

for $l < k$.

Repeating the procedure for c_{2k-1}, c_{2l-1}, we get that for $l < k$: $c_{2k-1} \left|a_1, a_2, \ldots, a_n\right\rangle = \zeta\, q^{a_k} q^{-\sum_{i<k} a_i} \left|a_1, a_2, \ldots, a_k + 1, \ldots, a_n\right\rangle$ implies

$$c_{2l-1}c_{2k-1} \left|a_1, a_2, \ldots, a_n\right\rangle = \zeta^2\, q^{a_k} q^{a_l} q^{-\sum_{i<k} a_i} q^{-\sum_{i<l} a_i} \left|a_1, a_2, \ldots, a_l + 1, \ldots, a_k + 1, \ldots, a_n\right\rangle$$

but swapping the order leads to

$$c_{2k-1}c_{2l-1} \left|a_1, a_2, \ldots, a_n\right\rangle = \zeta^2\, q^{a_k} q^{a_l} q^{-\sum_{i<k} a_i} q^{-\sum_{i<l} a_i} q^{-1} \left|a_1, a_2, \ldots, a_l + 1, \ldots, a_k + 1, \ldots, a_n\right\rangle$$

since the c_{2k-1} notices that the index on the l qudit has been increased by 1. Thus, $c_{2k-1}c_{2l-1} = q^{-1}c_{2l-1}c_{2k-1}$, i.e.

$$c_{2l-1}c_{2k-1} = q c_{2k-1}c_{2l-1}$$

for $l < k$.

Meanwhile, for c_{2k-1} and c_{2k}, we have that

$$c_{2k-1}c_{2k} \left|a_1, a_2, \ldots, a_n\right\rangle = \zeta\, q^{a_k+1} q^{-2\sum_{i<k} a_i} \left|a_1, a_2, \ldots, a_k + 2, \ldots, a_n\right\rangle$$

$$c_{2k}c_{2k-1} \left|a_1, a_2, \ldots, a_n\right\rangle = \zeta q^{a_k} q^{-2\sum_{i<k} a_i} \left|a_1, a_2, \ldots, a_k + 2, \ldots, a_n\right\rangle$$

so

$$c_{2k-1}c_{2k} = qc_{2k}c_{2k-1}.$$

For c_{2l-1}, c_{2k}, with $l < k$, we have that

$$c_{2l-1}c_{2k}\left|a_1, a_2, \ldots, a_n\right\rangle = \zeta q^{a_l} q^{-\sum_{i<l} a_i} q^{-\sum_{i<k} a_i}\left|a_1, a_2, \ldots, a_l + 1, \ldots, a_k + 1, \ldots, a_n\right\rangle$$

whereas

$$c_{2k}c_{2l-1}\left|a_1, a_2, \ldots, a_n\right\rangle = \zeta q^{a_l} q^{-\sum_{i<l} a_i} q^{-\sum_{i<k} a_i} q^{-1}\left|a_1, a_2, \ldots, a_l + 1, \ldots, a_k + 1, \ldots, a_n\right\rangle$$

since c_{2k} notices the change in the index of the lth qudit. So

$$c_{2l-1}c_{2k} = q\, c_{2k}c_{2l-1}$$

for $l < k$.

Finally, for c_{2l}, c_{2k-1} with $l < k$, we have that

$$c_{2l}c_{2k-1}\left|a_1, a_2, \ldots, a_n\right\rangle = \zeta q^{a_k} q^{-\sum_{i<k} a_i} q^{-\sum_{i<l} a_i}\left|a_1, a_2, \ldots, a_l + 1, \cdots, a_k + 1, \cdots, a_n\right\rangle$$

$$c_{2k-1}c_{2l}\left|a_1, a_2, \ldots, a_n\right\rangle = \zeta q^{a_k} q^{-\sum_{i<k} a_i} q^{-\sum_{i<l} a_i} q^{-1}\left|a_1, a_2, \ldots, a_l + 1, \cdots, a_k + 1, \cdots, a_n\right\rangle$$

so

$$c_{2l}c_{2k-1} = qc_{2k-1}c_{2l}$$

for $l < k$.

The above calculations showed that we have constructed a unitary representation of the generalized Clifford algebra. Now we have to show the other aspects of axiom 1 are true as well.

For the algebraic identity for c_{2k-1}, c_{2k}, and the ground state, we have that

$$c_{2k-1} \left|0, 0, \ldots, 0\right\rangle = \zeta \left|0, 0, \ldots, 0, 1, 0, \ldots, 0\right\rangle$$

and

$$c_{2k} \left|0, 0, \ldots, 0\right\rangle = \left|0, 0, \ldots, 0, 1, 0, \ldots, 0\right\rangle$$

with the 1 appearing on the kth qudit. Thus,

$$c_{2k-1} \left|0, 0, \ldots, 0\right\rangle = \zeta c_{2k} \left|0, 0, \ldots, 0\right\rangle .$$

For the algebraic identity involving c_{2k-1}, c_{2k}, E_k, we have

$$c_{2k-1}E_k \left|a_1, a_2, \ldots, a_{k-1}, a_k, a_{k+1}, \ldots, a_n\right\rangle = \zeta q^{-\sum_{i<k} a_i} \left|a_1, a_2, \ldots, a_{k-1}, 1, a_{k+1}, \ldots, a_n\right\rangle$$

$$c_{2k}E_k \left|a_1, a_2, \ldots, a_{k-1}, a_k, a_{k+1}, \ldots, a_n\right\rangle = q^{-\sum_{i<k} a_i} \left|a_1, a_2, \ldots, a_{k-1}, 1, a_{k+1}, \ldots, a_n\right\rangle .$$

Thus,

$$c_{2k-1}E_k = \zeta c_{2k}E_k$$

for all $k = 1, 2, 3, \ldots, n$.

This concludes the proof that axiom 1 is satisfied.

To show axiom 2 is satisfied, i.e. that the set $\{c_2^{a_1} c_4^{a_2} \ldots c_{2n}^{a_n} \left|0\right\rangle^{\otimes n} : a_i = 0, 1, \ldots, N-1\}$ is an orthonormal basis for $\mathcal{V}^{N^n}(\mathbb{C})$, it suffices to note that each power of c_{2k} raises the kth index by 1 and multiplies the state by a complex number of modulus 1. Thus, up to phase factors, the set $\{c_2^{a_1} c_4^{a_2} \ldots c_{2n}^{a_n} \left|0\right\rangle^{\otimes n} : a_i = 0, 1, \ldots, N-1\}$ is the same as $\{\left|a_1, a_2, \ldots, a_n\right\rangle : a_i = 0, 1, \ldots, N-1\}$, which by construction is an orthonormal basis for $\mathcal{V}^{N^n}(\mathbb{C})$. Hence, the set $\{c_2^{a_1} c_4^{a_2} \ldots c_{2n}^{a_n} \left|0\right\rangle^{\otimes n} : a_i = 0, 1, \ldots, N-1\}$ is an orthonormal basis as well.

□

2.3 Conclusion

This chapter gives an axiomatic framework for an entirely algebraic approach to doing computation with multiple qudits using the generalized Clifford algebra. While the area of fault-tolerant quantum computing with qudits has been relatively unexplored in the past (as compared to quantum computation using qubits), there has been increased interest in the native advantages which quantum computation in nonbinary bases may provide [37]. Given its simplicity and physical intuitiveness, the algebraic framework provided in this chapter may be useful for designing quantum computation schemes using qudits in a natural way using generalized Clifford algebras. Furthermore, it may open the way for the use of symbolic algebra methods, such as using Mathematica, to simplify complicated multi-qudit computations using GCA representations.

In this chapter, the major technical achievement is the abstraction of various concrete operational properties into high-level statements that highlight the nontrivial algebraic relations satisfied by the ground state and the projection operators under "local"[3] actions of the generalized Clifford algebra. Furthermore, the axiomatization emphasizes the particularly rigid structure imposed by the scalar product. Intuitively, this abstraction is a very appealing result, which appears to be related to standard themes in quantum error correction, in particular the stabilizer formalism of Gottesman [11]. One notable difference is that the operators involved in Gottesman's stabilizer formalism commute; in our case they do not.

In terms of physics, one may think of these algebraic identities as corresponding to the introduction of internal structure, in the sense of the particle physics mantra that if particles are not point particles (e.g., possessing spin or other quantum numbers), their internal dynamics

[3] Here, locality is to be understood in the sense of the index of the GCA generator i; the action of a GCA generator is *nonlocal* in the sense of a single-qudit action.

can be illuminated by scattering experiments (e.g., deep inelastic scattering experiments illuminated the quark structure of baryons). It seems reasonable to take such analogies more seriously in light of the recent scattering experiments with anyons [2].

At a mathematical level, the familiar adage is that "more structure equals more ease of computation"; at the same time, the more structure one has, the harder it becomes to verify that the resulting theory is a consistent one. Although one can work abstractly, the abstract proofs of consistency may not be accessible to physicists, at least not at a level at which he or she would be comfortable verifying. Thus, it is desirable to present explicit constructions of models satisfying an axiomatic theory, such as the one presented in this chapter.

3

A graphical calculus for multi-qudits using generalized Clifford algebras

3.1 Introduction

The following physics questions motivate this chapter[1]: Can we learn new things about quantum entanglement by studying a graphical calculus for the generalized Clifford algebras[2]?

[1] This chapter is adapted from the arXiv preprint [25] by the dissertation author.

[2] The earliest paper introducing generalized Clifford algebras appears to be [28] in 1952. Other early work included [45] in 1964, [36] in 1966, and [29] in 1967.

In this setting, braiding operators defined using the generalized Clifford algebra are unitary operations that entangle neighboring qudits (multi-dimensional vector spaces). Thus, when we apply a sequence of braiding operators to the ground (or vacuum) state, we expect different kinds of entangled states to result, depending on the sequence and on the braidings in the sequence. Is there an easy way to classify the resulting kinds of entanglement using the graphical calculus? How does the classification depend on the number of qudits involved?

To set the stage for a treatment of these questions in a systematic manner, a algebraic framework was presented in the previous chapter, based on [24]. While the algebraic framework is in it of itself sufficient for doing calculations and proving identities of various sorts, it turns out to be convenient to consider diagrammatic representations in order to obtain intuition about what kind of algebraic identities might be true. In contrast to the work of [15], the dissertation author will develop the graphical calculus along completely algebraic lines. A new result achieved in this chapter is an algebraic proof that a particular braid operator satisfies the Yang-Baxter equation, valid over all $N \geq 2$, which resolves an open question of Cobanera and Ortiz [4] about unitary self-dual braid group solutions for N even.

To enable users of the graphical calculus presented in this chapter to proceed in an entirely algebraic and rigorous way, the following flowchart is presented:

1. Write down an algebraic expression.

2. Convert it to one of the prescribed graphical forms.

3. Guess what graphical identities might be true for the graphical expression.

4. Write down conjectural algebraic identities corresponding to the conjectured graphical identities.

5. Prove the conjectured identities algebraically using explicit calculation with the algebraic framework for the generalized Clifford algebras, or using already proven algebraic

identities.

6. Repeat.

It is quite remarkable how far one can get with this approach, once the initial difficulties of getting algebraic identities is overcome. In particular, we show that the algebraic framework, coupled with some new technical innovations of ours, enables us to show **algebraically** for the first time why one can treat the braiding operator as a braid in the conventional sense (namely, it satisfies a Yang-Baxter equation[3]).

For logical consistency, the reader should consider the graphical calculus as simply a transcription of the algebraic framework into a combination of a few basic building blocks, which aids in intuition. While it may be tempting to imagine that the diagrams *mean something*, the reader will do well to remember that all our proofs are purely algebraic, and the diagrams are just (very helpful) visual aids.

In terms of the graphical representation, the diagrams allowed are a much smaller subset than as those of [15], in order to ensure *unambiguous* identification of a graphical diagram (via vertical decomposition) with an algebraic expression. In line with the requisite of unambiguity of graphical-to-algebraic correspondence, no independent interpretation is made of the subcomponents of the diagrams. The latter constraint imposed by the dissertation author makes its necessary to specify in advance all the possible configurations one may encounter in a full diagram, and the corresponding algebraic expressions. This specification is accomplished using the tool of diagrammatic composition, from the theory of Temperley-Lieb algebras [41],

[3] One important conceptual and technical point is that the Yang-Baxter equation [8], or rather, a braiding in the tensor categorical sense[31], appears to primarily refer to a morphism from A to $A \otimes A$, where A is an algebra, which embeds in $A \otimes A \otimes A$. The equation we will prove will have structural similarity to the Yang-Baxter equation, but to truly show that the equation is in fact a Yang-Baxter equation, it is necessary to show that the braid is a 2-local operator. This fact will be proven in this chapter. The reason for this subtlety is that generalized Clifford algebras have an additional time-ordering [15] when one wants to "tensor" elements together, and hence there is no global tensor product for the algebra. This additional structure could be useful in its own right.

applied to a particular (small) set of graphical primitives which are specified in their completeness.

From a physical perspective, while it has been previously thought [17] that the graphical representation of generalized Clifford algebras is akin to Feynman diagrams, in fact the particular graphical representation considered in this chapter is more accurately a description of *causal* diagrams, which arise in the old-fashioned perturbation theory approach to quantum field theory. Thus, the diagrams are more in the spirit of Schwinger's approach to quantum field theory than Feynman's, as *causality* was at the heart of Julian Schwinger's approach to quantum electrodynamics [39]. On a technical level, whereas the Feynman diagrams of Richard Feynman emphasize propagators in *momentum* space, Schwinger's approach emphasized Green's functions, which are correlation functions in *position* space.

This correspondence of the graphical representation with a causal description is *ensured* by the faithful transcription of diagrams into algebraic expressions. In other words, the identification of the time (vertical) axis with the order of operator composition from right to left has been elevated to the role of a *physical constraint* on the graphical representation. In this sense, the graphical identities that are proved in this chapter for vectors can be interpreted as showing that certain different unitary processes, when acting on a particular initial state, yield the same final state.

Overall, the results of this chapter may be summarized as the following: A graphical calculus is presented for multi-qudit computations with generalized Clifford algebras, using the algebraic framework developed in the previous chapter. A graphical calculus is built out of a fixed set of graphical primitives defined by algebraic expressions constructed out of elements of a given generalized Clifford algebra, a graphical primitive corresponding to the ground state, and also graphical primitives corresponding to projections onto the ground state of each qudit. Many graphical properties of the graphical calculus are proven using purely algebraic methods (as well as extended to algebraic identities which are not captured by the graphical representation), including a novel algebraic proof of a Yang-Baxter equation. Furthermore, we discover an important novel identity for bringing a charge over a braid, which are key to the proofs. In terms of physics, this identity and related braid identities reflect the presence of a conserved charge. Furthermore, it is shown that in many cases, the verification of involved vector identities can be reduced to the combinatorial application of two basic vector identities. Finally, it is shown how to explicitly compute various vector states in an efficient manner using algebraic methods.

3.2 The Graphical Calculus

3.2.1 Building Blocks

The philosophy followed in the graphical calculus presented is that the diagrams drawn are **indivisible**. No a priori meaning is assigned to the subcomponents of the diagrams, i.e. a single strand, or a single cap, or a single cup. The philosophy adopted is that the algebraic framework of the previous chapter ought to be robust enough that one can **derive** a posteriori a large number of algebraic relations, and therefore by proving more and more relations, the initially content-free diagrams acquire new, emergent properties. On a technical level, this approach leads to a more basic construction of a graphical calculus which is directly built out of the elements of the generalized Clifford algebra, which is justified by the axiomatic framework in the previous chapter.

In devising the graphical representation, we need to consider at the outset what kind of diagrams should be allowed. This is a subtle point that this dissertation brings to the fore. From the perspective of mathematical rigor, if one proceeds on entirely algebraic grounds, and it is decided to base the manipulation of graphical diagrams on corresponding algebraic identities, it becomes necessary that each graphical diagram have a *unique* algebraic expression. Note that the word “expression” is used, as opposed to “value.” Two expressions may evaluate to the same algebraic element in the generalized Clifford algebra. Likewise, two graphical diagrams may be *different* in the sense that they correspond to different algebraic expressions, but *equal* in the sense that the expressions they correspond to can be shown to be algebraically equal (under the relations of the generalized Clifford algebra and the two axioms).

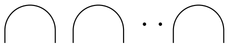
To be mathematically precise, one has to specify in what sense one means “uniqueness.” In this chapter, by uniqueness of the algebraic expression corresponding to a diagram, it is meant that the formal algebraic expression (forgetting all properties of the generalized Clifford algebra, *except* associativity, the property that $a(bc) = (ab)c$ for any elements a, b, c of the algebra) obtained from the diagram is invariant under vertical decomposition of the diagram, *up to* associativity. Thus, the graphical primitives are carefully chosen to guarantee uniqueness of an operator correspondence beyond diagrams and equations, a correspondence which is compatible with the vertical decomposition of diagrams. Adhering to this dictum results in a set of allowed diagrams that is much smaller than that of [15].

In the previous chapter, two axioms were presented as a way to abstract certain high-level properties of the generalized Clifford algebras. It was shown that these 2 axioms are satisfied by an explicit construction. These axioms will now be converted into graphical form. As before, let us fix N a positive integer greater than 1, n a positive integer at least 1, and consider the **generalized Clifford algebra** $\mathcal{C}_{2n}^{(N)}$ generated by c_1, c_2, c_3, . . . , c_{2n} subject to $c_i c_j = q c_j c_i$ if $i < j$, and $c_i^N = 1$ for all i. Here, $q = \exp(2\pi i/N)$ is a primitive Nth root of unity. When $N = 2$, one recovers the Clifford algebra with $2n$ generators.

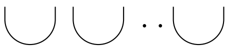
Let us first define a series of **graphical primitives**. These graphical primitives are the only allowed graphical elements in our graphical representation. Any diagram encoded using this set of graphical primitives must be specified by a sequence of graphical primitives. One may think of each diagram as a hieroglyph in an alphabet of hieroglyphs, and the sequence of hieroglyph as running from top to bottom. (This corresponds to the composition of operators, in which, in terms of the corresponding algebraic objects, the corresponding algebraic expression are given by a sequence of operations running from right to left.)

Fix $\delta = \sqrt{N} > 0$. The following graphical primitives are defined in terms of the distinguished ground state (satisfying the two axioms) via:

Definition 3.2.1.

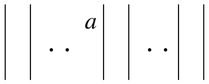


$$:= \delta^{n/2} |\Omega\rangle^{\otimes n} \tag{3.2.1}$$

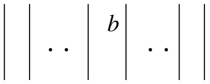


$$:= \delta^{n/2} \langle\Omega|^{\otimes n} \tag{3.2.2}$$

Definition 3.2.2.



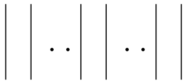
$$:= c^a_{2k-1} \tag{3.2.3}$$



$$:= c^b_{2k} \tag{3.2.4}$$

$\forall a, b \in \mathbb{Z}$. Here we mean for the label a to be placed immediately left of the $2k-1$-th strand, and the label b to be placed immediately left of the $2k$-th strand. There are $2n$ total strands in each diagram.

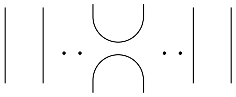
We also define for completion that



$$:= 1 \tag{3.2.5}$$

Note that the identity primitive composed with itself "is" itself, graphically, which is consistent with its definition as being equal to 1. Similarly, the identity primitive composed (in either order) with the primitives for the powers of the generators c_k again yields those same primitives. In this sense, the diagrammatic definitions are well-behaved.

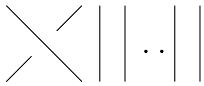
Definition 3.2.3.



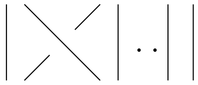
$$:= \delta E_k \tag{3.2.6}$$

Here we mean for the "cup-cap" combination to be replacing the $2k-1$ and $2k$th strands.[4] *There are $2n$ strands in total.*

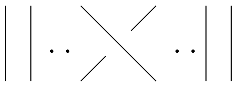
Definition 3.2.4. *We also define a graphical primitive, which we call the positive braid on strands l and $l+1$, for $l = 1, 2, \ldots, 2n-1$:*



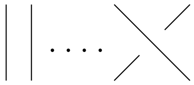
$$:= b_{12} \tag{3.2.7}$$



$$:= b_{23} \tag{3.2.8}$$



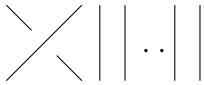
$$:= b_{k,k+1} \tag{3.2.9}$$



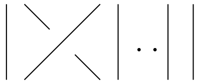
$$:= b_{2n-1,2n} \tag{3.2.10}$$

which defines $2n-1$ different braid operators.

We also define graphical primitives for the corresponding negative braids:

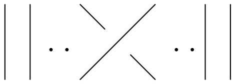


$$:= b_{21} \tag{3.2.11}$$

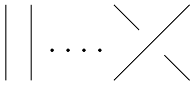


$$:= b_{32} \tag{3.2.12}$$

[4] In this respect, in our graphical calculus, we do not allow for the cup-cap combination which is prescribed in [15], i.e. we don't allow not-in-place placement, i.e. on the $2k$ and $(2k + 1)$th strands, which loosely speaking, straddles different qudits.



$$:= b_{k+1,k} \tag{3.2.13}$$



$$:= b_{2n,2n-1}. \tag{3.2.14}$$

The algebraic definition of these braid elements[5] *is given by*

$$b_{kl} := \frac{\omega^{1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} c_k^i c_l^{-i} \tag{3.2.15}$$

and

$$b_{lk} := \frac{\omega^{-1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} c_l^i c_k^{-i} \tag{3.2.16}$$

for $k < l$ *in* $\{1, 2, \ldots, 2n\}$. *Here,*

$$\omega := \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{i^2}. \tag{3.2.17}$$

Note that this is a general definition of the braid element, which goes beyond the diagrams above, since we allow for $|k - l| \neq 1$, which includes the local (nearest-neighbor) braid operators as a special case. We hasten to add that the terminology "braid element" at this point is only suggestive. To justify this terminology one has to prove that the braid elements satisfy braiding relations, in particular the Yang-Baxter equation, which is the subject of the section titled Applications on the Golden Rule.

Remark 3.2.5. *ω has modulus 1 (this fact is proven in Proposition 2.15 in [15]), implying that*

$$b_{kl}^{\dagger} = b_{lk} \tag{3.2.18}$$

[5] The special case in which k and l are adjacent was studied by Jaffe and Liu [15], which, to the best of the dissertation author's knowledge, is the first work to introduce this particular summation definition for the generalized Clifford algebra. A related summation expression for constructing a braid element is given by the work of Jones [19] in the case that N is a power of an odd prime.

for $k \neq l$.

Thus, in terms of terminology, we will refer to the positive braids as just braids, and the negative braids as adjoint braids.

3.2.2 Graphical Representation of the Axioms

Let us recall the axioms of the previous chapter:

Axiom 1: Let $\mathcal{V}^{N^n}(\mathbb{C})$ be a complex vector space upon which the generalized Clifford algebra is realized as unitary N^n by N^n matrix operators. Assume that there exists a state (which we call the ground state) which is a tensor of states $|\Omega\rangle$, $|\Omega\rangle^{\otimes n}$, that satisfies the following algebraic identity:

$$c_{2k-1}\,|\Omega\rangle^{\otimes n} = \zeta\, c_{2k}\,|\Omega\rangle^{\otimes n}$$

for all $k = 1, 2, \ldots, n$, where ζ is a square root of q such that $\zeta^{N^2} = 1$.

In addition, for each qudit, the projector E_k onto the kth qudit's ground state $|\Omega\rangle$ is assumed to satisfy

$$c_{2k-1}E_k = \zeta\, c_{2k}E_k.$$

Axiom 2: Scalar product: The set $\{c_2^{a_1}c_4^{a_2}\ldots c_{2n}^{a_n}\,|\Omega\rangle^{\otimes n} \;:\; a_i \;=\; 0, 1, \ldots, N-1\}$ is an orthonormal basis for $\mathcal{V}^{N^n}(\mathbb{C})$.

These axioms are now shown to give rise to basic graphical identities. The algebraic identities

$$c_i c_j = q c_j c_i$$

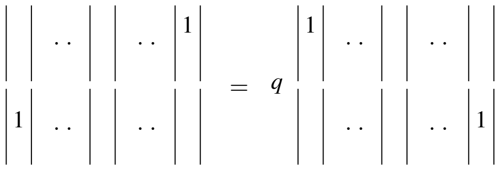
for $i < j$,

$$c_i^N = 1$$

for all $i = 1, 2, \ldots, 2n$, as well as

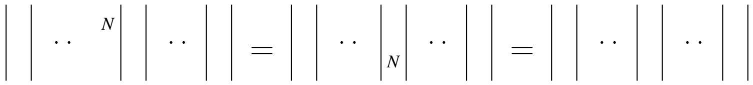
$$c_{2k-1}E_k = \zeta c_{2k}E_k$$

tell us that



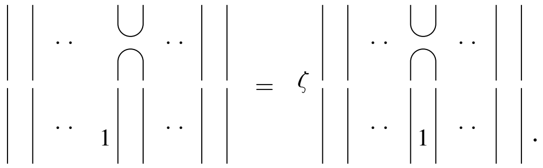
(3.2.19)

i.e. when the primitive for c_j precedes that for c_i, swapping the order of primitives yields a factor of q, for $i < j$, and also that



(3.2.20)

and

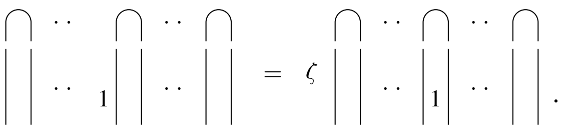


(3.2.21)

Furthermore, the vector identity

$$c_{2k-1}\left|\Omega\right\rangle^{\otimes n} = \zeta c_{2k}\left|\Omega\right\rangle^{\otimes n}$$

yields the diagrammatic "identity"



(3.2.22)

An additional identity which is useful [15] is the following:

Lemma 3.2.6.

$$c_i^a c_j^b = q^{ab} c_j^b c_i^a \tag{3.2.23}$$

for $i < j$, a, b integers.

Proof. By double induction on a and b. □

Another identity, due to [15], is

Lemma 3.2.7.

$$c_{2i-1}^a E_i = \zeta^{a^2} c_{2i}^a E_{2i} \tag{3.2.24}$$

for $i = 1, 2, \ldots, n$, a an integer.

Proof. By induction. □

3.3 Algebraic Identities from Algebraic Methods

Our aim in this section is to obtain a large swath of identities, which are related to the graphical representation we have presented, but for which we provide purely algebraic proofs. At the heart of the results of this section are a new "charge-braid" identity that answers an open question due to Jaffe, namely, how to bring the charge "over" the braid when $N \neq 2$. This seemingly innocuous result is used to great effect, by using the structural property that the generalized Clifford algebra generated by $c_1, c_2, \ldots, c_{2n}$ has trivial center. In particular, we provide an algebraic proof, using the proof strategy based on this structural characterization, that the braid elements b_{kl} satisfy many Yang-Baxter equations. Furthermore, we construct a general solution to the braid group relations, which enables us to resolve an open question of [4] for the case where N is even.

3.3.1 Structural Properties of the Generalized Clifford Algebras

Proposition 3.3.1. *The set* $\{c_1^{r_1}c_2^{r_2}\cdots c_{2n}^{r_{2n}} \ : \ r_1, r_2, \dots r_{2n} = 0, 1, \dots N-1\}$ *is a basis for the generalized Clifford algebra* $\mathcal{C}_{2n}^{(N)}$.

Proof. Any element of the generalized Clifford algebra is a finite sum of elements of the form $\alpha\, c_{k_1}^{\varepsilon_1}c_{k_2}^{\varepsilon_2}\cdots c_{k_m}^{\varepsilon_m}$ for $\alpha \in \mathbb{C}$, m a positive integer, k_i in the index set $I_{2n} = \{1, 2, \cdots, 2n\}$, and $\varepsilon_i \in \{1, -1\}$ for $i = 1, 2, \dots, m$. By repeatedly applying the relations $c_{k_i}^{-1} = c_{k_i}^{N-1}$ and $c_ic_j = qc_jc_i$ for $i < j$ to swap the order of multiplication, we can put each term in the sum into **normal form**, by which we mean that the term is of the form $\beta_{r_1r_2\dots r_{2n}}\, c_1^{r_1}c_2^{r_2}\cdots c_{2n}^{r_{2n}}$, for $r_i \in \{0, 1, 2, \dots, N-1\}$. Thus, we obtain that every element x of the generalized Clifford algebra is prescribed by a sum given by

$$x = \sum_{r_1, r_2, \dots r_{2n} = 0, 1, \dots N-1} x_{r_1r_2\dots r_{2n}}c_1^{r_1}c_2^{r_2}\cdots c_{2n}^{r_{2n}}.$$

Now we want to show that $x = 0$ in the algebra if and only if $x_{r_1r_2\cdots r_{2n}} = 0$ for all indices, i.e. the set $\{c_1^{r_1}c_2^{r_2}\cdots c_{2n}^{r_{2n}} \ : \ r_1, r_2, \dots r_{2n} = 0, 1, \dots N-1\}$ is a basis. The if direction is obviously true. For the only if direction, suppose $x = 0$. Then multiplying x by any product of generators c_i also yields zero. It is clear that we can multiply x on the left by the product $c_{2n}^{-r_{2n}}c_{2n-1}^{-r_{2n-1}}\cdots c_2^{-r_2}c_1^{-r_1}$ so that the constant term of $c_{2n}^{-r_{2n}}c_{2n-1}^{-r_{2n-1}}\cdots c_2^{-r_2}c_1^{-r_1}x$ is $x_{r_1r_2\cdots r_{2n}}$. Thus, without loss of generality, it suffices to show that if $x = 0$, then its constant term must vanish. Then the rest of the coefficients all vanish by applying the same result to $c_{2n}^{-r_{2n}}c_{2n-1}^{-r_{2n-1}}\cdots c_2^{-r_2}c_1^{-r_1}x$ for each index tuple.

To show that the constant term must vanish, we use an operator method. Consider the set of operators $L_k(y) = \sum_{i=0}^{N-1} c_k^i y c_k^{-i}$, and let $L_k^{(l)} := L_k^{(l-1)} \circ L_k$ and $L_k^{(0)} := 1$ define $L_k^{(l)}$ iteratively.

Then the operator $M_k = \sum_{l=0}^{N-1} L_k^{(l)}$ acting on a term $c_1^{r_1} c_2^{r_2} \cdots c_{2n}^{r_{2n}}$ yields

$$\left(\sum_{l=0}^{N-1} (q^{-\sum_{i<k} r_i + \sum_{i>k} r_i})^l \right) c_1^{r_1} c_2^{r_2} \cdots c_{2n}^{r_{2n}} = N\delta(\sum_{i<k} r_i, \sum_{i>k} r_i) c_1^{r_1} c_2^{r_2} \cdots c_{2n}^{r_{2n}}, \tag{3.3.1}$$

where $\delta(a, b) := 1$ if $a \equiv b \bmod N$, and 0 otherwise. Acting on x by the commuting operators $\frac{1}{N} M_k$ (which all have a diagonal action on $c_1^{r_1} c_2^{r_2} \cdots c_{2n}^{r_{2n}}$) thus projects x down to

$$(\prod_{k=1}^{2n} \frac{1}{N} M_k)(x) = \sum_{r_1, r_2, \ldots r_{2n} = 0, 1, \ldots N-1} \left(\prod_{k=1}^{2n} \delta(\sum_{i<k} r_i, \sum_{i>k} r_i) \right) x_{r_1 r_2 \ldots r_{2n}} c_1^{r_1} c_2^{r_2} \cdots c_{2n}^{r_{2n}}. \tag{3.3.2}$$

We first claim that the only terms that survive are those for which $r_k + r_{k+1} = 0 \bmod N$ for $k = 1, 2, \ldots, 2n-1$. This can be seen since

$$\sum_{i<k} r_i = \sum_{i>k} r_i \Rightarrow 2 \sum_{i<k} r_i + r_k = \sum_{i=1}^{2n} r_i \tag{3.3.3}$$

for all $k = 1, 2, \ldots, 2n$ implies that

$$2 \sum_{i<k} r_i + r_k = 2 \sum_{i<k+1} r_i + r_{k+1} = 2 \sum_{i<k} r_i + 2r_k + r_{k+1} \tag{3.3.4}$$

for all $k = 1, 2, \ldots, 2n-1$, and so

$$r_k + r_{k+1} = 0 \bmod N, \tag{3.3.5}$$

as desired.

As a result, we further obtain that

$$r_{2n} = 0$$

since

$$\sum_{i<2n-1} r_i = (r_1 + r_2) + (r_3 + r_4) + \cdots + (r_{2n-3} + r_{2n-2}) = 0 = r_{2n}.$$

Finally, using $r_k + r_{k+1} = 0$ for $k = 1, 2, \ldots, 2n-1$ we obtain that $r_k = 0$ for all $k = 1, 2, \ldots, 2n$. Hence the constant term is the only term left, and must equal 0 since $M_k(0) = 0$.

□

Proposition 3.3.2 (Golden Rule)**.** *The generalized Clifford algebra $\mathcal{C}_{2n}^{(N)}$ has trivial center, i.e. the only elements that commute with all elements of the generalized Clifford algebra are* $\mathbb{C}1$.

Proof. Every element of the generalized Clifford algebra is prescribed by a sum given by

$$x = \sum_{r_1, r_2, \ldots r_{2n} = 0, 1, \ldots N-1} x_{r_1 r_2 \ldots r_{2n}} c_1^{r_1} c_2^{r_2} \cdots c_{2n}^{r_{2n}}.$$

Using the basis property (Proposition 3.3.1), it becomes simple to show that the algebra has trivial center. Note that the basis property implies uniqueness of the sum decomposition. Let x lie in the center of the algebra, and $x \neq 0$. Then there is an index label $r_1, r_2, \cdots, r_{2n}$ such that $x_{r_1 r_2 \cdots r_{2n}} \neq 0$. Note that $xc_1 = c_1 x$ implies that $x_{r_1 r_2 \cdots r_{2n}} = q^{-(r_2 + r_3 + \cdots r_{2n})} x_{r_1 r_2 \cdots r_{2n}}$ by comparing the coefficient of $c_1^{r_1+1} c_2^{r_2} \cdots c_{2n}^{r_{2n}}$. Thus, $r_2 + r_3 + \cdots + r_{2n} = 0$. Similarly, $xc_k = c_k x$ implies that $q^{-\sum_{i<k} r_i} x_{r_1 r_2 \cdots r_{2n}} q^{\sum_{i>k} r_i} x_{r_1 r_2 \cdots r_{2n}} = 1$ and so

$$\sum_{i=1}^{2n} \varepsilon_{ik} r_i = 0 \text{ (mod } N), \tag{3.3.6}$$

for k from 1 to $2n$, where $\varepsilon_{ik} = 1$ if $i < k$ and -1 if $i > k$ and 0 if $i = k$, yielding $2n$ equations in $2n$ unknowns. Equivalently,

$$\sum_{i<k} r_i = \sum_{i>k} r_i \text{ (mod } N) \tag{3.3.7}$$

for all $k = 1, 2, \cdot, 2n$. Since in Proposition 3.3.1, it was shown that this set of equations is uniquely solved by $r_1 = r_2 = \cdots = r_{2n} = 0$, it follows that x is a multiple of the identity

1. □

3.3.2 An "Intertwining" Approach for New Identities for the Generalized Clifford Algebra

A Systematic Procedure

The golden rule of Proposition 3.3.2 allows us to give a systematic procedure for proving identities in the algebra. The basis of the procedure is the following proposition:

Proposition 3.3.3. *Let x, y lie in the generalized Clifford algebra, and suppose y is invertible. Further assume that the constant terms of x and y are nonzero. Then $x = y$ if and only if $y^{-1}x$ lies in the center of the generalized Clifford algebra, and the constant term in x agrees with the constant term in y.*

Proof. Clearly, the only if direction is true since $x = y$ implies $y^{-1}x = 1$. For the if direction, if $y^{-1}x$ lies in the center, by the golden rule, $y^{-1}x \in \mathbb{C}1$, i.e. $y = \alpha x$. In the proof of proposition 3.3.2, we showed that this implies that all terms of y and αx agree, in particular the constant terms. By hypothesis, the constant terms of y and x agree and are nonzero, so $\alpha = 1$. □

We now provide a concrete way to show that an element lies in the center of the generalized Clifford algebra.

Proposition 3.3.4. *An element x lies in the center of the generalized Clifford algebra if and only if it commutes with c_i for each $i = 1, 2, \ldots, 2n$.*

Proof. The only if direction is clearly true.

For the if direction, any element y in the algebra has a unique decomposition as

$$y = \sum_{r_1, r_2, \ldots r_{2n} = 0, 1, \ldots N-1} y_{r_1 r_2 \ldots r_{2n}} c_1^{r_1} c_2^{r_2} \cdots c_{2n}^{r_{2n}}.$$

By iterative commutation, using the commutation property of x with c_i, one can show that $x\, c_1^{r_1} c_2^{r_2} \cdots c_{2n}^{r_{2n}} \;=\; c_1^{r_1} c_2^{r_2} \cdots c_{2n}^{r_{2n}}\, x$. Multiplying by the constant prefactor and summing over the indices, one obtains that $xy = yx$, as desired, for arbitrary y in the algebra. □

Intertwining Identities

By intertwining identities, we mean identities of the form $bx \;=\; yb$. In this section, we present the following new intertwining identity for the braid b_{kl}. We first give a direct proof, and then give an alternate proof which involves some intermediate intertwining identities, the particular concatenation of which may have more general applications. This identity significantly generalizes a theorem of Jaffe and Liu [15] (Theorem 8.2), which is the special case for $a = 0$.

Proposition 3.3.5.

$$b_{kl} c_k^a c_l^b = q^{a^2+ab} c_k^{2a+b} c_l^{-a} b_{kl} \tag{3.3.8}$$

for $k < l$.

Proof. Since $b_{kl} = \frac{\omega^{1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} c_k^i c_l^{-i}$, it suffices to show that

$$\left(\sum_{i=0}^{N-1} c_k^i c_l^{-i}\right) c_k^a c_l^b = q^{a^2+ab} c_k^{2a+b} c_l^{-a} \left(\sum_{i=0}^{N-1} c_k^i c_l^{-i}\right).$$

Applying lemma 3.2.6, the LHS becomes

$$\sum_{i=0}^{N-1} q^{ai} c_k^{a+i} c_l^{b-i} \tag{3.3.9}$$

and the RHS becomes

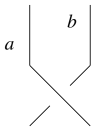
$$\sum_{i=0}^{N-1} q^{a^2+ab} q^{ai} c_k^{2a+b+i} c_l^{-a-i}. \tag{3.3.10}$$

By shifting the index of summation from i to $i + a + b$ in the LHS, the LHS becomes

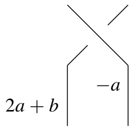
$$\sum_{i=0}^{N-1} q^{a(i+a+b)} c_k^{2a+b+i} c_l^{-a-i} \tag{3.3.11}$$

which is just the RHS. □

In terms of the graphical calculus, we economically write down the following diagrammatic identity, which is specific to b_{12} and the generalized Clifford algebra with only 2 generators c_1, c_2:



$$= q^{a^2+ab} \tag{3.3.12}$$



It is convenient to also write down the corresponding identity for the adjoint braid:

Corollary 3.3.6.

$$b_{lk} c_k^r c_l^s = q^{rs+s^2} c_k^{-s} c_l^{r+2s} b_{lk}. \tag{3.3.13}$$

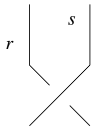
for k < l, and r,s integers.

Proof. The adjoint of the identity in 3.3.5 is $c_l^{-b} c_k^{-a} b_{lk} = q^{-a^2-ab} b_{lk} c_l^a c_k^{-2a-b}$, which becomes $q^{-ab} c_k^{-a} c_l^{-b} b_{lk} = q^{a^2} b_{lk} c_k^{-2a-b} c_l^a$ upon commutation. Now we let $r = -2a - b$, $s = a$, so

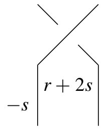
$$b_{lk} c_k^r c_l^s = q^{rs+s^2} c_k^{-s} c_l^{r+2s} b_{lk}, \tag{3.3.14}$$

which gives the desired result. □

The corresponding diagrammatic identity for the adjoint braid b_{21} arising from Corollary 3.3.6 for the generalized Clifford algebra with two generators c_1, c_2 is



$$= q^{rs+s^2} \tag{3.3.15}$$



We now pursue an alternate route to proving Equation 3.3.5, which illuminates complementary aspects. We start with an intertwining identity which is a commutation relation:

Lemma 3.3.7.

$$(c_k^b c_l^{-b})(c_k^a c_l^{-a}) = (c_k^a c_l^{-a})(c_k^b c_l^{-b}) \tag{3.3.16}$$

for $k < l$.

Proof. Applying lemma 3.2.6 to LHS yields $q^{ab} c_k^{a+b} c_l^{-(a+b)}$; applying lemma 3.2.6 to RHS yields $q^{ab} c_k^{a+b} c_l^{-(a+b)}$. Thus, LHS=RHS. □

We also note that the following commutation relation holds as well:

Lemma 3.3.8.

$$(c_k^a c_l^{-a}) c_p = c_p (c_k^a c_l^{-a}) \tag{3.3.17}$$

for $k < l$ and p satisfies $p < k < l$ or $p > l > k$.

Proof. If $k < l < p$, commuting c_p past (in front of) c_l^{-a} in the LHS yields q^{-a}; commuting it past c_k^a then yields an additional factor q^a. So we obtain the RHS. A similar proof applies for the case $p < k < l$. □

Now comes the exciting part. Since the braid b_{kl} is a sum of elements of the form $c_k^i c_l^{-i}$, it follows by linearity that

Lemma 3.3.9.

$$b_{kl}\, c_k^a c_l^{-a} = c_k^a c_l^{-a}\, b_{kl} \tag{3.3.18}$$

for $k < l$.

Proof. By linear extension of Lemma 3.3.7. □

Now we use a simple result due to Jaffe and Liu [15] (Theorem 8.2):

Lemma 3.3.10.

$$b_{kl}c_l = c_k b_{kl} \tag{3.3.19}$$

for $k < l$.

Proof. It suffices to show that

$$\left(\sum_{i=0}^{N-1} c_k^i c_l^{-i}\right) c_l = c_k \left(\sum_{i=0}^{N-1} c_k^i c_l^{-i}\right). \tag{3.3.20}$$

Collecting terms, it is equivalent to show that

$$\sum_{i=0}^{N-1} c_k^i c_l^{-(i-1)} = \sum_{i=0}^{N-1} c_k^{i+1} c_l^{-i}. \tag{3.3.21}$$

It is clear that the two are equal since the RHS is just the LHS with i shifted to $i-1$. □

It remains but to combine lemmas 3.3.9 and 3.3.10, giving us an alternate proof of proposition 3.3.5:

Alternate Proof of Proposition 3.3.5. We want to show that

$$b_{kl}c_k^a c_l^b = q^{a^2+ab} c_k^{2a+b} c_l^{-a} b_{kl} \tag{3.3.22}$$

for $k < l$. To use lemmas 3.3.9 and 3.3.10, we rewrite $b_{kl}c_k^a c_l^b$ as $b_{kl}c_k^a c_l^{-a} c_l^{a+b}$. This becomes $c_k^a c_l^{-a} b_{kl} c_l^{a+b}$ after commuting past the braid, and then $c_k^a c_l^{-a} c_k^{a+b} b_{kl}$ after applying lemma 3.3.10 $a+b$ times. Finally, applying lemma 3.2.6 to the middle two terms yields $q^{a^2+ab} c_k^{2a+b} c_l^{-a} b_{kl}$ as desired. □

The Notion of Charge Conservation

We now interpret the previous section's intertwining identities in terms of physics. In particular, it is observed that the new charge-braid identity in Proposition 3.3.5 is a consequence of a particular property of neutral pairings of c_k and c_l. The notion of charge and charge neutrality was first introduced by [15]. First, we define a charge operator C:

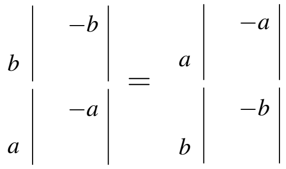
Definition 3.3.11. *Define C by linear extension of its action on the basis:*

$$C(c_1^{r_1}c_2^{r_2}\cdots c_{2n}^{r_{2n}}) := q^{r_1+r_2+\cdots+r_{2n}}c_1^{r_1}c_2^{r_2}\cdots c_{2n}^{r_{2n}} \tag{3.3.23}$$

*for all integer indices r_i. We call $r_1 + r_2 + \cdots + r_{2n}$ the **charge** of the basis element, following [15], which is well-defined modulo N. This terminology of an element's charge is also applicable for linear combinations of basis elements with the same charge.*

Then, lemma 3.3.7 tells us that eigenstates of C of eigenvalue 1 which lie in the subalgebra generated by c_k, c_l commute. We call eigenstates of C with eigenvalue 1 *neutral*.

Graphically, we can describe this commutation relation 3.3.7 for the algebra generated by c_1 and c_2 as



(3.3.24)

and there are analogous diagrams (with additional strands in between, and to the left and right) for the generalized Clifford algebras with more generators.

We now observe that the lemma 3.3.9 can be reinterpreted in terms of respecting charge conservation, i.e. bringing an element of definite charge across the braid will **conserve** the charge, which is in this case just 0. Thus, we say that the relation 3.3.9 provides a physical constraint on the action of the braid. In fact, this physical constraint provides a compelling explanation for why the master intertwining relation 3.3.5 holds; the latter is essentially forced by the constraint and the additional relation $b_{kl}c_l = c_k b_{kl}$.

3.3.3 Applications of the Golden Rule

Using the prior sections on the golden rule and various intertwining identities, we can now prove some identities involving the braid in a relatively straightforward manner. The following proof of unitarity is new, although the result is easily shown using explicit summation and is known in [15]. The importance of this new proof is that it introduces a new approach, using the trivial center property of the generalized Clifford algebra, which extends to proving identities for sums which are extremely difficult to calculate.

Unitarity

Proposition 3.3.12 (Unitarity of Braid Elements)**.** *Suppose $|k-l| = 1$, then*

$$b_{kl}b_{lk} = b_{lk}b_{kl} = 1. \tag{3.3.25}$$

(As was remarked in the definition of the braids, $b_{kl}^{\dagger} = b_{lk}$, so equivalently, b_{kl} is unitary.)

Proof. Fix $k < l$, so we fix the braid elements. To prove this identity, we rely on propositions 3.3.3 and 3.3.4. Thus, we just need to show that a) $b_{kl}b_{lk}$ and $b_{lk}b_{kl}$ lie in the center, and b) the constant terms of $b_{kl}b_{lk}$ and $b_{lk}b_{kl}$ are both 1. To show that they lie in the center, we need to check that c_p commutes with $b_{kl}b_{lk}$ for all p. Note that if $p < k < l$ or $p > l > k$, then c_p commutes with b_{kl} since it commutes with $c_k^a c_l^{-a}$ by lemma 3.3.8. We now note that $c_p b_{kl} = b_{kl} c_p$ implies the adjoint equation $b_{lk} c_p^{-1} = c_p^{-1} b_{lk}$, which further yields $b_{lk} c_p = c_p b_{lk}$ by iterating the commutation relation for c_p^{-1} $N-1$ times. Thus, c_p commutes with both b_{kl} and b_{lk}. Since $|k-l| = 1$, the only other possibilities we need to check for c_p are $p = k$ or $p = l$.

Recall that we have the master braid identity 3.3.5: $b_{kl}c_k^a c_l^b = q^{a^2+ab}c_k^{2a+b}c_l^{-a}b_{kl}$. Applying this identity allows us to bring c_k past $b_{kl}b_{lk}$ via

$$b_{kl}b_{lk}c_k = b_{kl}c_l b_{lk} \tag{3.3.26}$$

$$= c_k b_{kl}b_{lk}, \tag{3.3.27}$$

and c_l past $b_{kl}b_{lk}$ via the slightly more involved

$$b_{kl}b_{lk}c_l = q\, b_{kl}c_k^{-1}c_l^2 b_{lk} \tag{3.3.28}$$

$$= c_l b_{kl}b_{lk}. \tag{3.3.29}$$

Thus, $b_{kl}b_{lk}$ lies in the center. A similar argument using the adjoint braid identity, equation 3.3.6, yields the computation

$$b_{lk}b_{kl}c_l = b_{lk}c_k b_{kl} \tag{3.3.30}$$

$$= c_l b_{lk}b_{kl}, \tag{3.3.31}$$

and

$$b_{lk}b_{kl}c_k = q\, b_{lk}c_k^2 c_l^{-1}b_{kl} \tag{3.3.32}$$

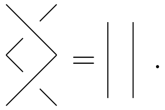
$$= c_k b_{lk}b_{kl}, \tag{3.3.33}$$

so $b_{lk}b_{kl}$ lies in the center as well.

We now need to compute the constant terms for $b_{kl}b_{lk}$ and $b_{lk}b_{kl}$. A direct computation shows that $b_{kl}b_{lk}$ has the constant term $\frac{1}{N}\sum_{i=0}^{N-1}(c_k^i c_l^{-i})(c_l^i c_k^{-i}) = 1$. Similarly, $b_{lk}b_{kl}$ has the constant term $\frac{1}{N}\sum_{i=0}^{N-1}(c_l^i c_k^{-i})(c_k^i c_l^{-i}) = 1$. Thus, applying proposition 3.3.3 in the case $x = b_{kl}b_{lk}$

and $y = 1$, we obtain that $b_{kl}b_{lk} = 1$. Similarly, again applying proposition 3.3.3 and setting $x = b_{lk}b_{kl}$ and $y = 1$, we obtain that $b_{lk}b_{kl} = 1$, concluding the proof. □

The corresponding graphical identity for unitarity, for the special case $n = 1$ (only two generators), $b_{21}b_{12} = b_{12}b_{21}$, is



(3.3.34)

Analogous graphical identities hold for $b_{k,k+1}$ and for general n, where one puts more strands to the left and right of the above diagram. Again, we emphasize the requirement of having a diagram being represented by all strands. Hence, the above diagram does *not* represent the unitarity condition for all b_{kl}, but merely for b_{12}.

In fact, we can now generalize the above unitarity condition extends to braid elements with no graphical interpretation at all:

Corollary 3.3.13.

$$b_{kl}b_{lk} = b_{lk}b_{kl} = 1 \tag{3.3.35}$$

for all $k \neq l$ in the set $\{1, 2, \ldots, 2n\}$.

Proof. Suppose without loss of generality that $k < l$, and consider the isomorphism of subalgebras $\langle c_1, c_2\rangle$ and $\langle c_k, c_l\rangle$ given by the linear mapping φ satisfying $\varphi(c_1^a c_2^b) := c_k^a c_l^b$, defining φ by its action on a basis for the subalgebra $\langle c_1, c_2\rangle$. This is an isomorphism since $\varphi((c_1^a c_2^b)(c_1^i c_2^j)) = \varphi(q^{-bi} c_1^{a+i} c_2^{b+j}) = q^{-bi} c_k^{a+i} c_l^{b+j} = c_k^a c_l^b c_k^i c_l^j = \varphi(c_1^a c_2^b)\varphi(c_1^i c_2^j)$, and the map is invertible. By double distributivity of multiplication in the two subalgebras, the mapping extends to a homomorphism, and thus is an isomorphism. The isomorphism maps $b_{12}b_{21}$ to $b_{kl}b_{lk}$ and 1 to 1, so we obtain that $b_{kl}b_{lk} = 1$. Similarly, $b_{lk}b_{kl} = 1$.

□

The above proof of proposition 3.3.12 may seem slightly over-kill, since we could have also expanded the product of b_{kl} and b_{lk}, and performed the double sum. The strength (and elegance) of the method becomes more apparent when one deals with more complicated products, which is what we take up next.

Yang-Baxter Equation and Braid Group Realization

We now give one of the main results of this chapter, which is an explicit algebraic proof of a Yang-Baxter equation, using the golden rule and a systematic application of the master braid and adjoint braid identities. The Yang-Baxter equation [46] reads as $ABA = BAB$ and is what is known as a braid relation. More formally, we will establish the *braid relations* satisfied by the braid group generated by the $b_{k,k+1}$'s. The braid group, introduced by Artin[1], is defined to be the object

$$B_L = \langle \sigma_1, \ldots, \sigma_{L-1} | \sigma_k \sigma_{k+1} \sigma_k = \sigma_{k+1} \sigma_k \sigma_{k+1}, \sigma_k \sigma_l = \sigma_l \sigma_k \text{ if } |k-l| \geq 2 \rangle. \tag{3.3.36}$$

We need to show that, setting $\sigma_k = b_{k,k+1}$ for $k = 1, 2, \cdots, 2n-1$, these σ_k's satisfy the relations for the braid group generators.

We first present a proof of a special case of the Yang-Baxter equation, specialized to a generalized Clifford algebra with three generators c_1, c_2, c_3:

Proposition 3.3.14 (Special Case of the Yang-Baxter Equation)**.**

$$b_{12} b_{23} b_{12} = b_{23} b_{12} b_{23} \tag{3.3.37}$$

Proof. Since the braid elements are unitary, it suffices to prove the assertion that $b_{32} b_{21} b_{32} b_{12} b_{23} b_{12}$ lies in the center and that the constant of proportionality between $b_{12} b_{23} b_{12}$ and $b_{23} b_{12} b_{23}$ is 1. By Proposition 3.3.4, to show that $b_{32} b_{21} b_{32} b_{12} b_{23} b_{12}$ lies in the center, we just need to show that it commutes with c_k for all $k = 1, 2, \cdots, 2n$. Clearly, for $k > 3$,

$b_{32}b_{21}b_{32}b_{12}b_{23}b_{12}$ commutes with c_k, since each braid element commutes with c_k. So we want to do case analysis for $k = 1, 2, 3$. For $k = 1$,

$$\begin{aligned} b_{32}b_{21}b_{32}b_{12}b_{23}b_{12}c_1 &= qb_{32}b_{21}b_{32}b_{12}b_{23}c_1^2c_2^{-1}b_{12} && (3.3.38) \\ &= q^2b_{32}b_{21}b_{32}b_{12}c_1^2c_2^{-2}c_3b_{23}b_{12} && (3.3.39) \\ &= q^2b_{32}b_{21}b_{32}c_1^2c_2^{-2}c_3b_{12}b_{23}b_{12} && (3.3.40) \end{aligned}$$

after applying the master braid identity, Proposition 3.3.5 thrice and using Lemma 3.3.8. Applying the adjoint braid identity thrice (equation 3.3.6) then yields

$$\begin{aligned} q^2b_{32}b_{21}b_{32}c_1^2c_2^{-2}c_3b_{12}b_{23}b_{12} &= qb_{32}b_{21}c_1^2c_2^{-1}b_{32}b_{12}b_{23}b_{12} && (3.3.41) \\ &= b_{32}c_1b_{21}b_{32}b_{12}b_{23}b_{12} && (3.3.42) \\ &= c_1b_{32}b_{21}b_{32}b_{12}b_{23}b_{12}, && (3.3.43) \end{aligned}$$

as desired. The cases $k = 2$, $k = 3$ are similarly shown to satisfy

$$b_{32}b_{21}b_{32}b_{12}b_{23}b_{12}c_k = c_kb_{32}b_{21}b_{32}b_{12}b_{23}b_{12} \qquad (3.3.44)$$

in like manner. Thus, we conclude that $b_{32}b_{21}b_{32}b_{12}b_{23}b_{12}$ lies in the center.

It remains to show that the constant of proportionality between $b_{12}b_{23}b_{12}$ and $b_{23}b_{12}b_{23}$ is 1. First focus on the constant terms. Since $b_{kl} = \frac{\omega^{1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} c_k^i c_l^{-i}$, it suffices to compare the constant terms of $\sum_{i,j,k=0}^{N-1}(c_1^ic_2^{-i})(c_2^jc_3^{-j})(c_1^kc_2^{-k})$ and $\sum_{i,j,k=0}^{N-1}(c_2^ic_3^{-i})(c_1^jc_2^{-j})(c_2^kc_3^{-k})$. Note that in the first sum, the constant term only includes terms with $i + k = 0$ and $j = 0$, so the constant is given by $\sum_{i=0}^{N-1}(c_1^ic_2^{-i})(c_1^{-i}c_2^i) = \sum_{i=0}^{N-1} q^{-i^2}$. In the second sum, the constant term only includes terms with $j = 0$ and $i + k = 0$, so the constant is given by $\sum_{i=0}^{N-1}(c_2^ic_3^{-i})(c_2^{-i}c_3^i) = \sum_{i=0}^{N-1} q^{-i^2}$. Clearly the constant terms agree. However, this is not sufficient to conclude the constant of proportionality is 1, since the constant term may vanish. In fact, for $N = 2 \pmod 4$, it does vanish, while it does not vanish for other N. This fact is due to the following formulas corresponding to Gauss' classical result for quadratic sums, which are tabulated in [14]:

$$\sum_{k=0}^{n-1} \sin\left(\frac{2\pi k^2}{n}\right) = \frac{\sqrt{n}}{2}\left(1+\cos(n\pi/2)-\sin(n\pi/2)\right) \tag{3.3.45}$$

$$\sum_{k=0}^{n-1} \cos\left(\frac{2\pi k^2}{n}\right) = \frac{\sqrt{n}}{2}\left(1+\cos(n\pi/2)+\sin(n\pi/2)\right) \tag{3.3.46}$$

Applying these formulas to $\sum_{i=0}^{N-1} q^{-i^2} = \sum_{k=0}^{N-1} \exp -2\pi i k^2/N$ yields that the real part of the sum vanishes if $1 + \cos(N\pi/2) + \sin(N\pi/2)$ vanishes, and the imaginary part vanishes if $1+\cos(N\pi/2)-\sin(N\pi/2)$ vanishes. Thus, we require that $\cos(N\pi/2) = -1$ and $\sin(N\pi/2) = 0$, so $N\pi/2 = \pi + 2m\pi$ and $N\pi/2 = l\pi$, i.e. $N = 2+4m$ and $N = 2l$, i.e. $N = 2 \pmod 4$. This shows that the constant term does not vanish unless $N = 2 \pmod 4$.

Now focus on the term with $c_2c_3^{-1}$. In the first sum, this term is $\left(\sum_{i=0}^{N-1} q^{i-i^2}\right) c_2c_3^{-1}$. In the second sum, this term is $\sum_{i,k=0}^{N-1}(c_2^i c_3^{-i})(c_2^{1-i}c_3^{i-1}) = \left(\sum_{i=0}^{N-1} q^{i-i^2}\right) c_2c_3^{-1}$, so the two terms are identical. The multiplicative factor $\sum_{i=0}^{N-1} q^{i-i^2} = q^{1/4}\sum_{k=0}^{N-1} q^{-(k-1/2)^2}$, which equals $q^{1/4}\sum_{k=0}^{N-1} e^{-2\pi i(2k-1)^2/4N}$, vanishes only for $N = 0$ (mod 4).[6]

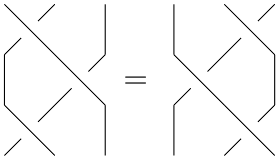
Thus, the constant term and the $c_2c_3^{-1}$ term agree and their sum can never vanish. Hence, we conclude that the constant of proportionality must be 1, as desired.

□

The corresponding graphical identity for the Yang-Baxter equation $b_{12}b_{23}b_{12} = b_{23}b_{12}b_{23}$ is

[6] I have not been able to find the corresponding Gauss sum identity in the literature, but have been able to verify this numerically using Mathematica, which shows that the half-integer-shifted quadratic Gauss sum multiplied by $1/\sqrt{N}q^{-1/4}$ is periodic in N mod 4.

given economically for the algebra with 3 generators c_1, c_2, c_3, as



(3.3.47)

For $2n$ generators, one needs to put $2n-3$ strands to the right of the diagram for completeness.

Similar to the case of the unitarity condition, a more general Yang-Baxter-like equation holds for braid elements which do not admit a graphical interpretation:

Proposition 3.3.15 (General Case of the Yang-Baxter Equation)**.** *Suppose $i<j<k$, then*

$$b_{ij}b_{jk}b_{ij} = b_{jk}b_{ij}b_{jk}. \tag{3.3.48}$$

Proof. We define an isomorphism, this time between the subalgebras $\langle c_1, c_2, c_3\rangle$ and $\langle c_i, c_j, c_k\rangle$. Specifically, define φ by its action on a basis for the subalgebra $\langle c_1, c_2, c_3\rangle$ via $\varphi(c_1^p c_2^q c_3^r) := c_i^p c_j^q c_k^r$ for all $p, q, r \in \{0, 1, \ldots, N-1\}$. Clearly, $\varphi(1) = 1$. Furthermore, φ is a homomorphism since

$$\begin{aligned}\varphi((c_1^u c_2^v c_3^w)(c_1^p c_2^q c_3^r)) &= \alpha\, \varphi(c_1^{u+p} c_2^{v+q} c_3^{w+r}) & (3.3.49)\\ &= \alpha\, c_i^{u+p} c_j^{v+q} c_k^{w+r} & (3.3.50)\\ &= (c_i^u c_j^v c_k^w)(c_i^p c_j^q c_k^r), & (3.3.51)\end{aligned}$$

where α collects all the phase factors from commuting the c's around. It is clear that φ is a one-to-one mapping. Then applying φ to the product formula

$$b_{32}b_{21}b_{32}b_{12}b_{23}b_{12} = 1 \tag{3.3.52}$$

yields

$$b_{kj}b_{ji}b_{kj}b_{ij}b_{jk}b_{ij} = 1, \tag{3.3.53}$$

which implies the desired result by taking the adjoint braids to the other side to become braids.

□

Now we claim that setting $\sigma_k = b_{k,k+1}$ yields the desired braid group.

Proposition 3.3.16. *Set $\sigma_k = b_{k,k+1}$. These elements generate a unitary representation of the braid group*

$$B_{2n} = \langle \sigma_1, \ldots, \sigma_{2n-1} | \sigma_k\sigma_{k+1}\sigma_k = \sigma_{k+1}\sigma_k\sigma_{k+1}, \sigma_k\sigma_l = \sigma_l\sigma_k \text{ if } |k-l| \geq 2\rangle. \tag{3.3.54}$$

Proof. The condition $\sigma_k\sigma_{k+1}\sigma_k = \sigma_{k+1}\sigma_k\sigma_{k+1}$ is true by Proposition 3.3.15 taking the three generators to be c_k, c_{k+1}, c_{k+2}. Meanwhile, the commutation relation $\sigma_k\sigma_l = \sigma_l\sigma_k$ for $|k-l| \geq 2$ follows by applying the linear extension of Proposition 3.3.8. □

Vector Identities for the Algebraic Framework

The fact that the Yang-Baxter equation holds for the elements b_{kl} of the generalized Clifford algebra suggests that perhaps some kind of identities should also hold for the *vectors* with respect to the action of the generalized Clifford algebra. While one might speculate that the vectors (caps and cups) automatically satisfy a kind of an isotopy invariance, taking this to be a built-in axiom (in, e.g., [15]) would most certainly be incompatible with the *algebraic* axiomatic approach we have taken. Any such property ought to be *derived* from the axioms we have presented, not simply taken to be true. Of course, when working with our vectors, we must stick to the representation we have chosen for the generalized Clifford algebra, so our investigation will by necessity proceed from axiom 1 of our algebraic framework.

To those who are familiar with some subfactor theory or category theory, it may be tempting to appeal to these theories as a kind of panacea for isotopy invariance with respect to braidings. However, it must be pointed out that one *cannot* rely on the algebraic results of subfactor theory[7] or tensor category theory[8] approaches for any $N > 2$ (we do not rule out the possibility of an explanation of the $N = 2$ case), as these *do not* cover the case of parastatistics for $N > 2$. In fact, our algebraic framework was devised precisely to enable one to circumvent these theoretical difficulties.

As the methods of proof we developed within the *algebra* in the previous section cannot logically extend to proofs for the *vectors*, we are forced to devise new methods to prove *vector identities*. These methods are independent of the Yang-Baxter equation. It turns out that the results we obtain using these methods include not only graphical identities, but also encompass more general algebraic identities which supersede the graphical identities. In terms of our results, we will show that in a *combinatorial* sense, two basic vector identities give rise to a plethora of identifications between different vectors generated from the ground state by braidings.

First, we begin by proving a general projection-braid identity and two basic vector identities which uniformly apply to a multi-qudit space of an arbitrary number of qudits. The second vector identity, which we call the "slip" move, appears to be new. In their full generality, our two vector identities go beyond a graphical representation. We then show by example that these identities can be thought of as representing *combinatorial* moves that one can perform on braided states without changing the state. We conclude with an example in which we show, *rigorously and without any computations*, that two entangled vector states can be shown to be equal using these combinatorial moves in combination.

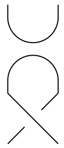
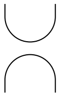
[7] Popa's results on the axiomatization of the standard invariant [35] are for subfactors; one would need a (conjectural) graded subfactor theory, as noted in [15].

[8] There *is* no tensor category here, since the tensor product is not defined between two nonneutral elements of the generalized Clifford algebra. See, e.g., [31], for a nice exposition of tensor category theory.

Thus, an important general result in this section is the introduction of a *reduction procedure*: in many cases, one may reduce the problem of showing equivalence of two different sequences of braidings applied to the ground state, to that of a tractable combinatorial problem, instead of one of explicit algebraic computation. The essential starting point for these vector identities is the identity lemma 3.2.7, and can be thought of as an important reason for using axiom 1 as an axiomatic starting point for the entire theory[9].

We start with the two main combinatorial moves we will need. In this section, as a matter of form, we will draw the diagrams first, and then writing out the algebraic expressions, as the diagrams in the vector representation take on increasing importance for intuition.

Proposition 3.3.17 (Projection-Braid Identity, or the "Twist" Move)**.**

 $= \omega^{-1/2}$  (3.3.55)

Equivalently (by scaling the graphical identity by δ),

$$b_{12}E_1 = \omega^{-1/2}E_1. \tag{3.3.56}$$

More generally,

$$b_{2k-1,2k}E_k = \omega^{-1/2}E_k \tag{3.3.57}$$

for $k = 1, 2, \ldots, n$.

[9] Given how the "rest" of the theory is following from the axiomatic framework, the reader perhaps is gaining more appreciation of why it was so important to separate the algebraic framework into two parts: axioms which allow one to do lots of derivations and algebraic proofs, and a proof of that these axioms are satisfied by an explicit example, i.e. the existence of a consistent vector representation of the generalized Clifford algebra that satisfied both axiom 1 and axiom 2. The division of labor is made clear, and thus each part can be independently rigorously verified.

Proof. By definition,

$$b_{12}E_1 = \frac{\omega^{1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} c_1^i c_2^{-i} E_1. \tag{3.3.58}$$

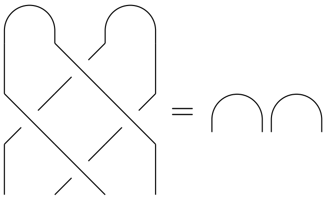
Recall that the axioms for the projectors imply via lemma 3.2.7 that $c_1^a E_1 = \zeta^{a^2} c_2^a E_1$. So the above equality translates to

$$b_{12}E_1 = \frac{\omega^{1/2}}{\sqrt{N}} \left(\sum_{i=0}^{N-1} \zeta^{-i^2} \right) E_1 \tag{3.3.59}$$

$$= \omega^{1/2}\omega^* E_1 = \omega^{-1/2} E_1. \tag{3.3.60}$$

The general statement $b_{2k-1,2k}E_k = \omega^{-1/2}E_k$ follows similarly since the same lemma gives $c_{2k-1}^a E_k = \zeta^{a^2} c_{2k}^a E_k$, which allows for a similar simplification from the sum over generators to a single complex number. □

Proposition 3.3.18 ("Slide" Move)**.**



(3.3.61)

More generally (i.e. for n (where 2n is the number of strands) not necessarily equal to 2),

$$b_{23}b_{34}b_{12}b_{23} \left|\Omega\right\rangle^{\otimes n} = \left|\Omega\right\rangle^{\otimes n}. \tag{3.3.62}$$

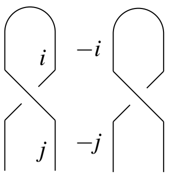
Proof. Graphically, it is wisest to expand the braids on the 2nd and 3rd strands, since we may use existing algebraic graphical identities to simplify the result. This yields

$$b_{23}b_{34}b_{12}b_{23}\,|\Omega\rangle^{\otimes n} = \frac{\omega}{N}\sum_{i,j=0}^{N-1} c_2^j c_3^{-j} b_{34} b_{12} c_2^i c_3^{-i}\,|\Omega\rangle^{\otimes n}. \tag{3.3.63}$$

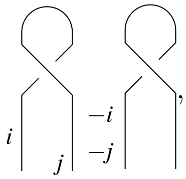
Note that b_{12}, b_{34} commute by linear extension of lemma 3.3.8 so the order doesn't matter.

In terms of a diagram, expanding the middle braids yields

$$\frac{\omega}{N}\sum_{i,j=0}^{N-1}$$



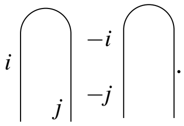
$$= \frac{\omega}{N}\sum_{i,j=0}^{N-1} \zeta^{i^2}$$



, (3.3.64)

where we have applied axiom 1 to bring the charge $-i$ over to the 4th strand, yielding the phase factor ζ^{i^2}, and then commuted it over the braid back to the 3rd strand. Similarly, the charge i can be brought over the braid. Note that no additional phase accumulates, since overall the relative vertical positions of the charges are unchanged. Now apply the twist move in proposition 3.3.17 to get the diagram

$$\frac{1}{N}\sum_{i,j=0}^{N-1} \zeta^{i^2}$$



. (3.3.65)

Following the logic of the diagram, we can perform the same operations to obtain that

$$b_{23}b_{34}b_{12}b_{23}\,|\Omega\rangle^{\otimes n} = \frac{1}{N}\sum_{i,j=0}^{N-1} \zeta^{i^2} c_2^j c_3^{-j} c_1^i c_3^{-i}\,|\Omega\rangle^{\otimes n}. \tag{3.3.66}$$

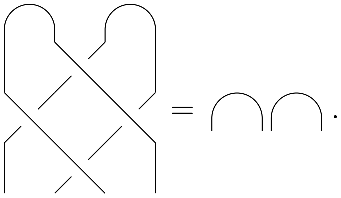
By unitarity of the braids, it suffices to show that $\langle\Omega|^{\otimes n} b_{23}b_{34}b_{12}b_{23}\,|\Omega\rangle^{\otimes n} = 1$.

Note that the projection onto the ground state yields $\frac{1}{N}\sum_{i,j=0}^{N-1}\zeta^{i^2}\,\langle\Omega|^{\otimes n} c_2^j c_3^{-j} c_1^i c_3^{-i}\,|\Omega\rangle^{\otimes n} = \frac{1}{N}\sum_{i,j=0}^{N-1}\zeta^{i^2}\,\langle\Omega|^{\otimes n} c_1^i c_2^j c_3^{-i-j}\,|\Omega\rangle^{\otimes n}$ by commuting c_1^i past the neutral $c_2^j c_3^{-j}$. By orthonormality of $c_2^a c_4^b \left|\Omega\right\rangle^{\otimes n}$ states, and equivalently, the orthonormality of $c_1^a c_3^b \left|\Omega\right\rangle^{\otimes n}$ states, only the terms with $-i-j = 0$ survive. Thus, the sum reduces to $\frac{1}{N}\sum_{i=0}^{N-1} \zeta^{i^2} \left\langle\Omega\right|^{\otimes n} c_1^i c_2^{-i} \left|\Omega\right\rangle^{\otimes n}$, and this is simply equal to 1 by lemma 3.2.7.

Thus, it follows by unitarity of the braids that

$$b_{23}b_{34}b_{12}b_{23} \left|\Omega\right\rangle^{\otimes n} = \left|\Omega\right\rangle^{\otimes n}. \tag{3.3.67}$$

In terms of the diagram, for $n = 2$, we have



(3.3.68)

□

In terms of combinatorial moves, this identity gives us a way to "slide" one cap over the other.

Corollary 3.3.19.

$$b_{12}b_{23} \left|\Omega\right\rangle^{\otimes n} = b_{43}b_{32} \left|\Omega\right\rangle^{\otimes n}. \tag{3.3.69}$$

Proof. By taking b_{34} and b_{23} to the right hand side in Proposition 3.3.18. □

The above "slide" move generalizes to the general result:

Proposition 3.3.20 (General "Slide" Move)**.**

$$b_{2k,2l-1}b_{2l-1,2l}b_{2k-1,2k}b_{2k,2l-1} \left|\Omega\right\rangle^{\otimes n} = \left|\Omega\right\rangle^{\otimes n} \tag{3.3.70}$$

for $k < l$ in $\{1, 2, \ldots, n\}$.

Note that this result does not generally have a graphical interpretation unless $l = k+1$.

Proof. Again, by expansion,

$$b_{2k,2l-1}b_{2l-1,2l}b_{2k-1,2k}b_{2k,2l-1}\left|\Omega\right\rangle^{\otimes n} = \frac{\omega}{N}\sum_{i,j=0}^{N-1} c_{2k}^{j}c_{2l-1}^{-j}b_{2l-1,2l}b_{2k-1,2k}c_{2k}^{i}c_{2l-1}^{-i}\left|\Omega\right\rangle^{\otimes n}. \qquad (3.3.71)$$

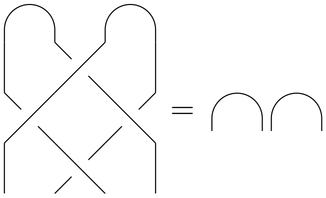
The same proof as before works in this general case since we can apply the braid intertwining identities and also the twist moves (for braids $b_{2l-1,2l}$ and $b_{2k-1,2k}$), and then apply the axioms to simplify the vacuum expectation value. So we conclude that

$$b_{2k,2l-1}b_{2l-1,2l}b_{2k-1,2k}b_{2k,2l-1}\left|\Omega\right\rangle^{\otimes n} = \left|\Omega\right\rangle^{\otimes n}. \qquad (3.3.72)$$

□

We would also like to be able to "slip" one cap in and out of another cap.

Proposition 3.3.21 ("Slip" Move)**.**



(3.3.73)

More generally, for n a positive integer not necessarily 1,

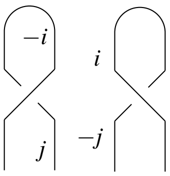
$$b_{23}b_{34}b_{21}b_{32}\left|\Omega\right\rangle^{\otimes n} = \left|\Omega\right\rangle^{\otimes n}.$$

Proof. As demonstrated in the proof of the "slide" move, this kind of proof doesn't depend on n, so long as $n \geq 2$, so let's specialize to $n = 2$ for convenience. The previous proposition gave a clear handle on how to manipulate the algebraic computations, so we'll stick with the algebra.

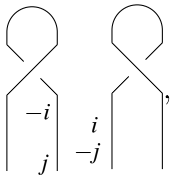
$$b_{23}b_{34}b_{21}b_{32}\left|\Omega\right\rangle^{\otimes n} = \frac{1}{N}\sum_{i,j=0}^{N-1} c_2^j c_3^{-j} b_{34} b_{21} c_3^i c_2^{-i}\left|\Omega\right\rangle^{\otimes n}. \tag{3.3.74}$$

In terms of a diagram, multiplying the state by δ (every cap contributes an extra factor of $\sqrt{\delta}$) yields

$$LHS = \frac{1}{N}\sum_{i,j=0}^{N-1}$$



$$= \frac{1}{N}\sum_{i,j=0}^{N-1}$$

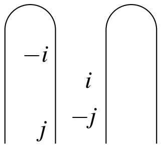


$$, \tag{3.3.75}$$

since the factors of ζ^{i^2} and ζ^{-i^2} cancel.

Undoing the twists yields factors of $\omega^{1/2}$ and $\omega^{-1/2}$, respectively, which cancel, so we are left with

$$LHS = \frac{1}{N}\sum_{i,j=0}^{N-1}$$



$$. \tag{3.3.76}$$

Converting back to the algebraic form, one has

$$b_{23}b_{34}b_{21}b_{32}\left|\Omega\right\rangle^{\otimes n} = \frac{1}{N}\sum_{i,j=0}^{N-1} c_2^j c_3^{-j} c_3^i c_2^{-i}\left|\Omega\right\rangle^{\otimes n}. \tag{3.3.77}$$

Note that the $\left|00\right\rangle$ component has norm 1, since setting $i = j$ yields the $\left|00\right\rangle$ component. Thus, by unitarity of the braid elements, the other basis state projections vanish, so

$$b_{23}b_{34}b_{21}b_{32}\left|\Omega\right\rangle^{\otimes n} = \left|\Omega\right\rangle^{\otimes n} \tag{3.3.78}$$

as desired.

□

As with the "slide" move, there is again an algebraic generalization to braid elements with no graphical interpretation:

Proposition 3.3.22 (General "Slip" Move)**.**

$$b_{2k,2l-1}b_{2l-1,2l}b_{2k,2k-1}b_{2l-1,2k}\left|\Omega\right\rangle^{\otimes n} = \left|\Omega\right\rangle^{\otimes n} \tag{3.3.79}$$

for $k < l$ in $\{1, 2, \ldots, n\}$.

Proof. By expansion,

$$b_{2k,2l-1}b_{2l-1,2l}b_{2k,2k-1}b_{2l-1,2k}\left|\Omega\right\rangle^{\otimes n} = \frac{1}{N}\sum_{i,j=0}^{N-1} c^{j}_{2k}c^{-j}_{2l-1}b_{2l-1,2l}b_{2k,2k-1}c^{i}_{2l-1}c^{-i}_{2k}\left|\Omega\right\rangle^{\otimes n}, \tag{3.3.80}$$

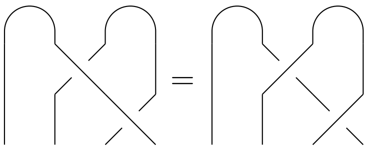
and the same proof follows through as before. □

Corollary 3.3.23.

$$b_{21}b_{32}\left|\Omega\right\rangle^{\otimes n} = b_{43}b_{32}\left|\Omega\right\rangle^{\otimes n} \tag{3.3.81}$$

Proof. By taking b_{23} and b_{34} to the right hand side in proposition 3.3.21. □

Proposition 3.3.24.



(3.3.82)

i.e.

$$b_{34}b_{23}\left|\Omega\right\rangle^{\otimes n} = b_{43}b_{32}\left|\Omega\right\rangle^{\otimes n} \tag{3.3.83}$$

Proof. It suffices to show that $b_{23}b_{34}b_{34}b_{23}\left|\Omega\right\rangle^{\otimes n} = \left|\Omega\right\rangle^{\otimes n}$, using the fact that $b_{jk}b_{kj} = 1$.

Note that this relation does **not** follow immediately from the Yang-Baxter-like equation, since the Yang-Baxter-like equation does not know about the vector structure, or even about the behavior of the ground state.

First recall that proposition 3.3.18 says that the ground state $|\Omega\rangle^{\otimes n}$ is invariant under a "slide" move via

$$|\Omega\rangle^{\otimes n} = b_{23}b_{34}b_{12}b_{23}\,|\Omega\rangle^{\otimes n} \tag{3.3.84}$$

and so we have that

$$b_{32}b_{43}b_{21}b_{32}\,|\Omega\rangle^{\otimes n} = |\Omega\rangle^{\otimes n}\,. \tag{3.3.85}$$

Thus,

$$b_{23}b_{34}b_{34}b_{23}\,|\Omega\rangle^{\otimes n} = b_{23}b_{34}b_{34}b_{23}b_{32}b_{43}b_{21}b_{32}\,|\Omega\rangle^{\otimes n} \tag{3.3.86}$$

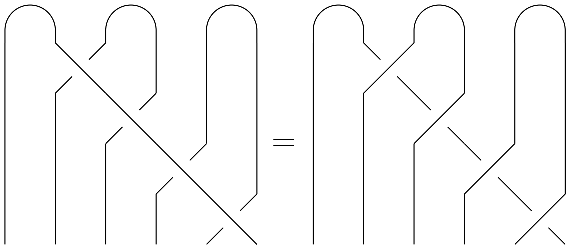
$$= b_{23}b_{34}b_{21}b_{32}\,|\Omega\rangle^{\otimes n} \tag{3.3.87}$$

which equals $|\Omega\rangle^{\otimes n}$ by proposition 3.3.21, as desired.

□

Now we prove something quite nontrivial using the above braiding relations in combination.

Proposition 3.3.25.



(3.3.88)

i.e.

$$b_{56}b_{45}b_{34}b_{23}\,|\Omega\rangle^{\otimes n} = b_{65}b_{54}b_{43}b_{32}\,|\Omega\rangle^{\otimes n}\,. \tag{3.3.89}$$

Proof. Equivalently, we will show that

$$b_{23}b_{34}b_{45}b_{56}b_{56}b_{45}b_{34}b_{23}\,|\Omega\rangle^{\otimes n} = |\Omega\rangle^{\otimes n}\,. \tag{3.3.90}$$

We first substitute $b_{32}b_{43}b_{21}b_{32}\left|\Omega\right\rangle^{\otimes n}$ for $\left|\Omega\right\rangle^{\otimes n}$ following Proposition 3.3.18. This kills off the b_{34} and b_{23} braids and we are left with

$$b_{23}b_{34}b_{45}b_{56}b_{56}b_{45}b_{21}b_{32}\left|\Omega\right\rangle^{\otimes n}. \tag{3.3.91}$$

Now we commute the braids which do not overlap so we get

$$b_{23}b_{34}b_{21}b_{32}b_{45}b_{56}b_{56}b_{45}\left|\Omega\right\rangle^{\otimes n}. \tag{3.3.92}$$

We now substitute $b_{54}b_{65}b_{43}b_{54}\left|\Omega\right\rangle^{\otimes n}$ for $\left|\Omega\right\rangle^{\otimes n}$ to get

$$b_{23}b_{34}b_{21}b_{32}b_{45}b_{56}b_{43}b_{54}\left|\Omega\right\rangle^{\otimes n} \tag{3.3.93}$$

upon braid and adjoint braid cancellation. Now we apply the slip move in reverse to get

$$b_{23}b_{34}b_{21}b_{32}\left|\Omega\right\rangle^{\otimes n} \tag{3.3.94}$$

and then apply the slip move in reverse again to get $\left|\Omega\right\rangle^{\otimes n}$, as desired. □

3.3.4 Significance of the Yang-Baxter Equation Proof

At this point, we wish to elaborate on the significance of our algebraic proof of the Yang-Baxter equation. This subsection is divided into two parts, the first being the particular *local* representation for the $b_{k,k+1}$'s built out of c_i's satisfying the two axioms, and the second being the local representation for an alternate local representation $b_{k,k+1}$'s built out of c_i's not conforming to the explicit representation we constructed to satisfy our two axioms, but still satisfying the relations of a generalized Clifford algebra. By local, we mean that the unitary braid elements are 2-qudit entangling gates or single-qudit gates, in the terminology of quantum circuits; and furthermore, only adjacent qudits are entangled. Via a suitable realization of the generalized Clifford algebras, the latter section provides a solution to an open question in the work of Cobanera and Ortiz [4], regarding the construction of unitary solutions realizing the braid group B_{2n} when the underlying qudit dimension N of the n-qudit system is even, of the "self-dual" form:

$$\rho_{sd}(\sigma_{2i-1}) = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} \alpha_m U_i^{-m}, i = 1, \ldots, n \tag{3.3.95}$$

$$\rho_{sd}(\sigma_{2i}) = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} \beta_m V_i^m V_{i+1}^{-m}, i = 1, \ldots, n-1. \tag{3.3.96}$$

Here, the operators V_k and U_k, termed Weyl generators, are defined by

$$V_k \left|a_1, a_2, \ldots, a_n\right\rangle = \left|a_1, a_2, \ldots, (a_k - 1)(\mathrm{mod}\, N), \ldots, a_n\right\rangle \tag{3.3.97}$$

and

$$U_k \left|a_1, a_2, \ldots, a_n\right\rangle = q^{a_k} \left|a_1, a_2, \ldots, a_k, \ldots, a_n\right\rangle . \tag{3.3.98}$$

V_k and U_k satisfy the commutation relation $V_k U_k = q U_k V_k$ and Weyl generators with different k's commute. The operators V_k, U_k correspond to the generalized Pauli operators X^{-1} (X is bit increment) and Z (Z is phase increment).

Local Representation of the $b_{k,k+1}$'s

We first recall from Ch. 2 the particular realization of the generalized Clifford algebras that we constructed in order to satisfy our two axioms:

$$c_{2k} \left|a_1, a_2, \ldots, a_n\right\rangle = q^{-\sum_{i<k} a_i} \left|a_1, a_2, \ldots, (a_k + 1)(\mathrm{mod}\, N), \ldots, a_n\right\rangle \tag{3.3.99}$$

and

$$c_{2k-1}\left|a_1, a_2, \ldots, a_n\right\rangle = \zeta\, q^{a_k} q^{-\sum_{i<k} a_i}\left|a_1, a_2, \ldots, (a_k+1)(\operatorname{mod} N), \ldots, a_n\right\rangle . \tag{3.3.100}$$

As a brief recap, the main goal of Ch. 2 was to lay down an algebraic framework for deriving general algebraic identities for *vectors*, thus enabling computations with multiple qudits. The *axiomatization* of the requisite properties for a general algebraic framework was the new direction introduced by the work of Ch. 2. To connect to [4], we need to rewrite c_{2k} and c_{2k-1} in terms of the single-qudit generalized Pauli operators, also called Heisenberg-Weyl operators. Such rewriting in terms of single-qudit operators is known as *a* Jordan-Wigner transformation [15]; the particular Jordan-Wigner transformation depends on some conventions about phases and the single-qudit operators chosen and needs to be computed explicitly. Thus, there was some nontriviality in verifying the axioms we presented, since we insisted on particular phases associated with the corresponding c_{2k} and c_{2k-1}'s in axiom 1, which depend in some way on the parity of N.

In our case, we compute the Jordan-Wigner transformation using the single-qudit operators of [4], U_k and V_k above. Thus,

$$c_{2k} = U_1^{-1} U_2^{-1} \cdots U_{k-1}^{-1} V_k^{-1} \tag{3.3.101}$$

and

$$c_{2k-1} = \zeta U_1^{-1} U_2^{-1} \cdots U_{k-1}^{-1} V_k^{-1} U_k. \tag{3.3.102}$$

First, we show that $c_{2k-1}c_{2k}^{-1}$ is 1-local:

Proposition 3.3.26. *$c_{2k-1}c_{2k}^{-1}$ is 1-local, i.e. it only acts on the kth qudit and leaves the rest fixed. In particular, $c_{2k-1}c_{2k}^{-1} = \zeta^{-1}U_k$.*

Proof.

$$c_{2k-1}c_{2k}^{-1} = \left(\zeta U_1^{-1}U_2^{-1}\cdots U_{k-1}^{-1}V_k^{-1}U_k\right)\left(U_1U_2\cdots U_{k-1}V_k\right) \tag{3.3.103}$$

$$= \zeta V_k^{-1}U_kV_k \tag{3.3.104}$$

$$= \zeta q^{-1}V_k^{-1}V_kU_k \tag{3.3.105}$$

$$= \zeta^{-1}U_k. \tag{3.3.106}$$

□

It will be convenient also to have c_{2k+1} and c_{2k+1}^{-1} at our disposal:

$$c_{2k+1} = \zeta U_1^{-1}U_2^{-1}\cdots U_{k-1}^{-1}U_k^{-1}V_{k+1}^{-1}U_{k+1} \tag{3.3.107}$$

$$c_{2k+1}^{-1} = \zeta^{-1}U_1U_2\cdots U_{k-1}U_kU_{k+1}^{-1}V_{k+1}. \tag{3.3.108}$$

Thus, the following combination is 2-local:

Proposition 3.3.27. *$c_{2k}c_{2k+1}^{-1}$ is 2-local, i.e. it only acts on the kth and $(k+1)$th qudits and leaves the rest of them fixed. In particular,*

$$c_{2k}c_{2k+1}^{-1} = \zeta^{-1}V_k^{-1}U_kU_{k+1}^{-1}V_{k+1}. \tag{3.3.109}$$

Proof. Using equations 3.3.101 and 3.3.108,

$$c_{2k}c_{2k+1}^{-1} = \left(U_1^{-1}U_2^{-1}\cdots U_{k-1}^{-1}V_k^{-1}\right)\left(\zeta^{-1}U_1U_2\cdots U_{k-1}U_kU_{k+1}^{-1}V_{k+1}\right) \tag{3.3.110}$$

$$= \zeta^{-1}V_k^{-1}U_kU_{k+1}^{-1}V_{k+1}. \tag{3.3.111}$$

Since U_k, V_k act only on the kth qudit, it follows that $c_{2k}c_{2k+1}^{-1}$ only acts on the kth and $(k+1)$th qudits. □

As a consequence, we obtain the important relation that the braid elements $b_{2k,2k+1}$ are 2-local:

Proposition 3.3.28. *$b_{2k,2k+1}$ is 2-local. In particular,*

$$b_{2k,2k+1} = \frac{\omega^{1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-i^2} W_k^i W_{k+1}^{-i}, \tag{3.3.112}$$

where $W_k = V_k^{-1} U_k$ for each $k \in \{1, 2, \dots, n\}$.

Proof. Recall that

$$b_{kl} := \frac{\omega^{1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} c_k^i c_l^{-i} \tag{3.3.113}$$

defines the braid elements. We will compute $b_{2k,2k+1}$ in terms of U_k, V_k, U_{k+1} and V_{k+1}.

Lemma 3.3.29. *Suppose $c_k c_l = Q c_l c_k$, then $(c_k c_l^{-1})^n = Q^{n(n-1)/2} c_k^n c_l^{-n}$.*

Proof. Suppose $c_k c_l = Q c_l c_k$, then

$$c_k c_l^{-1} = c_k c_l^{N-1} = Q^{N-1} c_l^{N-1} c_k = Q^{-1} c_l^{-1} c_k \tag{3.3.114}$$

. Thus, $c_k^n c_l^{-n}$ in terms of $(c_k c_l^{-1})^n$ is given by

$$\begin{aligned}
(c_k c_l^{-1})^n &= c_k c_l^{-1} c_k c_l^{-1} \cdots c_k c_l^{-1} && (3.3.115)\\
&= Q c_k^2 c_l^{-2} c_k c_l^{-1} \cdots c_k c_l^{-1} && (3.3.116)\\
&= Q^{1+2+\cdots+(n-1)} c_k^n c_l^{-n} && (3.3.117)\\
&= Q^{n(n-1)/2} c_k^n c_l^{-n}. && (3.3.118)
\end{aligned}$$

□

In particular, $c_{2k}c_{2k+1} = qc_{2k+1}c_{2k}$, so

$$c_{2k}^{n}c_{2k+1}^{-n} = q^{-n(n-1)/2}(c_{2k}c_{2k+1}^{-1})^{n}. \tag{3.3.119}$$

Thus, applying Proposition 3.3.27

$$\begin{aligned} b_{2k,2k+1} &= \frac{\omega^{1/2}}{\sqrt{N}}\sum_{i=0}^{N-1} q^{-i(i-1)/2}(c_{2k}c_{2k+1}^{-1})^{i} && (3.3.120)\\ &= \frac{\omega^{1/2}}{\sqrt{N}}\sum_{i=0}^{N-1} q^{-i(i-1)/2}(\zeta^{-1}V_k^{-1}U_kU_{k+1}^{-1}V_{k+1})^{i} && (3.3.121)\\ &= \frac{\omega^{1/2}}{\sqrt{N}}\sum_{i=0}^{N-1} q^{-i(i-1)/2}\zeta^{-i}(V_k^{-1}U_k)^{i}(U_{k+1}^{-1}V_{k+1})^{i} && (3.3.122)\end{aligned}$$

For convenience, set $W_k = V_k^{-1}U_k$ for each k, and rewrite $q = \zeta^2$, yielding

$$\begin{aligned} b_{2k,2k+1} &= \frac{\omega^{1/2}}{\sqrt{N}}\sum_{i=0}^{N-1} \zeta^{-i(i-1)}\zeta^{-i}W_k^{i}W_{k+1}^{-i} && (3.3.123)\\ &= \frac{\omega^{1/2}}{\sqrt{N}}\sum_{i=0}^{N-1} \zeta^{-i^2}W_k^{i}W_{k+1}^{-i}. && (3.3.124)\end{aligned}$$

□

As a consistency check, let us show that this form of the sum for $b_{2k,2k+1}$ is invariant under shifting the index by N. The proof is nontrivial in this generalized Pauli basis, as it requires a cancellation of covariant factors. From a physics perspective, we remark that the cancellation of covariant factors is reminiscent of the construction of scalars in the theory of general relativity.

Proposition 3.3.30 (Cancellation of Covariant Factors). *Each term in the sum $b_{2k,2k+1} = \frac{\omega^{1/2}}{\sqrt{N}}\sum_{i=0}^{N-1}\zeta^{-i^2}W_k^iW_{k+1}^{-i}$ is invariant under shifting the sum index by N. Thus, the sum is invariant under shifting the indexing by arbitrary integers.*

Proof. Note that $W_k^N = -1$ if N is even, since $V_k^N = U_k^N = 1$, $V_k U_k = qU_k V_k$ and we can apply Lemma 3.3.29 for $W_k = V_k^{-1} U_k$ to obtain that $W_k^N = Q^{N(N-1)/2}$. As $V_K^{-1} U_k = q^{-1} U_k V_k^{-1}$, it follows that $Q = q^{-1}$, so $W_k^N = q^{-N(N-1)/2}$. Since q is a primitive Nth root of unity, $q^{-N/2} = -1$, so $W_k^N = (-1)^{(N-1)} = -1$ if N is even. This is not a problem for the invariance of the sum of the braid, under shifting the index, since there are *two* W's, a W_k and a W_{k+1}, so under shifting by N, one acquires two factors of -1, which cancel each other out.

If N is odd, the W factors are invariant under shifting by N since

$$W_k^N = Q^{N(N-1)/2} = (Q^N)^{(N-1)/2} = 1 \tag{3.3.125}$$

since $(N-1)/2$ is an integer. Recall that in both cases, ζ is a square root of q such that $\zeta^{N^2} = 1$ so ζ^{-i^2} is invariant under translations by N. So each term in the sum is invariant under shifting the sum index by N.

Finally, it follows that shifting the indexing (e.g., from 0 to $N-1$, to 1 to N) by arbitrary integers preserves the entire sum, since we can simply maps the terms back into $\mathbb{Z}_N$ by subtracting from or adding to the index of the relevant terms appropriate multiples of N. □

It remains to compute the form of $b_{2k-1,2k}$, which is accomplished with the aid of Lemma 3.3.29 and Proposition 3.3.26:

Proposition 3.3.31. *$b_{2k-1,2k}$ is 1-local. In particular,*

$$b_{2k-1,2k} = \frac{\omega^{1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-i^2} U_k^i \tag{3.3.126}$$

Proof. Applying Lemma 3.3.29 and Proposition 3.3.26:

$$b_{2k-1,2k} == \frac{\omega^{1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} (c_{2k-1} c_{2k}^{-1})^i \tag{3.3.127}$$

$$= \frac{\omega^{1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} \left(\zeta^{-1} U_k\right)^i \tag{3.3.128}$$

$$= \frac{\omega^{1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} \left(\zeta^{-1} U_k\right)^i \tag{3.3.129}$$

$$= \frac{\omega^{1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-i(i-1)} \zeta^{-i} U_k^i \tag{3.3.130}$$

$$= \frac{\omega^{1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-i^2} U_k^i. \tag{3.3.131}$$

□

Note that the form of the braid group generators $b_{k,k+1}$ is *not* in the requisite form of [4] (one may neglect the unimodular phase factor ω in this comparison). It is, however, sufficiently similar, if one replaces V's by W's, that one expects that some adaptation of our approach should work to get solutions in the form desired by [4].

A General Solution to the Open Question of Cobanera and Ortiz

We now solve for braid elements of "self-dual" form given in [4]:

$$\rho_{sd}(\sigma_{2i-1}) = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} \alpha_m U_i^{-m}, i = 1, \ldots, n \tag{3.3.132}$$

$$\rho_{sd}(\sigma_{2i}) = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} \beta_m V_i^m V_{i+1}^{-m}, i = 1, \ldots, n-1. \tag{3.3.133}$$

Our construction of a realization of the braid group B_{2n} out of solutions of the self-dual form will depend on constructing a generalized Clifford algebra out of a particular combination of

U_k's and V_k's. We will need to verify that the resulting particular Jordan-Wigner transformation from U_k's and V_k's indeed satisfies the relations of a generalized Clifford algebra. This verification step is a nontrivial point. In fact, in the original work of [4], the Jordan-Wigner transformation presented, expressing their generators Γ_i and Δ_i (similar to our c_{2k-1} and c_{2k}'s) in terms of the U_i's and V_i's, is incorrect. In odd qudit dimension, they were able to use results of Goldschmidt and Jones (see [10] [19], namely equation 7-6) on braid group representations when N is a power of an odd prime, to find a solution of the self-dual form. The flaw is that for *even* qudit dimension, their Δ_i generators do not satisfy $\Delta_i^N = 1$! The solution, informed by our development of our algebraic framework, is to incorporate the factor of ζ (appearing in our axiom 1) to modify their Jordan-Wigner transformation. Thus, our construction illustrates once more the importance of the axiomatic approach we have pioneered in the first chapter, in which we both isolated the necessary algebraic structure in the two axioms, which depended on the choice of ζ, and justified the validity of the two axioms by an explicit construction[10]. Note that since for N even, ζ can have two possible values, our construction gives rise to two distinct classes of solutions of the self-dual form.

Our starting point is Proposition 3.3.16, which asserts that the $b_{k,k+1}$'s constructed out of the generators c_i, for $i = 1, 2, \ldots, 2n$, generate the braid group B_{2n}. Since this proof only depends on the properties of the generalized Clifford algebra, rather than on a particular representation of the algebra, the proof extends to any construction of generators $c_1, c_2, \ldots, c_{2n-1}, c_{2n}$ out of the Weyl generators U_j and V_j, which satisfies the relations of the generalized Clifford algebra, namely:

$$c_a c_b = q c_b c_a \text{ if } a < b \tag{3.3.134}$$

$$c_a^N = 1 \text{ for any } a = 1, 2, \ldots, 2n. \tag{3.3.135}$$

[10] As a reminder, ζ is a square root of q such that $\zeta^{N^2} = 1$, which guarantees that ζ^{-i^2} is invariant under shifting i by N.

In the following proposition, we construct an automorphism of the generalized Clifford algebra which gives the mapping into the "self-dual" form specified by [4]. We claim that using

$$u_{2k-1} = c_{2k}^{-1} \tag{3.3.136}$$

$$u_{2k} = \zeta c_{2k}^{-1} U_k \tag{3.3.137}$$

yields an automorphism. Since $U_k = \zeta c_{2k-1} c_{2k}^{-1}$, and phases that are powers of q do not affect the GCA relations, we can alternately use the mapping

$$u_{2k-1} = c_{2k}^{-1} \tag{3.3.138}$$

$$u_{2k} = c_{2k-1} c_{2k}^{-2} \tag{3.3.139}$$

Proposition 3.3.32. *Define u_a for $a = 1, 2, \ldots, 2n$ by*

$$u_{2k-1} = c_{2k}^{-1} \tag{3.3.140}$$

$$u_{2k} = c_{2k-1} c_{2k}^{-2} \tag{3.3.141}$$

Then u_a satisfies the relations of a generalized Clifford algebra, namely:

$$u_a u_b = q u_b u_a \text{ if } a < b \tag{3.3.142}$$

$$u_a^N = 1 \text{ for any } a = 1, 2, \ldots, 2n. \tag{3.3.143}$$

Proof. By Lemma 3.2.6, two elements x, y of charge -1, where x is located on generators (graphically, strands) which are left of all the generators (strands) on which y is located, commute past each other with $xy = qyx$, hence $u_a u_b = q u_b u_a$ for $a \in \{2k-1, 2k\}$ and $b \in$

$\{2l-1, 2l\}$, $k < l$. So we simply need to check the commutation of u_{2k-1} and u_{2k}.

$$u_{2k-1}u_{2k} = c_{2k}^{-1}c_{2k-1}c_{2k}^{-2} = qc_{2k-1}c_{2k}^{-1}c_{2k}^{-2} \tag{3.3.144}$$

$$= qu_{2k}u_{2k-1}. \tag{3.3.145}$$

Furthermore,

$$u_{2k-1}^{N} = c_{2k}^{-N} = 1 \tag{3.3.146}$$

$$u_{2k}^{N} = \left(c_{2k-1}c_{2k}^{-2}\right)^{N} = Q^{N(N-1)/2}c_{2k-1}^{N}c_{2k}^{-2N} \tag{3.3.147}$$

by Lemma 3.3.29, where $c_{2k-1}c_{2k}^{-2} = Qc_{2k}^{-2}c_{2k-1}$. It is clear that $Q = q^{-2}$, hence $Q^{N(N-1)/2} = q^{-N(N-1)} = 1$. Thus,

$$u_{2k}^{N} = 1. \tag{3.3.148}$$

Hence we have obtained an automorphism of the generalized Clifford algebra. □

Remark: Note that since one can construct c_{2k-1} and c_{2k} out of products of u_{2k-1} and u_{2k} and their powers and inverses, the size of the basis of the algebra is the same. This is a useful check to see whether the automorphism is actually an automorphism, independently of the relations. Later, in Ch. 5, we will treat the problem of constructing subalgebras of the generalized Clifford algebra, and the question of what conditions can guarantee that the subalgebra has trivial center. There are some similarities between the subalgebra construction problem and the automorphism problem considered here, in that both require one to have a trivial center, in order to prove unitarity and the Yang-Baxter equation.

Proposition 3.3.33. *Define $\beta_{k,l}$ by*

$$\beta_{k,l} = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} u_k^i u_l^{-i}, \tag{3.3.149}$$

where u_a are as above. Then setting $\sigma_k = \beta_{k,k+1}$ for $k = 1, 2, \ldots, 2n-1$ yields a unitary representation of the braid group B_{2n}.

Proof. This follows from the fact that the proof for Proposition 3.3.16, relying on the proof of the Yang-Baxter equation, and the commutation of elements of neutral charge, only depends on the properties of the generalized Clifford algebra as an algebra. Thus, we pass from c_a to u_a and Proposition 3.3.16 still holds. Finally, since there is freedom in the definition of the braid element by a complex phase factor, we may change ω to 1 without affecting unitarity. □

It remains to express the $\beta_{k,k+1}$'s in terms of the Weyl generators V_i,U_i.

Proposition 3.3.34. *$\beta_{2k-1,2k}$ is 1-local and $\beta_{2k,2k+1}$ is 2-local. They are given by*

$$\beta_{2k-1,2k} = \frac{\zeta}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-(i-1)^2} U_k^{-i} \text{ for } k = 1, 2, \ldots, n \tag{3.3.150}$$

$$\beta_{2k,2k+1} = \frac{\zeta}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-(i+1)^2} V_k^i V_{k+1}^{-i} \text{ for } k = 1, 2, \ldots, n-1 \tag{3.3.151}$$

Proof. Applying Lemma 3.3.29:

$$\beta_{2k-1,2k} = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} (u_{2k-1} u_{2k}^{-1})^i \tag{3.3.152}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} (c_{2k}^{-1} (c_{2k-1} c_{2k}^{-2})^{-1})^i \tag{3.3.153}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} (c_{2k}^{-1} c_{2k}^{2} c_{2k-1}^{-1})^i \tag{3.3.154}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} (c_{2k} c_{2k-1}^{-1})^i \tag{3.3.155}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} (c_{2k-1} c_{2k}^{-1})^{-i} \tag{3.3.156}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} (\zeta^{-1} U_k)^{-i} \tag{3.3.157}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-i(i-1)} \zeta^{i} U_k^{-i} \tag{3.3.158}$$

$$= \frac{\zeta}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-(i-1)^2} U_k^{-i} \tag{3.3.159}$$

where we applied Proposition 3.3.26 to simplify $c_{2k-1} c_{2k}^{-1}$.

Applying Lemma 3.3.29 again:

$$\beta_{2k,2k+1} = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} (u_{2k} u_{2k+1}^{-1})^i \tag{3.3.160}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} (c_{2k-1} c_{2k}^{-2} (c_{2k+2}^{-1})^{-1})^i \tag{3.3.161}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} (c_{2k-1} c_{2k}^{-2} c_{2k+2})^i \tag{3.3.162}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} ((\zeta U_1^{-1} U_2^{-1} \cdots U_{k-1}^{-1} V_k^{-1} U_k) \cdot (U_1^{-1} U_2^{-1} \cdots U_{k-1}^{-1} V_k^{-1})^{-2} \tag{3.3.163}$$

$$\cdot (U_1^{-1} U_2^{-1} \cdots U_{k-1}^{-1} U_k^{-1} V_{k+1}^{-1}))^i \tag{3.3.164}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} \zeta^i \left(V_k^{-1} U_k V_k^2 U_k^{-1} V_{k+1}^{-1} \right)^i \tag{3.3.165}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} \zeta^i \left(q^{-2} V_k V_{k+1}^{-1} \right)^i \tag{3.3.166}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} q^{-i(i-1)/2} \zeta^i q^{-2i} V_k^i V_{k+1}^{-i} \tag{3.3.167}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-i(i-1)} \zeta^i \zeta^{-4i} V_k^i V_{k+1}^{-i} \tag{3.3.168}$$

$$= \frac{\zeta}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-(i+1)^2} V_k^i V_{k+1}^{-i}. \tag{3.3.169}$$

□

In the braid elements, the indexing of the coefficients $\zeta^{-(i-1)^2}$ and $\zeta^{-(i+1)^2}$ is quite curious. Partially inspired by the suggestion of Cobanera and Ortiz [4] that there may be many classes of braid group solutions of the self-dual form, we may try to extrapolate the coefficient to have different indexing. In particular, we may use the fact that the relations of the generators forming the generalized Clifford algebra are preserved under the scaling of generators c_a and c_b

by factors of q to generate different coefficients in the self-dual solutions. This appears to be related to a choice of **gauge** on each generator. Let us define $w_a(r_1, r_2, \dots, r_{2n})$ by

$$w_a = q^{r_a} u_a, \tag{3.3.170}$$

where $r_a \in \mathbb{Z}_N$. Then the w_a's again form a generalized Clifford algebra. Then the new braid elements $\gamma_{k,k+1}$ are given by the following proposition:

Proposition 3.3.35.

$$\gamma_{2k-1,2k+1} = \frac{\zeta^{(r_{2k}-r_{2k-1}-1)^2}}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-(i+(r_{2k}-r_{2k-1}-1))^2} U_k^{-i} \quad \textit{for } k = 1, 2, \dots, n \tag{3.3.171}$$

$$\gamma_{2k,2k+1} = \frac{\zeta^{(1+r_{2k+1}-r_{2k})^2}}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-(i+(1+r_{2k+1}-r_{2k}))^2} V_k^i V_{k+1}^{-i} \quad \textit{for } k = 1, 2, \dots, n-1. \tag{3.3.172}$$

Proof. We simply need to add in the rescaling factors induced in by the rescaling of the generators by phase factors:

$$\gamma_{2k-1,2k} = \frac{\zeta}{\sqrt{N}} \sum_{i=0}^{N-1} (q^{r_{2k-1}} q^{-r_{2k}})^i \zeta^{-(i-1)^2} U_k^{-i} \tag{3.3.173}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{2(r_{2k-1}-r_{2k})i} \zeta^{-i^2+2i} U_k^{-i} \tag{3.3.174}$$

$$= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-(i^2+2(r_{2k}-r_{2k-1}-1)i)} U_k^{-i} \tag{3.3.175}$$

$$= \frac{\zeta^{(r_{2k}-r_{2k-1}-1)^2}}{\sqrt{N}} \sum_{i=0}^{N-1} \zeta^{-(i+(r_{2k}-r_{2k-1}-1))^2} U_k^{-i}. \tag{3.3.176}$$

$$\gamma_{2k,2k+1} = \frac{\zeta}{\sqrt{N}}\sum_{i=0}^{N-1}(q^{r_{2k}}q^{-r_{2k+1}})^i\zeta^{-(i+1)^2}V_k^iV_{k+1}^{-i} \tag{3.3.177}$$

$$= \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}\zeta^{2(r_{2k}-r_{2k+1})i}\zeta^{-i^2-2i}V_k^iV_{k+1}^{-i} \tag{3.3.178}$$

$$= \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}\zeta^{-(i^2+2(1+r_{2k+1}-r_{2k})i)}V_k^iV_{k+1}^{-i} \tag{3.3.179}$$

$$= \frac{\zeta^{(1+r_{2k+1}-r_{2k})^2}}{\sqrt{N}}\sum_{i=0}^{N-1}\zeta^{-(i+(1+r_{2k+1}-r_{2k}))^2}V_k^iV_{k+1}^{-i}. \tag{3.3.180}$$

□

Since the phase of each braid element does not affect the braid group relations, it follows that up to phase, the set of self-dual braid group solutions that we have obtained is indexed by a $2n$-dimensional vector $(r_1, r_2, \dots, r_{2n})$ in $\mathbb{Z}_N^{2n}$. Thus, using a particular *automorphism* of the generalized Clifford algebra and the *gauge symmetry* for each generator of the generalized Clifford algebra, we have obtained, from our proof of the Yang-Baxter equation and the related braid group construction, a general set of solutions to the braid group satisfying the "self-dual" form of Cobanera and Ortiz [4], which works for both odd and even N ($N \geq 2$).

From a quantum computation standpoint, the braid elements are 2-local, and hence it is feasible that one might try to implement these gates. In fact, from the commutation relations 3.3.5 between the braid elements and the elements c_a, and the representation of c_a's in terms of the generalized Pauli operators V_k and U_k from equations 3.3.101 and 3.3.102, it is further evident that they *almost* normalize the generalized Pauli group on n qudits, the *almost* being due to the extra factor of ζ. To see this, simply examine the equation $b_{12}c_1 = qc_1^2c_2^{-1}b_{12}$; c_1 has a prefactor ζ, but c_1^2 has a prefactor of q, so the ζ factor remains. Further, observe that we may recover V_k in terms of ζ's and the generalized Clifford algebra by using the expression for c_{2k} in terms of U_i's and the expression for U_i in terms of c_a's. Thus, we can access the entire generalized Pauli group, which is generated by V_k and U_k's, by appropriate products of generators of the generalized Clifford algebra, combined with appropriate factors of ζ (q is contained in the generalized Pauli group, so it would be redundant to keep track of factors of q). Since these products of c_a's can be commuted past the braid elements to yield again products of c_a's time powers of q, it follows from the representation of any generalized Pauli operator as a product of generators of the algebra up to powers of ζ that these braid elements are *almost* Clifford gates, where the Clifford group [12] refers to the normalizer of the generalized Pauli group within the special unitary group over n qudits of dimension N.

3.4 Explicit Computation of Some Entangled Vector States

This section is devoted to explicit algebraic computations of some entangled vector states, to demonstrate some of the variety of entangled states that can arise by braid element actions. Whereas the previous section was devoted to proof methods for showing that two vector states are equal, it did not resolve the question of what those states were, which is clearly a more complicated matter, from the computational standpoint. In proving vector identities, we were able to cleverly chain together two basic moves, the "slide" and "slip" moves, which enable one to maneuver neighboring caps over and under, as well as in and out of each other. Clearly, different methods are needed for explicit computation of the states.

In this section, we develop computational techniques which enable one to reduce vector state computation in various cases to the evaluation of a single explicit inner product, i.e. a single vacuum expectation value. Thus, the novelty here, compared with [17], for example, which also studies state computations, is that we show that state computation of entangled states using the generalized Clifford algebra is quite doable using purely algebraic methods. In fact, as we demonstrate in the final example, the braiding structures can inform one as to the strategy one should employ to reduce the state computation to the evaluation of a single explicit vacuum expectation value.

The braid elements preserve the charge of states of definite charge under the charge operator C, so there is an extra symmetry. So some algebraic structure may be expected to emerge from the application of braid elements to the ground state, which is neutral.

For example, we have the following identity:

Proposition 3.4.1.

$$b_{34}b_{23}\left|\Omega\right\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}\zeta^{i^2}c_2^i c_3^{-i}\left|\Omega\right\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}q^{i^2}c_2^i c_4^{-i}\left|\Omega\right\rangle^{\otimes n} \tag{3.4.1}$$

Proof. By direct expansion, $b_{34}b_{23}\left|\Omega\right\rangle^{\otimes n} = \frac{\omega}{N}\sum_{i,j=0}^{N-1} c_3^j c_4^{-j} c_2^i c_3^{-i}\left|\Omega\right\rangle^{\otimes n}$. As a prelude to putting the sum in normal order, we put each term into "pairwise" normal order, so $b_{34}b_{23}\left|\Omega\right\rangle^{\otimes n} = \frac{\omega}{N}\sum_{i,j=0}^{N-1} c_2^i(c_3^j c_4^{-j} c_3^{-i})\left|\Omega\right\rangle^{\otimes n}$. Now the action of the c_3 and c_4 elements on the ground state can be combined to yield $q^{-j^2}\zeta^{(j-i)^2}c_4^{-i}\left|\Omega\right\rangle^{\otimes n}$. This is by first shifting c_3's to the right of c_4 and then combining the powers of c_3, convert the c_3's to c_4's via their action on the ground state.

At this point, the sum over j can be explicitly evaluated since

$$\sum_{j=0}^{N-1} q^{-j^2}\zeta^{(j-i)^2} = \sum_{j=0}^{N-1}\zeta^{-(i+j)^2}q^{i^2}. \tag{3.4.2}$$

Summing over j yields $\sqrt{N}\omega^{-1}q^{i^2}$ (since the sum is shift invariant due to the axiom $\zeta^{(i+N)^2} = \zeta^{i^2}$). So we are left with $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} q^{i^2}c_2^i c_4^{-i}\left|\Omega\right\rangle^{\otimes n}$, which equals $\sum_{i=0}^{N-1}\zeta^{i^2}c_2^i c_3^{-i}\left|\Omega\right\rangle^{\otimes n}$ as desired. □

Remark 3.4.2. *Note that if we restrict to the case of the 2-qudit ground state, then up to phase redefinition of the basis, the resulting state is of the form* $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}\left|i,-i\right\rangle$ *(as noted in [16]). More generally, we have (up to phase redefinitions)* $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}\left|i,-i,0,0,\ldots,0\right\rangle$.

There is actually an easier way to get this state algebraically, using b_{42}, one of the nonlocal braids we defined:

Proposition 3.4.3.

$$b_{42} \left|\Omega\right\rangle^{\otimes n} = \omega^{-1/2} b_{34} b_{23} \left|\Omega\right\rangle^{\otimes n} \tag{3.4.3}$$

Proof. Since $b_{42} = \frac{\omega^{-1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} c_4^{-i} c_2^{i} = \frac{\omega^{-1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} q^{i^2} c_2^{i} c_4^{-i}$, if we apply it to $\left|\Omega\right\rangle^{\otimes n}$ we get $\frac{\omega^{-1/2}}{\sqrt{N}} \sum_{i=0}^{N-1} q^{i^2} \zeta^{-i^2} c_2^{i} c_3^{-i} \left|\Omega\right\rangle^{\otimes n}$ by bringing the charge i from the fourth strand over to the third strand using the property of the ground state. Thus,

$$b_{42} \left|\Omega\right\rangle^{\otimes n} = \omega^{-1/2} b_{34} b_{23} \left|\Omega\right\rangle^{\otimes n} \tag{3.4.4}$$

□

We can also get rid of the extra constant factor by the following corollary:

Corollary 3.4.4.

$$b_{42} \left|\Omega\right\rangle^{\otimes n} = b_{34} b_{23} b_{34} \left|\Omega\right\rangle^{\otimes n} \tag{3.4.5}$$

Proof. It follows from $b_{34} \left|\Omega\right\rangle^{\otimes n} = \omega^{-1/2} \left|\Omega\right\rangle^{\otimes n}$ by proposition 3.3.17. □

We now compute the state given by $b_{56} b_{45} b_{34} b_{23} \left|\Omega\right\rangle^{\otimes n}$:

Proposition 3.4.5.

$$b_{56} b_{45} b_{34} b_{23} \left|\Omega\right\rangle^{\otimes n} = \frac{1}{N} \sum_{j,l=0}^{N-1} q^{-jl} q^{l^2+j^2} c_2^{l} c_4^{j-l} c_6^{-j} \left|\Omega\right\rangle^{\otimes n} \tag{3.4.6}$$

Proof. We give a direct computation analogous to that of proposition 3.4.1. Expanding all of the braids yields $\frac{\omega^2}{N^2} \sum_{i,j,k,l=0}^{N-1} c_5^{i} c_6^{-i} c_4^{j} c_5^{-j} c_3^{k} c_4^{-k} c_2^{l} c_3^{-l} \left|\Omega\right\rangle^{\otimes n}$. Our strategy is to put all the terms in "pairwise" normal order, so we get $\frac{\omega^2}{N^2} \sum_{j,l=0}^{N-1} \sum_{i,k=0}^{N-1} q^{-jl} c_2^{l} (c_4^{j} c_3^{k} c_4^{-k} c_3^{-l})(c_5^{i} c_6^{-i} c_5^{-j}) \left|\Omega\right\rangle^{\otimes n}$. Using the property of the ground state under action of the c_{2k-1}'s, we can reduce $(c_5^{i} c_6^{-i} c_5^{-j}) \left|\Omega\right\rangle^{\otimes n}$ to $q^{-i^2} \zeta^{(i-j)^2} c_6^{-j} \left|\Omega\right\rangle^{\otimes n}$, and then reduce $(c_4^{j} c_3^{k} c_4^{-k} c_3^{-l}) \left|\Omega\right\rangle^{\otimes n}$ to $q^{-k^2} \zeta^{(k-l)^2} c_4^{j-l} \left|\Omega\right\rangle^{\otimes n}$. So we are left to evaluate

$$\frac{\omega^2}{N^2}\sum_{j,l} q^{-jl}c_2^l\left(\sum_k q^{-k^2}\zeta^{(k-l)^2}\right)c_4^{j-l}\left(\sum_i q^{-i^2}\zeta^{(i-j)^2}\right)c_6^{-j}\left|\Omega\right\rangle^{\otimes n} \tag{3.4.7}$$

which yields

$$\frac{\omega^2}{N^2}\sum_{j,l} q^{-jl}c_2^l\left(\sqrt{N}\omega^{-1}q^{l^2}\right)c_4^{j-l}\left(\sqrt{N}\omega^{-1}q^{j^2}\right)c_6^{-j}\left|\Omega\right\rangle^{\otimes n} \tag{3.4.8}$$

which is just

$$\frac{1}{N}\sum_{j,l=0}^{N-1} q^{-jl}q^{l^2+j^2}c_2^l c_4^{j-l}c_6^{-j}\left|\Omega\right\rangle^{\otimes n} \tag{3.4.9}$$

as desired.

□

As a simple example, suppose we take $N = 3$, so there are nine terms on the right-hand-side, yielding

$$b_{56}b_{45}b_{34}b_{23}\left|\Omega\right\rangle^{\otimes n} = \frac{1}{3}\sum_{j=0}^{2}\left(q^{j^2}c_4^j c_6^{-j} + q^{-j}q^{1+j^2}c_2c_4^{j-1}c_6^{-j} + q^{-2j}q^{4+j^2}c_2^2c_4^{j-2}c_6^{-j}\right)\left|\Omega\right\rangle^{\otimes n}. \tag{3.4.10}$$

Interestingly, we can write the coefficient term as $\zeta^{a_1^2+a_2^2+a_3^2}$, which allows us to rewrite the sum as

$$\frac{1}{N}\sum_{a_1+a_2+a_3=0 \text{ mod N}} \zeta^{a_1^2+a_2^2+a_3^2}c_2^{a_1}c_4^{a_2}c_6^{a_3}\left|\Omega\right\rangle^{\otimes n}. \tag{3.4.11}$$

Following this pattern, we may conjecture that the general case is given by

$$b_{2k-1,2k}b_{2k-2,2k-1}\cdots b_{34}b_{23}\left|\Omega\right\rangle^{\otimes n} = \frac{1}{N^{(k-1)/2}}\sum_{\sum_{i=1}^k a_i=0}\zeta^{\sum_{i=1}^k a_i^2}c_2^{a_1}c_4^{a_2}\cdots c_{2k}^{a_k}\left|\Omega\right\rangle^{\otimes n}. \tag{3.4.12}$$

Clearly, the case $k = 2$ and $k = 3$ hold. It turns out that this is indeed the case in general:

Proposition 3.4.6. *Suppose $k \leq n$. Then*

$$b_{2k-1,2k}b_{2k-2,2k-1}\cdots b_{34}b_{23}\left|\Omega\right\rangle^{\otimes n} = \frac{1}{N^{(k-1)/2}}\sum_{\sum_{i=1}^{k} a_i=0} \zeta^{\sum_{i=1}^{k} a_i^2} c_2^{a_1}c_4^{a_2}\cdots c_{2k}^{a_k}\left|\Omega\right\rangle^{\otimes n}. \qquad (3.4.13)$$

Equivalently,

$$b_{2k-1,2k}b_{2k-2,2k-1}\cdots b_{34}b_{23}\left|\Omega\right\rangle^{\otimes n} = \frac{1}{N^{(k-1)/2}}\sum_{\sum_{i=1}^{k} a_i=0} c_1^{a_1}c_3^{a_2}\cdots c_{2k-1}^{a_k}\left|\Omega\right\rangle^{\otimes n}. \qquad (3.4.14)$$

Proof. By unitarity of the braid element, it suffices to show that

$$\left\langle\Omega\right|^{\otimes n} c_{2k-1}^{a_k}c_{2k-3}^{a_{k-1}}\cdots c_3^{a_2}c_1^{a_1}b_{2k-1,2k}b_{2k-2,2k-1}\cdots b_{34}b_{23}\left|\Omega\right\rangle^{\otimes n} = \frac{1}{N^{(k-1)/2}} \qquad (3.4.15)$$

whenever $\sum_{i=1}^{k} a_i = 0$. The norm of the sum over these states is already 1, so this would imply that there cannot be components in addition to these neutral states.

First, observe[11] that we can change the $c_1^{a_1}$ to $\zeta^{-a_1^2}c_2^{a_1}$ by commuting past the other c_i's to act on the bra vector and then commuting back to its original position. Then we can commute $c_2^{a_1}$ past the braids until we get $c_2^{a_1}b_{23}\left|\Omega\right\rangle^{\otimes n}$, which is just $b_{23}c_3^{a_1}\left|\Omega\right\rangle^{\otimes n} = b_{23}\zeta^{a_1^2}c_4^{a_1}\left|\Omega\right\rangle^{\otimes n}$. This phase factor cancels the previous $\zeta^{-a_1^2}$ so we are left with the $b_{34}b_{23}c_4^{a_1}\left|\Omega\right\rangle^{\otimes n}$, acted on by a product of c_i's and braids. We can then move $c_4^{a_1}$ past b_{23} and then apply $b_{34}c_4^{a_1} = c_3^{a_1}b_{34}$. After commuting this c_3 past the other braids we finally get

$$\left\langle\Omega\right|^{\otimes n} c_{2k-1}^{a_k}c_{2k-3}^{a_{k-1}}\cdots c_3^{a_2+a_1}b_{2k-1,2k}b_{2k-2,2k-1}\cdots b_{34}b_{23}\left|\Omega\right\rangle^{\otimes n}. \qquad (3.4.16)$$

[11] This series of manipulations is motivated by drawing the diagram for this vacuum expectation value, and trying to transfer the charge on the first strand over to the third strand.

Applying this same procedure iteratively, the end result is

$$\langle\Omega|^{\otimes n}\, c_{2k-1}^{a_k+a_{k-1}+\cdots+a_1} b_{2k-1,2k} b_{2k-2,2k-1} \cdots b_{34} b_{23}\, |\Omega\rangle^{\otimes n}\,. \tag{3.4.17}$$

By assumption $a_k + a_{k-1} + \cdots + a_1 = 0$, so we just need to compute

$$\langle\Omega|^{\otimes n}\, b_{2k-1,2k} b_{2k-2,2k-1} \cdots b_{34} b_{23}\, |\Omega\rangle^{\otimes n}\,. \tag{3.4.18}$$

Since $b_{l,l+1} = \frac{\omega^{1/2}}{\sqrt{N}} \sum_{m=0}^{N-1} c_l^m c_{l+1}^{-m}$, the only terms that contribute to the projection onto the ground state are[12] from the constant component of b_{23}, and similarly, the constant component of b_{45}, b_{67}, etc. So we are left to evaluate

$$\frac{\omega^{(k-1)/2}}{N^{(k-1)/2}} \langle\Omega|^{\otimes n}\, b_{2k-1,2k} b_{2k-3,2k-2} b_{2k-5,2k-4} \cdots b_{34}\, |\Omega\rangle^{\otimes n}\,. \tag{3.4.19}$$

Applying the twist move $k-1$ times to get rid of the braids yields $\omega^{-(k-1)/2}$, so this expression evaluates to $\frac{1}{N^{(k-1)/2}}$, as desired.

□

Remark 3.4.7. *As seen in numerous computations for vector states, the key is to latch onto a symmetry (which may be more readily deduced from the* ***diagram****) of the vector state under the action of a neutral product of generators c_{2k-1} (which act on the vacuum state to form a basis; it is important that we project onto a basis). For a complete set of such symmetries (i.e. enough so that the square norm of the sum of projections onto the corresponding states is 1), the computation of a normalized vector state reduces to the computation of the projection onto a single vector state. Thus, in the end, only one explicit computation (expanding braid elements) must be performed.*

[12] This fact is justified by the axiom that the $c_2^{a_1} c_4^{a_2} \cdots c_{2n}^{a_n} |\Omega\rangle^{\otimes n}$ form a basis. Drawing the diagram for the expanded braid sums makes the deduction apparent.

3.5 Conclusion

In this chapter, we showed that the algebraic framework we developed in [24] allows us to construct a purely definitional graphical calculus for multi-qudit computations with the generalized Clifford algebra. Using purely algebraic methods, we established many graphical and beyond graphical identities of the representation of generalized Clifford algebras considered in the previous chapter, including a novel algebraic proof of a Yang-Baxter equation and a construction of a corresponding braid group representation. Our algebraic proof also enabled a resolution of an open problem in [4] on the construction of self-dual braid group representations for N even. We also derived several new identities for the braid elements, which are key to our proofs. In terms of physics, we connected these braid identities to physics by showing the presence of a conserved charge. Furthermore, we demonstrated that in many cases, the verification of involved vector identities can be reduced to the combinatorial application of two basic vector identities. Finally, we showed how to explicitly compute various vector states in an efficient manner using algebraic methods.

From a practical standpoint, a coherent and self-contained algebraic framework for working with GCAs, as presented in the previous chapter, is the first step toward using symbolic algebra methods, such as Mathematica, to simplify complicated multi-qudit computations using GCA representations. In this chapter, we have provided many new algebraic tools at an operator and vector level, which provide the next crucial step in this endeavor.

4

Quantum channels on group algebras

In this chapter[1], we introduce a new decomposition of quantum channels acting on group algebras, which we term Kraus-like operator decompositions (Kraus-like decompositions for short). An important motivation for this new decomposition is a general nonexistence result that we show for Kraus operator decompositions for quantum channels in this setting. We show that the notion of *convex* Kraus-like operator decompositions (in which the coefficients in the sum decomposition are nonnegative and satisfy a sum rule) that are induced by the ir-

[1] This chapter is adapted from the joint work [27] by the dissertation author and Jonathan Boretsky, a graduate student in the mathematics department at Harvard University.

reducible characters of a finite group is equivalent to the notion of a conditionally negative-definite length when the length is a class function. For a general finite group G, we prove a stability condition which shows that if the semigroup associated with a length has a convex Kraus-like operator decomposition for all $t > 0$ small enough, then it has a convex Kraus-like operator decomposition for all time $t > 0$. Using the stability condition, we show that for a general finite group, conditional negativity of the length function is equivalent to a set of semidefinite linear constraints on the length function. By Schoenberg's theorem [38], our result implies that in the group algebra setting, a semigroup P_t induced by a length function which is a class function is a *quantum channel* for all $t \geq 0$ if and only if it possesses a convex Kraus-like operator decomposition for all $t > 0$.

4.1 Introduction

The notion of a completely positive, trace-preserving map (CPTP map), also called a *quantum channel*, is important in a variety of areas, including quantum information theory and the study of various inequalities for operator algebras. Quantum channels are often studied in particular mathematical settings, such as full matrix algebras or other particular kinds of C^* algebras. The setting of full matrix algebras is of particular importance in quantum information theory via the study of finite-dimensional density matrices and their properties (with respect to norms, entropies, etc.). In such a situation, quantum channels are characterized by the well-known Kraus operator decomposition theorem [40][3][34].

In this article, we specialize to the particular case of group algebras where the underlying group is finite[2]. Quantum channels in the group algebra setting possess similar desirable properties as those in the full matrix algebra setting, and thus are of independent interest. For example, the interpolation theory of Uhlmann [42] extends the monotonicity of the relative en-

[2] The group algebra setting has previously been studied in quantum computation in Kitaev's quantum double model for finite groups [22] (see [7] for recent results in this direction).

tropy under identity-preserving completely positive maps from the usual matrix algebra setting to arbitrary $*$-algebras, which contains group algebras as a special case. We prove a nonexistence result for a Kraus operator decomposition of the quantum channel in terms of Kraus operators lying within the group algebra. This motivates us to introduce operators which allow one to decompose certain quantum channels acting on the group algebra. The decomposition we introduce involves a sum over operators which come with real-valued coefficients. Much as the work of Choi [3] shows that the existence of a Kraus operator decomposition in the matrix algebra case implies that the corresponding linear mapping is a quantum channel, we will obtain a result in the group algebra case showing that, for particular naturally arising operator semigroups P_t, if a decomposition of P_t in terms of the operators we introduced satisfies a positivity condition on the coefficients, then the elements of the semigroup are quantum channels for all $t \geq 0$. Hence, we term these operators *Kraus-like operators* and the corresponding decompositions *Kraus-like operator decompositions*. We further define *convex* Kraus-like operator decompositions to be those in which the coefficients in the sum decomposition are nonnegative and satisfy a particular sum rule, which we will discuss explicitly later.

Based on Schoenberg's theorem[38], one may observe that the imposition of a conditionally negative-definite length on the finite group underlying the group algebra results in the induced semigroup P_t (specifically, take the semigroup of operators P_t defined by $P_t\lambda(g) = e^{-tl(g)}\lambda(g)$ where $\lambda(g)$ is a multiplier and l is a scalar-valued function on the group, and extend by linearity to all of $\mathcal{L}G$) being a quantum channel for all $t \geq 0$. This fact is not so easily used in general, as one must prove the conditional negative-definite property for a length function. Historically, Haagerup famously proved the conditional negative-definiteness of a particular length function on a free group with finitely many generators [13] (see Lemma 1.2 of the paper). By restricting to length functions which are class functions, and passing to the Kraus-like operator decomposition, we show that the condition of conditional negative-definiteness on finite groups can be efficiently verified by checking a number of semidefinite linear constraints on the length function. We show that the latter is a necessary and sufficient condition for conditional negative-definiteness, and thus for the semigroup to be a quantum channel for all $t \geq 0$.

The choice of multipliers in our framework is canonical, as we induce the multipliers by the characters of the finite group upon which the group algebra is built. This enables us to use representation theory of finite groups to achieve our results.

In terms of our proof method, for a general finite group G, in order to obtain our semi-definite linear constraints, we prove a stability condition which shows that if the semigroup associated with a length has a convex Kraus-like operator decomposition for all $t > 0$ small enough, then it has a convex Kraus-like operator decomposition for all time $t > 0$. Thus, to obtain global positivity of the coefficients, it suffices to check positivity near $t = 0^+$, which reduces to a bound on the derivatives. This derivative bound is what yields the semi-definite linear constraints.

4.2 Definitions

The main objects we are working with in this chapter are the left regular representation of a finite group G, and a semigroup acting on the elements in the left regular representation. Later in this section, we will find it useful to restrict to semigroups which are induced by conditionally negative-definite length functions on G, in a way to be precisely defined.

Definition 4.2.1 (Left Regular Representation)**.** *Given a group G, let $\mathcal{F}G$ be the vector space of complex-valued functions on G. We denote by λ the* ***left regular representation*** *of G, which acts on $\mathcal{F}G$ by: $(\lambda(g)f)(h) = f(hg^{-1})$ for $g \in G$ and $f \in \mathcal{F}G$. Denote the $\mathbb{C}-$linear span of $\{\lambda(g)\}_{g\in G}$ by $\mathcal{L}G$.*

As it is a property we will use repeatedly, we emphasize that by definition of a representation, for each g, h in G, we have the equality $\lambda(g)\lambda(h) = \lambda(gh)$ of operators on $\mathcal{F}G$.

Recall the standard inner product on $\mathcal{F}G$, given by $\langle f, h\rangle_{\mathcal{F}G} = \sum_{g\in G}\overline{f(g)}h(g)$ for $f, h \in \mathcal{F}G$. The space $\mathcal{L}G$ also comes with a natural inner product. Let δ_e be the function on G defined by $\delta_e(g) = \delta_{g=e}$. Then, we define $\langle x, y\rangle_{\mathcal{L}G} = \langle \delta_e, x^* y\, \delta_e\rangle_{\mathcal{F}G}$, where the $*$ operation is defined on $\mathcal{L}G$ antilinearly with $\sum_i \alpha_i\lambda(g_i) \mapsto \sum_i \bar{\alpha}_i\lambda(g_i^{-1})$. It is straightforward to verify that this is in fact an inner product and thus, $(\mathcal{L}G, \langle\cdot,\cdot\rangle_{\mathcal{L}G})$ is a Hilbert space.

To define a semigroup on $\mathcal{L}G$, one needs the notion of a length function on G. Following [20], we restrict ourselves to conditionally negative-definite lengths.

Definition 4.2.2. *A* ***length function*** $l : G \to \mathbb{R}$ *on a group G with identity e is a function which satisfies $l(e) = 0$, $l(g) = l(g^{-1})$ and $l(g) \geq 0$ for all g in G.*

If $l(g) > 0$ for all $g \neq e$, then we will call l a *strict* length function.

Definition 4.2.3 ([43])**.** *A length function $l : G \to \mathbb{R}$ is said to be* ***conditionally negative-definite*** *if for any $\alpha_1, \cdots \alpha_n \in \mathbb{C}$ satisfying $\sum_{i=1}^n \alpha_i = 0$ and any $g_1, \cdots, g_n \in G$, one has*

$$\sum_{i,j=1}^{n} \alpha_i\overline{\alpha_j} l(g_i^{-1}g_j) \leq 0. \tag{4.2.1}$$

An important additional assumption we adopt in this work is the assumption that all length functions are class functions, meaning they are constant on conjugacy classes. Symbolically, this means $l(g) = l(h^{-1}gh)$ for any g, h in G. This assumption will be greatly exploited in our results and we will derive new characterizations of these conditionally negative-definite class function lengths.

We consider the semigroup P_t of operators on $\mathcal{L}G$ induced by a length function $l(\cdot)$ which is given on generators of $\mathcal{L}G$ by the action

$$P_t\lambda(g) = e^{-t\,l(g)}\lambda(g), \tag{4.2.2}$$

and extended linearly. Observe that indeed, P_0 acts by the identity and $P_{t_1}P_{t_2} = P_{t_1+t_2}$.

Our goal is to characterize P_t from various perspectives. Our new perspectives on P_t will shed light on a known characterization of P_t [20] presented in the continuation of this section.

Definition 4.2.4. *A Hermitian function $K : G \times G \to \mathbb{C}$ is said to be a* ***positive definite kernel*** *if for any $\alpha_1, \cdots, \alpha_n \in \mathbb{C}$ and any $g_1, \cdots, g_n \in G$, we have*

$$\sum_{i,j=1}^{n} \alpha_i \overline{\alpha_j} K(g_i, g_j) \geq 0. \tag{4.2.3}$$

Schoenberg's theorem provides a characterization of positive definite kernels in terms of conditionally negative-definite lengths:

Theorem 4.2.5 (Schoenberg's Theorem [43])**.** *Let G be a group. A function $l : G \to \mathbb{R}$ satisfying $l(g) = l(g^{-1})$ for all $g \in G$ is conditionally negative definite if and only if the following conditions hold:*

1. *$l(e) = 0$, for e the identity of G, and*
2. *The function $G \times G \to \mathbb{C}$ defined by $(g, h) \mapsto e^{-t\,l(gh^{-1})}$ is positive definite.*

In Proposition 4.2.7, we recall an equivalent characterization of conditionally negative-definite lengths in terms of the notion of complete positivity, which is important in quantum physics and quantum information theory. Recall that a linear map is **positive** if it maps positive elements to positive elements. Following [33],

Definition 4.2.6. *Let $\mathcal{A}$ and $\mathcal{B}$ be C^* algebras, and $\theta : \mathcal{A} \to \mathcal{B}$ be a linear map. The map θ is called* ***completely positive*** *if*

$$\theta \otimes id : \mathcal{A} \otimes Mat_n(\mathbb{C}) \to \mathcal{B} \otimes Mat_n(\mathbb{C}) \tag{4.2.4}$$

is positive for any $n \in \mathbb{N}$.

A consequence of Schoenberg's theorem is that the semigroup P_t is completely positive if and only if $l(\cdot)$ is conditionally negative-definite (stated, but not proved, in [20]). To be complete, we provide a proof:

Proposition 4.2.7. *P_t is completely positive if and only if l is conditionally negative-definite.*

Proof. ($\Leftarrow$) By Schoenberg's theorem, if l is conditionally negative-definite, then $\left(e^{-t\,l(g^{-1}h)}\right)_{g,h\in G}$ is a positive semi-definite matrix. From appendix A of [33], $P_t : \mathcal{L}G \to \mathcal{L}G$ is completely positive if and only if

$$\sum_{i,j=1}^{n} b_i^* P_t(a_i^* a_j) b_j \geq 0 \tag{4.2.5}$$

for any $n \in \mathbb{N}$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathcal{L}G$. We show that the latter holds.

Fix n. Take $a_i = \sum_{g\in G} a_i(g)\lambda(g)$. Then

$$P_t(a_i^* a_j) = \sum_{g,h\in G} a_i(g)^* a_j(h) e^{-t\,l(g^{-1}h)} \lambda(g^{-1}h). \tag{4.2.6}$$

So we want to show that

$$S := \sum_{i,j=1}^{n} \sum_{g,h\in G} b_i^* a_i(g)^* a_j(h) e^{-t\,l(g^{-1}h)} \lambda(g^{-1}h) b_j \tag{4.2.7}$$

is non-negative. We note that this can be rearranged by setting $v_g = \sum_{i=1}^{n} a_i(g)\lambda(g)b_i$. So the sum becomes

$$\sum_{g,h\in G} v_g^* e^{-t\,l(g^{-1}h)} v_h. \tag{4.2.8}$$

Note that since $\left(e^{-t\,l(g^{-1}h)}\right)_{g,h\in G}$ is positive semi-definite, we have that

$$e^{-tl(g^{-1}h)} = \sum_{x\in G} r_x(t) \left(w_x(t)^* w_x(t)\right)_{g,h} \tag{4.2.9}$$

for some matrices $\{w_x(t)|x \in G\}$, and nonnegative numbers $\{r_x(t)|x \in G\}$.

Thus,

$$S = \sum_{g,h\in G} v_g^* \sum_{x\in G} r_x(t) \left(w_x(t)^* w_x(t)\right)_{g,h} v_h \tag{4.2.10}$$

$$= \sum_{x\in G} r_x(t) \sum_{g,h\in G} v_g^* \left(w_x(t)^* w_x(t)\right)_{g,h} v_h \tag{4.2.11}$$

$$= \sum_{x\in G} r_x(t) \sum_{g,h\in G} v_g^* \sum_{m\in G} \left(w_x(t)^*\right)_{g,m} \left(w_x(t)\right)_{m,h} v_h \tag{4.2.12}$$

Set

$$q_{x,m}(t) = \sum_{g\in G} \left(w_x(t)\right)_{m,g} v_g \tag{4.2.13}$$

then

$$S = \sum_{x} r_x(t) \sum_{m\in G} q_{x,m}^*(t) q_{x,m}(t). \tag{4.2.14}$$

Thus, S is positive semi-definite, as desired.

($\Rightarrow$) Conversely, suppose P_t is completely positive. Then, with notation as above, for all $n \in \mathbb{N}$ and $a_1, \cdots, a_n, b_1, \cdots, b_n \in \mathcal{L}G$,

$$S := \sum_{i,j=1}^{n} b_i^* P_t(a_i^* a_j) b_j = \sum_{g,h\in G} v_g^* e^{-t\ell(g^{-1}h)} v_h \geq 0, \tag{4.2.15}$$

where $v_g := \sum_{i=1}^{n} a_i(g)\lambda(g)b_i$. Since this holds for any choice of n, a_i and b_i, we can fix $n = |G|$. Order the elements of G so that $G = \{g_1, \cdots, g_n\}$. Choose $b_i = \lambda(g_i^{-1})$ and choose a_i such that $a_i(g_j) = c_j\delta_{ij}$ for some $c_j \in \mathbb{C}$. Then, for each $j = 1, \cdots n$, $v_{g_j} = c_j\lambda(e)$. This reduces eq. (4.2.15) to

$$\left(\sum_{i,j=1}^{n} \overline{c_i} e^{-t\ell(g_i^{-1}g_j)} c_j\right) \lambda(e) \geq 0, \tag{4.2.16}$$

for any choice of $c_1, \cdots c_n \in \mathbb{C}$. Now we claim that if $A\lambda(e) \geq 0$ with $A \in \mathbb{C}$, then $A \geq 0$. This follows since $\lambda(e)$ acts as the identity, and so its spectrum is just 1, and so the spectrum of $A\lambda(e)$ is just A. Thus, for any choice of $c \in \mathbb{C}^n$, we have

$$\sum_{i,j=1}^{n} \overline{c_i} e^{-t\ell(g_i^{-1} g_j)} c_j \geq 0. \tag{4.2.17}$$

By definition, this means that the matrix $\{e^{-t\ell(g_i^{-1} g_j)}\}_{i,j=1}^n$ is positive semi-definite and so, by Schoenberg's theorem, ℓ is a conditionally negative-definite length. □

Corollary 4.2.8. *P_t is a quantum channel.*

Proof. Since P_t is also trace-preserving, it follows by definition that P_t is a quantum channel [34]. □

4.3 Kraus-Like Operator Decompositions

In quantum information theory, *Kraus operators* are used in sum representations of quantum channels which describe the dynamics of the density matrix of a system [34]. In fact, in the matrix case, quantum channels can be characterized by the existence of a Kraus operator decomposition. Equivalently, one may describe a quantum channel as the result of tracing out a subsystem from a unitary operator acting on a composite system. Conversely, one may always "lift" a quantum channel on a density matrix to a corresponding unitary operator on a larger system, a process known as Stinespring dilation [40].

One of the main questions which drives this work is whether the usual intuition for quantum channels on density matrices extends to those on group algebras. Namely, does one get Kraus operators? And what do they look like?

What we find is that the Kraus operators, if they exist, are certainly not generally elements of the group algebra. This is in direct contrast to the case of quantum channels acting on density matrices, where the Kraus operators are themselves matrices.

This nonexistence result motivates us to look for alternate decompositions of the quantum channel, in the spirit of the Kraus operator decomposition. The main idea is to relax the action of Kraus operators as $E \cdot E^\dagger$ to some linear operator $\sigma\cdot$, where σ acts on $\mathcal{L}G$. We call our new σ's *Kraus-like* operators.

For a suitable choice of σ's, we can obtain an explicit condition on the decomposition of a semigroup P_t induced by a length function l which is also a class function, which determines whether or not P_t is a quantum channel.

4.3.1 An algebraic obstruction result on Kraus operator decompositions

Consider the semigroup P_t, induced by a length l, which acts on the Hilbert space $\mathcal{H} = \mathcal{L}G$. We recall that this is given as the linear extension of:

$$P_t\lambda(g) = e^{-tl(g)}\lambda(g). \tag{4.3.1}$$

A Kraus decomposition of P_t is a decomposition of P_t given by

$$P_t(x) = \sum_i E_i x E_i^\dagger, \tag{4.3.2}$$

where the elements E_i satisfy $\sum_i E_i^\dagger E_i \leq I$ [34]. The E_i are called Kraus operators. For simplicity, we focus only on the case where $\sum_i E_i^\dagger E_i = I$, corresponding to the case where one can dilate P_t to a unitary in the matrix case [34]. In the usual matrix algebra setting for Kraus operator decompositions, quantum information theory, x would be a finite-dimensional density matrix and P_t would be a completely positive map from density matrices to density matrices. The elements E_i would be matrices. For the group algebra setting, it is not *a priori* obvious where the E_i's would live, so we will make some natural assumptions.

Since we are working with group algebras, to employ Kraus operator decompositions, some choices must be made as to the proper identification of terms. The natural mapping, extending the setting of matrix algebras to direct sum of matrix algebras, is to take P_t to map $\mathcal{L}G$ into $\mathcal{L}G$. While one could also embed $\mathcal{L}G$ into a matrix algebra by the regular representation, this is fairly unnatural from the point of respecting the symmetry of the group, as different irreducible representations ought not to interact from a physical perspective.

For a Kraus operator decomposition, since we work in G, it is further natural, or at least convenient, to assume that the E_i's all lie in $\mathcal{L}G$. Note that this is not the most general setting, since if we interpret $\mathcal{L}G$ as a vector space of dimension $|G|$, the dimension of $\mathcal{B}(\mathcal{L}G)$ is $|G|^2$, whereas the embedding of $\mathcal{L}G$ inside $\mathcal{B}(\mathcal{L}G)$ only has dimension $|G|$. So we are deliberately choosing to focus on a smaller space of possible Kraus operators. However, we show that with this simple, and perhaps most natural, choice, we run into issues.

The following proposition shows that a Kraus operator decomposition as described in the previous paragraph is not the right tool for the job at the hand, in the sense that Kraus operator decompositions will not be readily available in many semigroups of interest.

Proposition 4.3.1. *Any finite group G whose group algebra $\mathcal{L}G$ has a non-zero element of the form $\sum_{e \neq g \in G} a_g \lambda(g)$ in its center will not admit a Kraus operator decomposition for the operator P_t induced by a **strict** length function l via equation 4.2.2, in terms of Kraus operators lying in $\mathcal{L}G$.*

In particular, the hypothesis of this proposition holds for the expression $\sum_{e \neq g \in G} \lambda(g) \in \mathcal{L}G$ when G is any nontrivial finite group.

Proof. Let h be an element satisfying the conditions of the proposition. Suppose P_t admits a Kraus decomposition of the form $P_t(x) = \sum_i E_i x E_i^\dagger$, where $E_i \in \mathcal{L}G$. Since $\lambda(e)$ is the identity, it follows that

$$\lambda(e) = \exp(-l(e)t)\lambda(e) = P_t\lambda(e) = \sum_i E_i E_i^\dagger. \tag{4.3.3}$$

Now, consider $P_t(h)$. Since h is in the center, we have

$$P_t(h) = \sum_i E_i h E_i^\dagger = \sum_i E_i E_i^\dagger h = \lambda(e)h = h. \tag{4.3.4}$$

However, by assumption, $h = \sum_{g\neq e} a_g \lambda(g)$, so

$$P_t(h) = \sum_{g\neq e} e^{-l(g)t} a_g \lambda(g) = h = \sum_{g\neq e} a_g \lambda(g). \tag{4.3.5}$$

By the basis property, this implies that $(e^{-l(g)t} - 1)a_g = 0$ for all $g \neq e$ and for all $t \geq 0$. Since for a length function l, $l(g) > 0$ for all $g \neq e$, this implies that $a_g = 0$ for all $g \neq e$. Thus, $h = 0$.

□

Discussion of dilation theorems

Some remarks must be made with respect to the Stinespring dilation theorem [40], and the associated Choi isomorphism theorem [3]. Firstly, the Stinespring dilation theorem still applies in this context of group algebras, but the construction of a dilation is so general as not to yield anything resembling a Kraus operator decomposition. The much sharper construction of Choi applies in the case of a finite-dimensional Hilbert space. When we look at the group algebras, the theorem of Choi is hard to apply directly, for the following reason: Embedding the group algebra $\mathcal{L}G$ into a matrix algebra via the left regular representation is a sparse isometric embedding[3], since the former has a basis set of size $|G|$ whereas the latter has a basis

[3] To see that the embedding is isometric, we can first note that in the case of $\mathbb{Z}_N$, one easily sees that all the elements in the left-regular representation (except the identity) have no fixed points, so $\langle \rho(g), \rho(h) \rangle \quad :=$

set of size $|G|^2$. Thus, our definition of P_t as a completely positive, trace-preserving map on the group algebra $\mathcal{L}G$ does *not* mean that P_t is a completely positive, trace-preserving map on the corresponding *matrix* algebra, because the action of P_t is not even specified for matrices outside of the left regular representation. What one would be looking for instead is some analogue of Choi's isomorphism theorem, which applies to a map which is completely-positive and trace-preserving on a subalgebra of a matrix algebra. Such a kind of *restriction theorem*[4] would be interesting in its own right. Of course, one would be working with objects which are not really quantum channels, but only behave like quantum channels when applied to a subalgebra of the matrix algebra (as justified by Corollary 4.2.8). The corresponding *extension* problem has been considered recently by [44] on an extension result for quantum Markov semigroups (completely positive maps which form a semigroup) defined on a subalgebra to a quantum Markov semigroup over the full matrix algebra.

4.3.2 Kraus-like Operator Decompositions

What is a Kraus-like Operator Decomposition?

The above nonexistence result motivates us to look for a more general decomposition of a semigroup, which *will* exist even when a Kraus operator decomposition in terms of group algebra elements is not available. We introduce the notion of a Kraus-like operator decomposition, which replaces the Kraus form by a multiplier on the group algebra. Under several equivalent hypotheses on the length function, we will be able to show that the coefficients of the decomposition satisfy a sum rule and are positive, hence admitting a possible probabilistic interpretation. In this respect, our motivation is to establish something analogous to the mixed-unitary

$\mathrm{tr}(\rho(g)\rho(h)^\dagger = \mathrm{tr}(\rho(gh^{-1}) = 0$ unless $g = h$. For the general finite group case, an element $\rho(g)$ has an element on the diagonal only if $gh = h$ for some h. But this implies that $g = e$ since all elements are invertible in a group. So no non-identity elements of the left-regular representation have elements on the diagonal. Thus, the embedding is isometric in general.

[4] We are inspired by Stein's restriction conjecture in analysis to use this suggestive vocabulary.

quantum channel for our Kraus-like operator decomposition.

We now present a prototype for what we consider to be a Kraus-like operator decomposition. Consider a decomposition of the operator semigroup P_t into a sum of isometries, rather than taking a sum of $E_i x E_i^\dagger$ operators. Let us show that, at least in a particularly simple example, such a decomposition does in fact exist.

Example 4.3.2. *Let G be an arbitrary group with the length $l(g) = 1 - \delta_{g=e}$ for $g \in G$. Let $p = \frac{1-e^{-t}}{2}$. Define the isometry*

$$\sigma(\lambda(g)) = \begin{cases} -\lambda(g), & g \neq e \\ \lambda(e), & g = e \end{cases} \tag{4.3.6}$$

Then for any $g \in G$, one can easily verify that $P_t(\lambda(g)) = (1-p)\lambda(g) + p\sigma(\lambda(g))$. The $\lambda(g)$ span $\mathcal{L}G$ so this proves that $P_t = (1-p)\mathbb{I} + p\sigma$ as operators on $\mathcal{L}G$.

Let us make a few observations about this decomposition. The coefficients of the two isometries in the decomposition are $(1-p)$ and p. We note that by the definition of p, these are both non-negative numbers for $t \geq 0$. Moreover, they evidently sum to 1.

This is a basic example, but we already see that there is hope that our decomposition might have a probabilistic interpretation. Motivated by this example, we introduce the following notion as an analog to Kraus operator decompositions:

Definition 4.3.3. *For a group G and operator semigroup $P_t : \mathcal{L}G \to \mathcal{L}G$, a* ***Kraus-like operator decomposition*** *of P is a decomposition*

$$P_t = \sum_i p_i(t)\sigma_i \tag{4.3.7}$$

where each operator $\sigma_i : \mathcal{L}G \to \mathcal{L}G$ is diagonal in the basis of left-multipliers $\lambda(g)$, and $p_i(t)$'s are complex-valued functions.

If the $p_i(t)$'s are all nonnegative, and satisfy a sum rule $\sum_i \alpha_i p_i(t) = 1$, for some positive α_i's independent of t, then we say that we have a ***convex Kraus-like operator decomposition****.*

The natural next question is if this sort of decomposition can be generalized to the semigroups generated by other lengths. We will show that, indeed, it can. In fact, for a specific class of naturally arising σ_i operators, we will even be able to describe a condition which classifies precisely which lengths on a given group will yield semigroups with convex Kraus-like operator decompositions.

4.4 Character-Induced Kraus-Like Operator Decompositions

4.4.1 Kraus-like operator decompositions for finite abelian groups

Our next goal is to consider a general abelian group G and think more broadly about when we have a convex Kraus-like operator decomposition.

Fix a finite abelian group G of size n. It is natural to consider maps which are induced by the characters of G. Explicitly, if the characters of G are denoted by $\{\chi_i\}_{i=1}^n$, then we consider the maps which act on generators by $\sigma_i : \lambda(g) \mapsto \chi_i(g)\lambda(g)$ and extend by linearity. Note that since G is abelian, all characters are simply one-dimensional representations. These are, in fact, isometries and the multiplicative structure they inherit from the fact that they are representations will prove useful later.

Let l be any length on G. Note that the characters of a group span the class functions on that group and, in the case of an abelian group where each element is its own conjugacy class, this means that the characters span the complex-valued functions on the group. Thus, we can write P_t as a sum $P_t = \sum_{k=1}^n p_k \sigma_k$ for appropriate p_k. By applying both sides of the previous equation to $\lambda(g)$ for each $g \in G$ and comparing coefficients, one finds that the p_k must satisfy:

$$\sum_{l=1}^{n} \chi_l(g) p_l = \exp(-tl(g)). \tag{4.4.1}$$

Recall that part of our goal in all this is to understand if there is an interpretation of the p_k as probabilities. As we now show, this is equivalent to demanding that $f(g) = \exp(-tl(g))$, as a function of $g \in G$, be of positive type. In other words, we must have that $f(gh^{-1})$ is a positive-definite kernel, when considered as a function of both g and h.

Proposition 4.4.1 (Bochner-like Theorem)**.** *Let G be a finite abelian group of size n with characters $\{\chi_l\}_{l=1}^{n}$, and suppose $f : G \to \mathbb{C}$, and $p \in \mathbb{C}^n$ are related by $f(g) = \sum_{l=1}^{n} p_l \chi_l(g)$ for all $g \in G$.*

Then p is a probability measure on G, that is, $p_i \geq 0$ for all i and $\sum_i p_i = 1$, if and only if $f(gh^{-1})$, considered as a function of $g, h \in G$, is a positive definite kernel, and $f(e) = 1$.

Proof. Note that the positive definiteness of f is equivalent to the non-negativity of the following expression, for any choice of $\phi : G \to \mathbb{C}$:

$$\begin{aligned}\sum_{g\in G}\sum_{h\in G} f(gh^{-1})\phi(g)\phi(h)^* &= \sum_{l=1}^{n} p_l \sum_{g\in G}\sum_{h\in G} \chi_l(gh^{-1})\phi(g)\phi(h)^* \\ =&\sum_{l=1}^{n} p_l \left(\sum_{g\in G}\chi_l(g)\phi(g)\right)\left(\sum_{h\in G}\chi_l(h)\phi(h)\right)^* = \sum_{l=1}^{n} p_l \left|\sum_{g\in G}\chi_l(g)\phi(g)\right|^2,\end{aligned}$$

where the second equality follows from the general fact that $\chi(g^{-1}) = \chi(g)^*$ and also the fact that any representation of an abelian group is 1 dimensional, so the characters of such a group are multiplicative. Note that if each $p_k \geq 0$, then this expression is surely non-negative for any choice of ϕ. On the other hand, if some p_k is not greater than or equal to 0, then set $\phi(g) = \chi_k(g)$. By the orthogonality of characters, this will result in the entire expression failing to be greater than or equal to zero. Thus, we conclude that f is positive definite if and only if each of the $p_l \geq 0$ for all $1 \leq l \leq n$. Additionally, the condition that $\sum_{l=0}^{N-1} p(l) = 1$ is equivalent to the condition that $f(e) = 1$, completing our proof.

□

Our goal was to characterize the lengths l on a finite abelian group G for which we obtain a probability measure p in the convex Kraus-like operator decomposition of the operator semigroup P_t induced by l. Using Schoenberg's theorem, we can easily obtain such a condition.

Proposition 4.4.2. *Let l be any length on a finite abelian group G and let $\{\chi_l\}_{l=1}^{n}$ be the characters of G. Suppose the semigroup P_t is defined by $P_t : \lambda(g) \mapsto e^{-t|g|}\lambda(g)$, which extends linearly to all of $\mathcal{L}G$. Let P_t satisfy $P_t = \sum_{k=1}^{n} p_k \sigma_k$, where $\sigma_k(\lambda(g)) = \chi_k(g)\lambda(g)$ for all $g \in G$. Then p is a probability measure on G if and only if l is a conditionally negative-definite length.*

Proof. This follows by combining the previous proposition with Schoenberg's theorem, which says that l is conditionally negative-definite if and only if $f(gh^{-1}) = \exp(-tl(gh^{-1}))$ is a positive-definite kernel in $g, h \in G$ which satisfies $f(e) = 1$. □

Thus, we have established a nice coherent story for finite abelian groups. We have characterized a large class of lengths on these groups which admit a convex Kraus-like operator decomposition. However, this is hardly satisfying. For one thing, it is not clear whether the relationship between a conditionally negative-definite length and a convex Kraus-like decomposition is an accident or has some more fundamental significance. Moreover, it would be valuable to move this analysis beyond abelian groups. Thus, we explore next the notion of Kraus-like operator decompositions for general finite groups.

4.4.2 Kraus-like decompositions for general finite groups

In the more general setting of finite groups, there are two basic questions we need to answer.

1. What is the appropriate generalization of the Kraus-like operator decomposition to a general finite group G, based on the model we considered for $\mathbb{Z}_N$?
2. What is the corresponding condition for the coefficients p_i arising in the decomposition to be non-negative, or more specifically, for the p_i's to be a probability distribution (at least up to rescaling)?

The answer to the question (1) is that we can simply define multipliers induced by characters in the following way: Since we suppose that l is a class function, P_t acts as a constant multiple of the identity on the left-multipliers $\lambda(g)$ for $g \in C_i$, for each conjugacy class C_i. Accordingly,

$$P_t = \oplus_i \left(e^{-t\,l(C_i)} \otimes 1_{\#C_i} \right), \tag{4.4.2}$$

where $l(C_i)$ is the unique value of the length function on the conjugacy class C_i.

We may also use the irreducible characters χ of the group G, which are themselves class functions, to induce maps with similar direct sum decompositions,

$$\sigma_\chi := \oplus_i \left(\chi(C_i) \otimes 1_{\#C_i} \right). \tag{4.4.3}$$

From the similar forms of these operators, it seems reasonable to study relationships of the form

$$P_t = \sum_\chi p_\chi \sigma_\chi, \tag{4.4.4}$$

for complex numbers p_χ. We call this expression a *character-induced Kraus-like* operator decomposition of the semigroup P_t.

Let $\{\chi_1, \cdots, \chi_m\}$ be the irreducible characters of G. We can quickly determine the coefficients p_j. By applying the map $P_t = \sum_j p_j \sigma_{\chi_j}$ to $\lambda(g)$ for $g \in C_i$ and setting the two sides equal to each other, one obtains, for each i, the equation:

$$\sum_j p_j \chi_{ji} = e^{-t\,l(C_i)} \tag{4.4.5}$$

where $\chi_{ji} = \chi_j(C_i)$. We can consider these as entries of a matrix $\chi := (\chi_{ij})$. Note that χ is simply the character table of the group. With this, we can see eq. (4.4.5) as a matrix equation.

As a preliminary step, we obtain a **sum rule** for the p_i's:

Lemma 4.4.3 (Sum Rule for p_i's)**.**

$$\sum_i p_i \chi_i(e) = 1. \tag{4.4.6}$$

Proof. This follows from equation 4.4.5 applied to the conjugacy class $\{e\}$. □

We can solve for the p_i's by inverting the matrix equation 4.4.5. There is a trick to do this which is well known in the representation theory of groups: If one normalizes the χ_{ji}'s, then one gets a unitary matrix. Namely,

$$\hat{\chi}_{ji} = \chi_{ji} \cdot \frac{\sqrt{\#C_i}}{\sqrt{\#G}} \tag{4.4.7}$$

defines a unitary matrix. Using unitarity, we can solve for the $p_i's$ by applying the adjoint of $\hat{\chi}$ to the matrix equation, and use well known properties of the character, to get that

$$p_i(t) = \sum_j \frac{\sqrt{\#C_j}}{\sqrt{\#G}} e^{-t\,l(C_j)} (\hat{\chi}^\dagger)_{ji} = \sum_j \frac{\#C_j}{\#G} e^{-t\,l(C_j)} \chi^*_{ij}. \tag{4.4.8}$$

To answer question (2), we need to study the convexity of the Kraus-like decomposition. Since we already have a sum rule, we now need to find conditions which ensure that $p_i \geq 0$ for $1 \leq i \leq n$.

Our following theorem gives the answer for question (2):

Theorem 4.4.4. *The character-induced Kraus-like decomposition of P_t under the class function length l is convex if and only if*

$$p_i'(t=0) = -\sum_j \frac{\#C_j}{\#G} l(C_j)\chi_{ij}^* \geq 0 \tag{4.4.9}$$

for all $i \geq 2$.

We split the proof of Theorem 4.4.4 into two parts, necessity and sufficiency.

Proposition 4.4.5 (Necessity)**.** *If the character-induced Kraus-like decomposition of P_t is convex, then*

$$p_i'(t=0) = -\sum_j \frac{\#C_j}{\#G} l(C_j)\chi_{ij}^* \geq 0 \tag{4.4.10}$$

for all $i \geq 2$.

Proof. First observe that since χ_1 is the character for the identity representation, $\chi_1(C_i) = 1 = \chi_{1i}$ for all i, and so by the well known orthogonality of characters,

$$p_i(t=0) = \langle \chi_i, \chi_1 \rangle = \delta_{i1} \tag{4.4.11}$$

where $\langle f, g \rangle := \sum_j \frac{\#C_j}{\#G} f(C_j)^* g(C_j)$ for f, g class functions on G.

Thus, if $p_i(t)$ is always positive, it is necessary that $p_i'(t=0) \geq 0$ for all $i \geq 2$. □

We will next show that this condition is actually sufficient for any finite group, and has a group-theoretical explanation. Before demonstrating the sufficiency of this condition in general, we show how one might go about it in a few specific cases. For the sake of our proofs, we state explicitly the nonnegative bounds for the length, even though it is explicit in the definition. We hope these examples highlight how quickly it becomes difficult to study the inequalities $p_i \geq 0$ due to the interdependency of the p_i.

Sufficiency of $p_i'(0) \geq 0$ for S_3

The character table for S_3 is given by:

$$\chi = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 0 & -1 \\ 1 & -1 & 1 \end{pmatrix} \tag{4.4.12}$$

with $\#C_1 = 1$, $\#C_2 = 3$, $\#C_3 = 2$. This yields

$$\hat{\chi} = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & \sqrt{3} & \sqrt{2} \\ 2 & 0 & -\sqrt{2} \\ 1 & -\sqrt{3} & \sqrt{2} \end{pmatrix} \tag{4.4.13}$$

For convenience, denote $l(C_i)$ by l_i, and take $l_1 = 0$ so that the identity is of length 0. This yields the following equations for the p_i:

$$p_1(t) = \frac{1}{6}\left(1 + 3e^{-tl_2} + 2e^{-tl_3}\right) \tag{4.4.14}$$

$$p_2(t) = \frac{1}{6}\left(2 - 2e^{-tl_3}\right) \tag{4.4.15}$$

$$p_3(t) = \frac{1}{6}\left(1 - 3e^{-tl_2} + 2e^{-tl_3}\right). \tag{4.4.16}$$

Note that p_1, p_2 are clearly non-negative for all $t \geq 0$. It is also automatic that $p_1'(0) \geq 0$ and $p_2'(0) \geq 0$.

It is certainly necessary that $6p_3'(0) = 3l_2 - 2l_3 \geq 0$. This will in fact turn out to be a sufficient condition.

Proposition 4.4.6. *In the set up for S_3 described above, all the p_i are non-negative for all $t \geq 0$ if and only if $l_2 \geq \frac{2}{3}l_3 \geq 0$.*

Proof. The only if direction is clear.

For the if direction, as already noted, for any $t \geq 0$, the non-negativity of p_1 and p_2 is independent of the choice of l_i.

If $l_2 \geq \frac{2}{3}l_3$ we consider 2 cases

1. Suppose $\frac{2}{3}l_3 \leq l_2 \leq l_3$. Then

$$6p_3'(t) = 3l_2e^{-tl_2} - 2l_3e^{-tl_3} \geq (3l_2 - 2l_3)e^{-tl_3} \geq 0.$$

   Thus, $p_3(0) = 0$ and $p_3(t)$ is increasing, so $p_3(t) \geq 0$ for all $t \geq 0$.

2. Suppose $l_2 \geq l_3$. Then $6p_3(t) \geq 1 - 3^{-tl_2} + 2e^{-tl_2} = 1 - e^{-tl_2} \geq 0$ for all $t \geq 0$.

□

As an example of what we have just shown, we will evaluate two natural notions of length on the group S_3. Let $|\cdot| = n - \#$ of cycles. Then $l_1 = 3 - 3 = 0$, $l_2 = 3 - 2 = 1$ and $l_3 = 3 - 1 = 2$. Clearly, $(l_1, l_2, l_3) = (0, 1, 2)$ violates the conditions of the above theorem and so it does not yield a probabilistic interpretation of the p_i.

On the other hand, if $|\cdot| = \sqrt{n - \# \text{ of cycles}}$, then $(l_1, l_2, l_3) = (0, 1, \sqrt{2})$ and we do indeed obtain such a probabilistic interpretation.

Sufficiency of $p_i'(0) \geq 0$ for Q_8

The character table for Q_8 is

$$\chi = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 2 & -2 & 0 & 0 & 0 \end{pmatrix} \tag{4.4.17}$$

where the conjugacy classes associated to the columns, in order, have sizes $1, 1, 2, 2$ and 2. This means that

$$\hat{\chi} = \frac{1}{2\sqrt{2}} \begin{pmatrix} 1 & 1 & \sqrt{2} & \sqrt{2} & \sqrt{2} \\ 1 & 1 & \sqrt{2} & -\sqrt{2} & -\sqrt{2} \\ 1 & 1 & -\sqrt{2} & \sqrt{2} & -\sqrt{2} \\ 1 & 1 & -\sqrt{2} & -\sqrt{2} & \sqrt{2} \\ 2 & -2 & 0 & 0 & 0. \end{pmatrix} \tag{4.4.18}$$

Let $l_i = l(C_i)$, where we always take $l_1 = 0$ (i.e the identity element has length 0). This yields the following expressions for the p_i:

$$p_1 = \frac{1}{8}\left(1 + e^{-tl_2} + 2e^{-tl_3} + 2e^{-tl_4} + 2e^{-tl_5}\right) \tag{4.4.19}$$

$$p_2 = \frac{1}{8}\left(1 + e^{-tl_2} + 2e^{-tl_3} - 2e^{-tl_4} - 2e^{-tl_5}\right) \tag{4.4.20}$$

$$p_3 = \frac{1}{8}\left(1 + e^{-tl_2} - 2e^{-tl_3} + 2e^{-tl_4} - 2e^{-tl_5}\right) \tag{4.4.21}$$

$$p_4 = \frac{1}{8}\left(1 + e^{-tl_2} - 2e^{-tl_3} - 2e^{-tl_4} + 2e^{-tl_5}\right) \tag{4.4.22}$$

$$p_5 = \frac{1}{8}\left(2 - 2e^{-tl_2}\right) \tag{4.4.23}$$

It is clear that p_1 and p_5 are positive for all $t \geq 0$ and also that both $p_1'(0)$ and $p_5'(0)$ are non-negative. Note that when $t = 0$, we have $p_2 = p_3 = p_4 = 0$. Let us focus momentarily on p_2. To make $p_2'(0) \geq 0$, we must have $-l_2 - 2l_3 + 2l_4 + 2l_5 \geq 0$. The analogous computations for p_3 and p_4 show that $p_2'(0), p_3'(0)$ and $p_4'(0)$ are non-negative if and only if $l_2 \leq \min\{2l_4 + 2l_5 - 2l_3, 2l_3 + 2l_5 - 2l_4, 2l_3 + 2l_4 - 2l_5\}$. In fact, this condition turns out to be essentially sufficient.

Proposition 4.4.7. *In the set up for S_3 described above, all the p_i are non-negative for all $t \geq 0$ if and only if $0 \leq l_2 \leq \min\{2l_4 + 2l_5 - 2l_3, 2l_3 + 2l_5 - 2l_4, 2l_3 + 2l_4 - 2l_5\}$ and all the lengths are non-negative.*

Proof. The only if direction is clear. For the if direction, as explained above, the non-negativity of p_1 and p_5 for $t \geq 0$ is independent of the choice of the l_i.

Note that l_2, l_3 and l_4 are symmetric in the equations for the p_i in the sense that by relabeling the conjugacy classes, we can always assume WLOG that $l_3 \leq l_4 \leq l_5$. In this case, $p_4 \leq p_3$ and $p_4 \leq p_2$, so it suffices to show that for any $t \geq 0$,

$$8p_4(t) = 1 + e^{-tl_2} + 2(e^{-tl_5} - e^{-tl_3} - e^{-tl_4}) \geq 0.$$

To this end, let $a = e^{-tl_3}$, $b = e^{-tl_4}$, $c = e^{-tl_5}$. By assumption, $e^{-tl_2} \geq \left(\frac{ab}{c}\right)^2$. Thus it suffices to show that $1 + \left(\frac{ab}{c}\right)^2 + 2(c - a - b) \geq 0$ if $0 \leq c \leq b \leq a \leq 1$.

First, we make a change of variable, setting $x = \frac{c}{b} \leq 1$. The desired inequality now reads $2(a + b(1-x)) \leq 1 + \frac{a^2}{x^2}$ for $0 \leq b \leq a \leq 1$. Clearly, it suffices to check $b = a$, since the left-hand-side is monotonically increasing in b. So we only need to show that

$$2a(2-x) \leq 1 + \frac{a^2}{x^2}.$$

It is easy to see that the right-hand-side is at least $\frac{2a}{x}$ by the inequality of arithmetic and geometric means (AM-GM). Thus, our desired inequality is reduced to $4 - 2x \leq \frac{2}{x}$. This is true since $\frac{1}{x} + x \geq 2$, by AM-GM once more. □

Extensions of these methods allow one to compute that for S_4, it is sufficient to have $p_j'(0) \geq 0$ for all $j \geq 2$ in order to guarantee the non-negativity of all the p_i's. The computations for S_4 introduce new tools in addition to those used in the cases already presented, which may be useful for similar computations in larger groups. That being said, the proof for S_4 is significantly longer than the proof for the other groups, due to there being essentially three independent variables as opposed to two. The main additional technique involved in the proof for S_4 is a method to reduce the number of variables by Fourier-Motzkin elimination [9], which is an iterative approach. Due to the length of this computation, we relegate it to Appendix A.

Since the number of cases one needs to consider grows rapidly with the number of variable lengths involved, even with the algorithmic reduction method used for S_4, it is unlikely that the method is useful for any but low-dimensional groups. This leaves us looking for a more powerful, more general approach, which we take up next.

Sufficiency of $p_i'(0) \geq 0$ for General Finite Groups

Following the character-based method introduced in [26], we now prove that the condition

$$p_i'(t=0) = -\sum_j \frac{\#C_j}{\#G} l(C_j)\chi_{ij}^* \geq 0 \tag{4.4.24}$$

for all $i \geq 2$ is actually sufficient to guarantee that $p_j(t) \geq 0$ for all $1 \leq j \leq m$ and for all $t \geq 0$, where m is the number of conjugacy classes of G, and equivalently the number of distinct irreducible representations of G.

Let $\{\chi_r\}_{r=1}^m$ be the irreducible characters of G, and for each r, define $\sigma_r\lambda(g) = \chi_r(g)\lambda(g)$. Further assume that l is a class function. Then, since characters span the class functions, P_t admits a decomposition as $P_t = \sum_r p_r(t)\sigma_r$.

Theorem 4.4.8. *If there exists $\varepsilon > 0$ such that for all $1 \leq r \leq m$, $p_r(t) \geq 0$ for all $0 \leq t \leq \varepsilon$, then for any $1 \leq s \leq m$, $p_s(t) \geq 0$ for all $t \geq 0$.*

Proof. For any $t > 0$, take n large such that $t/n < \varepsilon$. Then, $P_t = P_{n\left(\frac{t}{n}\right)} = \left(P_{\frac{t}{n}}\right)^n = \left(\sum_{i=1}^m p_i(t/n)\sigma_i\right)^n$ since P_t is a semigroup. For $1 \leq r \leq m$, let ρ_r denote the irreducible representation with character χ_r. The tensor product of irreducible representations of a finite group can be completely reduced, and the multiplicity of the irreducible representation ρ_c in $\rho_a \otimes \rho_b$, n_{ab}^c, is always non-negative. By extension, we can write $\sigma_{a_1}\sigma_{a_2}\cdots\sigma_{a_n} = \sum_{i=1}^m n_{a_1 a_2 \ldots a_n}^i \sigma_i$, where $n_{a_1 a_2 \ldots a_n}^i$ is the multiplicity of the irreducible representation ρ_i in $\rho_{a_1} \otimes \rho_{a_2} \otimes \cdots \otimes \rho_{a_n}$.

Thus,

$$P_t = \sum_{a_1,\cdots,a_n} \sum_{b} p_{a_1}(t/n) p_{a_2}(t/n) \cdots p_{a_n}(t/n) n^b_{a_1 a_2 \ldots a_n} \sigma_b. \tag{4.4.25}$$

Note that the coefficients in the above expression are all non-negative. Thus, for any $1 \leq b \leq m$, we find that $p_b(t)$, the coefficient of σ_b, is nonnegative for all $t \geq 0$. □

Corollary 4.4.9. *If there exists $\varepsilon > 0$ such that for all $1 < r \leq m$, $p_r(t) \geq 0$ for all $t \leq \varepsilon$, then for any $1 \leq s \leq m$, $p_s(t) \geq 0$ for all $t \geq 0$.*

Proof. Since $p_i(t = 0) = \delta_{i1}$ and the p_i are continuous, there is certainly a neighborhood of 0^+ where $p_1(t) > 0$. The conclusion then follows since all the hypotheses of Thm 4.4.8 are satisfied. □

Corollary 4.4.10. *If the $p'_i(t = 0)$'s are positive for all $i \geq 2$, then for any $1 \leq s \leq m$, $p_s(t) \geq 0$ for all $t \geq 0$.*

Proof. The continuity of the p_i's, combined with the positivity of the derivative, guarantees that there is a neighborhood of 0^+ in which $p_i(t) > 0$ for all $i \geq 2$. So Corollary 4.4.9 can be applied. □

Now we wish to strengthen Corollary 4.4.10 so that it suffices that all $p'_i(t = 0)$'s are *non-negative* for all $i \geq 2$. To do so, it suffices to show that the set of lengths satisfying $p_i(t) \geq 0$ for all $t \geq 0$ is a closed set. This simply follows from the fact that the arbitrary intersection of closed sets is closed, applied to the set of lengths which satisfies $\{p_i(t_0) \geq 0\}$ for $t_0 \in [0, \infty)$, in the Euclidean topology. We offer a different argument in the next section, which uses structural features from the condition of conditional negativity. This corollary, together with Proposition 4.4.5, completes the proof of Theorem 4.4.4.

4.5 Conditional Negativity Revisited

In the previous section, it was shown that for the abelian finite groups, the notion of conditional negativity of a length function was equivalent with positing the existence of a convex Kraus-like decomposition. At the end of section 3.1, in particular, we used the need to understand this relationship on a more fundamental level to motivate our study of Kraus-like decompositions for general finite groups. In this section, we now give the characterization of the relationship between conditional negativity and the existence of a *character-induced* convex Kraus-like decomposition in the full finite group case.

In the context of character-induced Kraus-like decompositions, the object of study is the decomposition of *G-circulant* matrices [30] $A = (A_{ij})$ with entries given by

$$A_{ij} = f(g_i g_j^{-1}) = \sum_{r \text{ an irrep}} p_r \chi_r(g_i g_j^{-1}) \tag{4.5.1}$$

where f is a class function on G. Such a decomposition exists since the irreducible characters form a basis of the set of class functions on G.

We wish to show the following theorem:

Theorem 4.5.1 (Decomposition Theorem)**.** *A G-circulant matrix is positive semidefinite if and only if the p_r's arising in the decomposition are all nonnegative.*

By Schoenberg's theorem, if we can show this, then we obtain the following theorem:

Theorem 4.5.2. *Suppose l is a class function on G satisfying $l(e) = 0$. Then the corresponding character-induced Kraus-like decomposition is convex (i.e. the p_r's are all nonnegative and satisfy a sum rule) if and only if l is a conditionally negative-definite length.*

Proof of Theorem 4.5.1. Define A to be the matrix with entries $f(g_i g_j^{-1})$. We first prove the if direction. Observe that if the p_r's are all non-negative, then A is self-adjoint since

$$A_{ij} = \sum_{r \text{ an irrep}} p_r \chi_r(g_i g_j^{-1}) \tag{4.5.2}$$

and

$$A^*_{ji} = \sum_{r \text{ an irrep}} p_r \chi_r(g_j g_i^{-1})^* = \sum_{r \text{ an irrep}} p_r \chi_r(g_j g_i^{-1})^* \tag{4.5.3}$$

and we can write

$$\chi_r(g_j g_i^{-1})^* = (\sum_{n,m} r(g_j)_{n,m} r(g_i)^{-1}_{m,n})^* \tag{4.5.4}$$

$$= (\sum_{n,m} r(g_j)^*_{n,m} r(g_i)^{-1\,*}_{m,n}) \tag{4.5.5}$$

$$= \sum_{m,n} r(g_j)^\dagger_{m,n} (r(g_i)^{-1})^\dagger_{n,m} \tag{4.5.6}$$

$$= \sum_{m,n} r(g_j^{-1})_{m,n} r(g_i)_{n,m} \tag{4.5.7}$$

$$= \chi_r(g_i g_j^{-1}) \tag{4.5.8}$$

where we have used the fact that the irreducible representations of finite groups are unitary.

Since A is self-adjoint, it has a full spectrum. We want to show that the spectrum is nonnegative. It suffices to show that the matrices $(\chi_r(g_i g_j^{-1}))_{i,j}$, which by the above are self-adjoint, are in fact (up to normalization) orthogonal projections, in particular, that they satisfy

$$\sum_{j=1}^{|G|} \chi_r(g_i g_j^{-1}) \chi_s(g_j g_k^{-1}) = \delta_{r,s} \frac{|G|}{\chi_r(e)} \chi_r(g_i g_k^{-1}). \tag{4.5.9}$$

This would imply that the eigenvalues of A are simply given by p_r's up to positive rescaling (with additional multiplicities to account for the size of the subspace with the same eigenvalue).

We prove this result using the idempotent method. Namely, it is known (see e.g., [18]) that within the group algebra of a finite group, one has the idempotents

$$e_r = \frac{\chi_r(e)}{|G|} \sum_{g \in G} \chi_r(g^{-1}) \lambda(g) \tag{4.5.10}$$

where $\lambda(g)$ is the left-regular representation of the finite group G. These idempotents satisfy

$$e_r e_s = \delta_{r,s} e_r. \tag{4.5.11}$$

Comparing coefficients of $\lambda(g)$ in $e_r e_r$ and e_r, one obtains that

$$\frac{\chi_r(e)}{|G|} \sum_{h \in G} \chi_r(hg^{-1}) \chi_r(h^{-1}) = \chi_r(g^{-1}) \tag{4.5.12}$$

for all $g \in G$. Setting $g^{-1} = g_i g_k^{-1}$, and rewriting the dummy element h as $h = g_j g_i^{-1}$ and summing over g_j, equation 4.5.12 becomes

$$\frac{\chi_r(e)}{|G|} \sum_{g_j \in G} \chi_r(g_j g_k^{-1}) \chi_r(g_i g_j^{-1}) = \chi_r(g_i g_k^{-1}) \tag{4.5.13}$$

and so we have shown that equation 4.5.9 is true for $r = s$. When $r \neq s$, one has that $e_r e_s = 0$, so the coefficient of each $\lambda(g)$ must vanish, yielding

$$\frac{\chi_r(e)}{|G|} \sum_{g_j \in G} \chi_r(g_j g_k^{-1}) \chi_s(g_i g_j^{-1}) = 0. \tag{4.5.14}$$

This completes the proof of equation 4.5.9.

For the only if direction, assume A is positive semi-definite. Applying A to an eigenvector v of $(\chi_r(g_i g_j^{-1}))_{i,j}$ yields $p_r v$ up to a positive rescaling factor (since $(\chi_r(g_i g_j^{-1}))_{i,j}$ is a projection up to positive rescaling; we will fix the overall constant in the next section). So p_r must be nonnegative. Since this must be true for any irrep r, the p_r's must all be nonnegative.

□

Bearing in mind that positive constant multiples of conditionally negative-definite lengths are conditionally negative-definite, we may summarize the theorems of this section as follows:

Theorem 4.5.3. *Fix a group $G = \{g_1 = e, \cdots, g_n\}$ and let M be a G-circulant matrix such that $M_{1,1} = 1$. Since the χ_r form a basis for class functions, there exists a decomposition $M_{ij} = \sum_{irreps} p_r \chi_r(g_i g_j^{-1})$. The following are equivalent:*

- *M is positive semi-definite.*
- *Each p_r is non-negative.*
- *The length defined by $l(g_i) = -\ln(M_{i1})$ is conditionally negative-definite.*

Thus, if we take p_r to be the $p_r(t)$ *induced* by the conditionally negative-definite length l via our Kraus-like decomposition, then $p_r(t) \geq 0$ for all $t \geq 0$. Conversely, if $p_r(t) \geq 0$, then one obtains canonically a conditionally negative-definite length defined by $l(g_i) = -\frac{1}{t}\ln(M_{i1}(t))$. Hence, the set of class function lengths such that P_t has a convex character-induced Kraus-like decomposition is precisely the set of conditionally negative-definite class function lengths.

Based on this equivalence, we offer a different proof that the set of definite linear constraints we obtained to show the nonnegativity of all $p_i(t)$'s for all $t \geq 0$ in Corollary 4.4.10 can be improved to semidefinite linear constraints.

The idea is to interpret that the length function l as a point in a finite-dimensional space. Following Corollary 4.4.10, one knows that the pre-image of the positive orthant O under the map

$$\Phi(l) = (\Phi_2(l), \Phi_3(l), \cdots, \Phi_k(l)), \tag{4.5.15}$$

where $\Phi_i(l) := -\sum_j \frac{\#C_j}{\#G} l(C_j)\chi^*_{ij}$ from $(l(C_2), \cdots, , l(C_k))$ to $\mathbb{R}^{k-1}$, where k is the number of conjugacy classes (recall that $l(C_1) = 0$), is *contained* in the set of conditionally negative-definite lengths. Note that Φ is a map to $k-1$ dimensional space and does not have a coordinate $\Phi_1(l)$, even though $\Phi_1(l)$ is defined.

We now prove two technical lemmas to support our proof that the definite constraints can be replaced by semi-definite constraints:

Lemma 4.5.4. *Let G be a group with $|G| = n$ and let $A \subset \mathbb{C}^n$ be the set of conditionally negative-definite lengths on G, where we identify a function $f : G \to \mathbb{C}$ with the vector $(f(g_1), \cdots, f(g_n)) \in \mathbb{C}^n$. Then A is closed.*

Proof. We show that A^C is open. Let $f \in A^C$. Then there exists some $\{\alpha_i\}_{i=1}^n$ such that

$$\sum_{i=1}^{n} \alpha_i = 0 \tag{4.5.16}$$

and

$$\sum_{i,j=1}^{n} \alpha_i \overline{\alpha_j} f(g_i^{-1} g_j) > 0. \tag{4.5.17}$$

This is an open condition, and so if we obtain a new length f_ε by changing f by an ε amount in each coordinate, for ε sufficiently small, it will continue to hold with the same $\{\alpha_i\}_{i=1}^n$. Thus, $f_\varepsilon \in A^C$ as well. This proves that A^C is open and so also proves that A is closed. □

Lemma 4.5.5. *The map Φ is invertible.*

Proof. Note that in our proof, the condition eq. (4.4.6), which says $\sum_{i=1}^k p_i \chi_i(e) = 1$, translates to a linear condition on the $\Phi_i(l)$ which involves all the $\Phi_i(l)$ and in particular $\Phi_1(l)$. Thus, given $\Phi(l) = (\Phi_2(l), \ldots, \Phi_k(l))$, we can determine $\Phi_1(l)$.

Observe that eq. (4.4.24) gives an explicit expression for $\{\Phi_i(l)\}_{i=1}^k$. Note that it is immediately clear from character theory that χ^*_{ij} is invertible. It then follows that the map from l to

$(\Phi_1(l), \Phi_2(l), \ldots, \Phi_k(l))$ is invertible as well. Due to the addition of Φ_1, note that this is not the map Φ.

Putting this all together, it follows that given $x = (\Phi_2(l), \ldots, \Phi_k(l))$, we can determine $\Phi_1(l)$ and then uniquely recover $l = \Phi^{-1}(x)$. □

Proposition 4.5.6. *Fix $l(C_1) = 0$, and take $l(C_i)$ to be variable for $i = 2, \ldots, k$. If the $p_i'(t = 0)$'s are nonnegative for all $i \geq 2$, then for any $1 \leq s \leq k$, $p_s(t) \geq 0$ for all $t \geq 0$.*

Proof. Since Φ is invertible and linear, Φ^{-1} is continuous. Thus, $\Phi^{-1}(\overline{O}) \subset \overline{\Phi^{-1}(O)}$, where O is the set of points with coordinates $x_i > 0$ for all $i = 1, 2, \ldots, k-1$. The latter is a subset of the set of conditionally negative-definite lengths (since this set is closed). Hence, any length whose image lies in $\bar{O}$ is conditionally negative-definite. Thus, we have strengthened the constraints from definite linear constraints (defined by O) to semidefinite linear constraints (defined by $\bar{O}$). □

4.5.1 Values and Multiplicities of Eigenvalues

We further show that the rank of $(\chi_r(g_i g_j^{-1}))_{i,j}$ is given by $\chi_r(e)^2$. To prove this, first note that $\chi_r(g_i g_j^{-1}) = \chi_r(g_j g_i^{-1})^*$, so $(\chi_r(g_i g_j^{-1}))_{g_i,g_j}$ is Hermitian, and is fully diagonalizable. Furthermore, by rescaling equation 4.5.9, we get that

$$\sum_{j=1}^{|G|} \left(\frac{\chi_r(e)}{|G|} \chi_r(g_i g_j^{-1}) \right) \left(\frac{\chi_r(e)}{|G|} \chi_s(g_j g_k^{-1}) \right) = \delta_{r,s} \frac{\chi_r(e)}{|G|} \chi_r(g_i g_k^{-1}), \tag{4.5.18}$$

and so the $\frac{\chi_r(e)}{|G|}(\chi_r(g_i g_j^{-1}))_{g_i,g_j}$ is are orthogonal projection matrices, with eigenvalues 0 or 1. Thus, to compute its rank, we just need its trace, which is $|G| \cdot \frac{\chi_r(e)}{|G|}(\chi_r(e)) = (\chi_r(e))^2$. It follows that the multiplicity of the eigenvalue 1 in the projection matrix corresponding to irrep r is $(\chi_r(e))^2$.

Rewriting the decomposition of A given by eq. (4.5.1) in terms of the projections, one has that

$$f(g_i g_j^{-1}) = \sum_{r \text{ an irrep}} \left(\frac{|G|}{\chi_r(e)} p_r \right) \left(\frac{\chi_r(e)}{|G|} \chi_r(g_i g_j^{-1}) \right) \tag{4.5.19}$$

and so the eigenvalues are given by $\left(\frac{|G|}{\chi_r(e)} p_r \right)$. Since these are orthogonal projections, we thus have shown that the multiplicity of each eigenvalue $\frac{|G|}{\chi_r(e)} p_r$ in the matrix given by eq. (4.5.1) is given by $(\chi_r(e))^2$.

4.6 Conclusion

In this chapter, we have presented a new way to approach semigroups acting on group algebras, namely, *Kraus-like decompositions*. By modifying the action of possible operators which can be used in the sum decomposition of a semigroup, our approach allows us to introduce operator decompositions in problems where they were not readily available before. In particular, we are able to explore quantum channels induced by length functions in the context of group algebras. For length functions that are additionally class functions, we obtain several equivalent necessary and sufficient conditions on the length function for the semigroup P_t to be a quantum channel for all time $t \geq 0$.

Specifically, for *character-induced* Kraus-like decompositions, we have proven that a set of semidefinite linear constraints is necessary and sufficient to guarantee the positivity of the coefficients appearing in the decomposition for all $t \geq 0$. We also proved that this same set of semidefinite linear constraints suffices to characterize the conditionally negative-definite lengths, a class of length functions that are of independent interest. Using Schoenberg's theorem, we further relate this to conditions on the complete positivity of semigroups P_t induced by lengths which are class functions. These constraints follow from the fact that for a semigroup P_t, the property of admitting a Kraus-like decomposition can be checked globally using a more local condition. Specifically, if one can show that P_t admits a Kraus-like decomposition for $t > 0$ sufficiently small, then the same can be concluded for all $t > 0$.

The coefficients of our p_i's are defined canonically. Moreover, they are nonnegative and satisfy a sum rule. Thus, the coefficients may have physical meaning (under appropriate rescaling) as *probabilities*. These possible interpretations await further investigation.

4.7 Appendix: Proof of Stability Condition for S_4

We have a direct proof that the *a priori* necessary conditions on the p_i are sufficient to ensure the existence of a convex Kraus-like decomposition in the context of S_4 as well. We use methods that are similar to those presented above but more computationally involved due to the parameter space being of a larger dimension.

The character table for S_4 is

$$\chi = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 3 & 1 & 0 & -1 & -1 \\ 2 & 0 & -1 & 2 & 0 \\ 3 & -1 & 0 & -1 & 1 \\ 1 & -1 & 1 & 1 & -1 \end{pmatrix} \tag{4.7.1}$$

and the sizes of the conjugacy classes are $(C_i)_{i=1,\ldots,5} = (1, 6, 8, 3, 6)$.

Accordingly,

$$p_1 = \frac{1}{24}\left(1+6e^{-tl_2}+8e^{-tl_3}+3e^{-tl_4}+6e^{-tl_5}\right) \tag{4.7.2}$$

$$p_2 = \frac{1}{8}\left(1+2e^{-tl_2}-e^{-tl_4}-2e^{-tl_5}\right) \tag{4.7.3}$$

$$p_3 = \frac{1}{12}\left(1-4e^{-tl_3}+3e^{-tl_4}\right) \tag{4.7.4}$$

$$p_4 = \frac{1}{8}\left(1-2e^{-tl_2}-e^{-tl_4}+2e^{-tl_5}\right) \tag{4.7.5}$$

$$p_5 = \frac{1}{24}\left(1-6e^{-tl_2}+8e^{-tl_3}+3e^{-tl_4}-6e^{-tl_5}\right). \tag{4.7.6}$$

Thus, at $t=0$, $p_1=1$ and all the others are equal to 0.

The constraint that the probabilities be nonnegative at time $\varepsilon > 0$ for ε arbitrarily small tells us that $p_i'(t=0) \geq 0$ for $2 \leq i \leq 5$, In particular,

$$24p_2'(0) = -6l_2 + 3l_4 + 6l_5 \geq 0 \tag{4.7.7}$$

$$24p_3'(0) = 8l_3 - 6l_4 \geq 0 \tag{4.7.8}$$

$$24p_4'(0) = 6l_2 + 3l_4 - 6l_5 \geq 0 \tag{4.7.9}$$

$$24p_5'(0) = 6l_2 - 8l_3 - 3l_4 + 6l_5 \geq 0. \tag{4.7.10}$$

We can clean this up a little bit by setting $a = e^{-tl_2}$, $b = e^{-tl_3}$, $c = e^{-tl_4}$, $d = e^{-tl_5}$.

Theorem 4.7.1. *In the set up for S_4 described above, all the p_i are non-negative for all $t \geq 0$ if and only if the lengths are all non-negative and the above necessary conditions hold. Expressed in terms of a, b, c and d, the necessary and sufficient conditions are equivalent to the following system of inequalities:*

$$0 \leq a, b, c, d \leq 1. \tag{4.7.11}$$

$$a^2 c^{-1} d^{-2} \geq 1 \tag{4.7.12}$$

$$b^{-4} c^3 \geq 1 \tag{4.7.13}$$

$$a^{-2} c^{-1} d^2 \geq 1 \tag{4.7.14}$$

$$a^{-6} b^8 c^3 d^{-6} \geq 1. \tag{4.7.15}$$

.

Proof. We first express our goal, the non-negativity of the p_i, in terms of a, b, c and d as follows:

$$1 + 2a - c - 2d \geq 0 \tag{4.7.16}$$

$$1 - 4b + 3c \geq 0 \tag{4.7.17}$$

$$1 - 2a - c + 2d \geq 0 \tag{4.7.18}$$

$$1 - 6a + 8b + 3c - 6d \geq 0 \tag{4.7.19}$$

To prove these inequalities, we must consider a number of cases.

The $a = d$ case

We want to show that

$$b^{-4} c^3 \geq 1 \tag{4.7.20}$$

$$a^{-12} b^8 c^3 \geq 1 \tag{4.7.21}$$

implies

$$1 - 4b + 3c \geq 0 \tag{4.7.22}$$

$$1 - 12a + 8b + 3c \geq 0, \tag{4.7.23}$$

since the other inequalities become trivial in this case. The inequality $1 - 4b + 3c \geq 0$ holds true since $1 - 4b + 3c \geq 1 - 4b + 3b^{4/3}$, which is nonnegative on $[0, 1]$ since its derivative is nonpositive and it evaluates to 0 at $b = 1$.

Note that $a \leq b^{2/3}c^{1/4}$, so $1 - 12a + 8b + 3c \geq 1 - 12b^{2/3}c^{1/4} + 8b + 3c$. We want to minimize this subject to $b^4 \leq c^3$, and show that the minimum is at least 0. If $b^4 = c^3$, we obtain that the lower bound is given by $1 - 12b^{2/3}b^{1/3} + 8b + 3b^{4/3} = 1 - 4b + 3b^{4/3}$. This is the same situation as in the previous case and as such, is non-negative for $b \in [0, 1]$. Taking a partial derivative with respect to b, we get $-8b^{-1/3}c^{1/4} + 8 \leq -8b^{-1/3}b^{1/3} + 8 = 0$, so $1 - 12b^{2/3}c^{1/4} + 8b + 3c$ is non-negative at points (b, c) where $b \in [0, c^{3/4}]$. This is precisely the range of values of b allowed by the first inequality, so we are done.

Relaxing the condition $a = d$: We now treat the full set of inequalities. We rewrite our assumptions in terms of c:

$$c \leq \min(a^2d^{-2}, a^{-2}d^2) \tag{4.7.24}$$

and

$$c \geq \max(b^{4/3}, a^2d^2b^{-8/3}). \tag{4.7.25}$$

In particular, we have that

$$\max(b^{4/3}, a^2d^2b^{-8/3}) \leq \min(a^2d^{-2}, a^{-2}d^2), \tag{4.7.26}$$

and so

$$b^{2/3}a \leq d \leq b^{2/3} \tag{4.7.27}$$

$$b^{2/3}d \leq a \leq b^{2/3} \tag{4.7.28}$$

are necessary conditions.

We first prove that $1 + 2a - c - 2d \geq 0$. Note that everything is symmetric in a and in d, so without loss of generality, suppose $a \geq d$, then

$$1 + 2a - c - 2d \geq 1 + 2a - d^2/a^2 - 2d = 2(a - d) + 1 - d^2/a^2 \geq 0. \tag{4.7.29}$$

Next, we show $1 + 2d - c - 2a \geq 0$. Continuing to assume that $a \geq d$, we note that

$$1 + 2d - c - 2a \geq 1 + 2d - d^2/a^2 - 2a. \tag{4.7.30}$$

We want to minimize $1 + 2d - d^2/a^2 - 2a$ over the region of permitted values of a and d, so we start by fixing b and a, and requiring d to lie between $b^{2/3}a$ and $b^{2/3}$. (Note that we will be a bit lackadaisical with the constraint on a. This is justified since we just need a lower bound on the constraint region, which is guaranteed if we work with a region containing the constraint region.)

Taking a partial derivative with respect to d yields $2 - 2d/a^2$ which changes sign at $d = a^2$, from positive to negative, so this is a maximum. We must evaluate this expression at the boundary of the allowed d values as well. These are $d = b^{2/3}a$ and $d = a$ (since, by assumption, $d \leq a$). Evaluating at $d = b^{2/3}a$, we obtain $1 - 2(1 - b^{2/3})a - b^{4/3} \geq 1 - 2(1 - b^{2/3})b^{2/3} - b^{4/3} = 1 - 2b^{2/3} + b^{4/3} = (1 - b^{2/3})^2 \geq 0$, where in the first inequality, we used $a \leq b^{2/3}$. For $d = a$, we get $1 + 2a - 1 - 2a = 0$.

Next, we want to show that

$$1 - 4b + 3c \geq 0. \tag{4.7.31}$$

Since $c \geq b^{4/3}$, we obtain $1 - 4b + 3c \geq 1 - 4b + 3b^{4/3} \geq 0$, as we showed earlier.

Finally, we want to show

$$1 - 6(a + d) + 8b + 3c \geq 0. \tag{4.7.32}$$

It is natural to split into two cases.

Case 1: $b^2 \leq ad$**:** In this case, we have $c \geq (ad)^2 b^{-8/3}$ as the stronger lower bound. Using this bound yields

$$1 - 6(a + d) + 8b + 3c \geq 1 - 6(a + d) + 8b + 3(ad)^2 b^{-8/3}. \tag{4.7.33}$$

We will minimize the sum $1 - 6(a + d) + 8b + 3(ad)^2 b^{-8/3}$ for fixed b. We can still assume without loss of generality that $a \geq d$. Recall that $b^{2/3}a \leq d$. So we want to minimize $1 - 6(a + d) + 8b + 3(ad)^2 b^{-8/3}$ as a function of a and d subject to the two constraints

$$b^{2/3}a \leq d \leq a \leq b^{2/3} \tag{4.7.34}$$

and

$$ad \geq b^2. \tag{4.7.35}$$

The shape of this domain is a three-sided region dependent on the value of b. In the plane with a as its y-axis and d as its x-axis, we have a region upper bounded by the line $a = b^{2/3}$, right-bounded by the line $d = a$, and southwest-bounded by the curve $ad = b^2$. The corners of the region are $(d = b^{4/3}, a = b^{2/3})$, $(d = b^{2/3}, a = b^{2/3})$, and $(d = b, a = b)$.

For fixed a, we can differentiate with respect to d, obtaining $-6 + 6a^2 d b^{-8/3}$. Note that $a \geq b$ and $d \geq b^{4/3}$ on this region, so we have an upper bound on this derivative of $-6 +$

$6b^2b^{4/3}b^{-8/3} = -6 + 6b^{2/3} \leq 0$. Thus, the derivative is non-positive, and the function is non-increasing in d. As such, it will suffice to take d lying on the boundary to the right, where $d = a$. We are thus left with considering $d = a$ yielding the expression $1 - 12a + 8b + 3a^4b^{-8/3}$.[5] Taking a derivative with respect to a, we obtain $-12 + 12a^3b^{-8/3}$, which equals 0 when $a^3b^{-8/3} = 1$, which is to say, when $a = b^{8/9}$. Note that $-12 + 12a^3b^{-8/3} < 0$ for $a < b^{8/9}$ and $-12 + 12a^3b^{-8/3} > 0$ for $a > b^{8/9}$, so we obtain a minimum at $a = b^{8/9}$ and it suffices to use this value going forward. Thus, we want to minimize $1 - 12b^{8/9} + 8b + 3b^{32/9}b^{-8/3} = 1 - 9b^{8/9} + 8b$. This has derivative $8 - 8b^{-1/9} \leq 0$, so it suffices to verify $1 - 9b^{8/9} + 8b \geq 0$ at $b = 1$, which certainly holds.

Case 2: $b^2 \geq ad$**:** Then $c \geq b^{4/3}$ is the meaningful lower bound on c. So we wish to minimize

$$1 - 6(a + d) + 8b + 3b^{4/3} \tag{4.7.36}$$

on the domain

$$b^{2/3}a \leq d \leq a \leq b^{3/2} \tag{4.7.37}$$

and

$$ad \leq b^2. \tag{4.7.38}$$

This domain is also a three-sided region dependent on the value of b. It is bounded on the left by the line $d = b^{2/3}a$, on the right by the line $a = d$, on the northeast by the curve $ad = b^2$. The corners of the region are $(0,0)$, $(d = b^{4/3}, a = b^{2/3})$, and (b, b).

The partial derivative of $1 - 6(a + d) + 8b + 3b^{4/3}$ with respect to d is -6, so due to the geometry of the domain boundary, this expression is minimized on the $d = a$ boundary if $a \leq b$ and on the $ad = b^2$ boundary if $a \geq b$.

For $a \leq b$ and $d = a$, we have $1 - 6(a+d) + 8b + 3b^{4/3} = 1 - 12a + 8b + 3b^{4/3} \geq 1 - 4b + 3b^{4/3}$.

[5] Note that we had not considered this case yet. When we had $d = a$ earlier, we were directly considering the inequalities we wanted to prove, not the strengthened one we are working with here.

This is non-negative, as we showed earlier.

For $a \geq b$ and $ad = b^2$, we obtain $1 - 6(a+d) + 8b + 3b^{4/3} = 1 - 6(a + b^2/a) + 8b + 3b^{4/3}$. Taking a derivative with respect to a, one $-6(1 - b^2/a^2)$. Thus, $1 - 6(a + b^2/a) + 8b + 3b^{4/3}$ has a maximum at $a = b$, and achieves its minimums at a boundary value of a. The boundary values of a in the region we are considering are $a = b^{2/3}$ and $a = b$. If $a = b^{2/3}$, we get $1 + 8b - 3b^{4/3} - 6b^{2/3}$, which has derivative $-\frac{4(-1+b^{1/3})^2}{b^{1/3}} \leq 0$. Thus, $1 + 8b - 3b^{4/3} - 6b^{2/3}$ is minimized when $b = 1$, yielding 0. If $a = b$, we get $1 - 4b + 3b^{4/3}$, which is non-negative, as shown earlier. □

5

Building lattice structures using generalized Clifford algebras

5.1 Introduction

Lattice-based cryptography is a promising candidate for post-quantum cryptography [32], i.e. cryptography in the era of quantum computers. We would like to study lattices from the perspective of generalized Clifford algebras, using the kinds of methods we established in earlier chapters, and their extension to the lattice case. One motivation may be said to be the problem of devising a publicly secure quantum money protocol using lattices [21]. Our results in this chapter shed light on the structure of the Hilbert space associated to lattices, by constructing new kinds of unitary operators one can work with, and thus contribute to an understanding of the quantum operations that may be performed on a lattice.

The lattice used in [21] is generated by a code C, which is a matrix whose rows are vectors in $\mathbb{Z}_P$, adjoined with the vectors at the corners of the d-dimensional cube of length P, which has one corner at the origin. The code is embedded into $\mathbb{R}^d$. The dual lattice of this lattice is defined with respect to the inner product $x \cdot y = \frac{1}{P}\sum_{i=1}^{d} x_i y_i$. Under this inner product, the lattice is generically **not integral**, i.e. it is not generally true that $x \cdot y \in \mathbb{Z}$ for all x, y in the lattice. This has important ramifications since many nice mathematical theorems cannot be applied; in particular, as a result, the lattice is not contained in its dual. Instead, a different characterization arises.

Consider the extension of C to a lattice $\mathcal{L} \subset \mathbb{R}^d$. Suppose that the lattice has a basis e_i, $i = 1, 2, \ldots, d$. The dual lattice is defined to be the set of all vectors v in $\mathbb{R}^d$ such that $x \cdot v \in \mathbb{Z}$ if $x \in \mathcal{L}$. Alternately, the dual lattice is generated, upon identification with vectors in $\mathbb{R}^d$ via Riesz representation, by vectors e'_i satisfying $e'_i \cdot e_j = \delta_{ij}$. Note that, using the first characterization of the dual lattice, $(P, 0, 0, \cdots, 0)$ belongs in the dual lattice since x_1 is an integer for $x \in \mathcal{L}$. Similarly, it follows that all the corners of the d-dimensional cube of length P with one corner at the origin and edges parallel to the axes belong to the dual lattice. To complete the basic description of the dual lattice, we show the following:

1. The dual lattice contains only vectors with integer entries.
2. The dual lattice is equal to the extension of $C^{\perp}$ in $\mathbb{R}^d$ by the aforementioned cube corner vectors.

The first follows by considering that the lattice contains $(P, 0, \cdots, 0)$, and so if v is in the dual lattice, then $(P, 0, \cdots, 0) \cdot v = v_1 \in \mathbb{Z}$. Similarly, for the other corner vectors, we have that

$v_i \in \mathbb{Z}$ for each $i = 1, 2, \cdots, d$. Hence, the dual lattice is an integer lattice.

Thus, the relation $x \cdot v = \frac{1}{P}\sum_{i=1}^{d} x_i v_i \in \mathbb{Z}$ can literally be taken as the number-theoretic relation $\sum_{i=1}^{d} x_i v_i = 0$ (mod P). Hence, $C^{\perp}$ is in the dual lattice. Furthermore, quotienting the dual lattice by the edge vectors $(P, 0, \cdots, 0)$, $(0, P, \cdots, 0)$, ..., $(0, 0, \cdots, \cdots, P)$, maps the equality into a relation over $\mathbb{Z}_P$, which says that $\sum_{i=1}^{d} \bar{x}_i \bar{v}_i = 0$. So $\bar{v}$ is contained in $\mathbb{C}^{\perp}$. Lifting this homomorphism by the kernel (which is spanned by the above edge vectors), tells us that the dual lattice is equal to the extension of $C^{\perp}$ in $\mathbb{R}^d$ by the aforementioned cube corner vectors. QED

In [21], another restriction is that the determinant of the lattice (not the code) be $\pm P$. Since the covolume of the lattice is the volume of a unit cell, and to each lattice point in the code C (which the lattice on the corresponding d-torus), one can attach a non-overlapping unit cell. It follows that the volume of d-torus, which is P^d, is given by $P \cdot n = P^d$, where n is the number of lattice points. So $n = P^{d-1}$, and the code is rank $d-1$. Thus, the dual code is rank 1. More properly, the restriction in [21] is to consider the class $\mathcal{C}_P$ of such lattices that have exactly one lattice vector in each hyper-row, i.e. if one considers a $(d-1)$-dimensional face of the cube $\{(x_1, x_2, \cdots, x_i, \cdots, x_d : x_i = 0, x_{j \neq i} \in \mathbb{Z}_P\}$, one can parameterize the set of all lattice points *functionally* over the face coordinates by $x_i = f(x_1, x_2, \cdots, \hat{x}_i, \cdots, x_d)$, where $\hat{x}_i$ denotes the exclusion of the corresponding coordinate. Since it is clear that the number of lattice points is given by P^{d-1}, it again follows from the preceding argument that the determinant of the lattice is $\pm P$.

A converse lemma regarding the structure of the lattice which allows one to obtain a code C is given in [21] as the following:

Lemma 5.1.1 ([21]). *Let P be prime. If an integer lattice in d dimensions which is not periodic with period* 1 *along any coordinate has determinant* $\pm P$ *and rank d, then it is periodic in every dimension with period P.*

Proof. We present a more algebraic-flavored proof than [21] which has the same starting point. Since the lattice is rank d, there must be a lattice point $(T, 0, 0, \cdots, 0)$ on the x_1-axis, otherwise the lattice basis may be augmented by the vector $(1, 0, 0, \cdots, 0)$ and still remain a basis (as the basis property is preserved if there is no solution to $b(1, 0, 0, \cdots, 0) \in \mathcal{L}$ for $b \neq 0$), contradicting the fact that the lattice has rank d. Then the determinant of the lattice may be computed to be T times the determinant of the cofactor A_{11} where A is the generator matrix, and equal to $\pm P$. So $TK = P$, where K is an integer and $T \neq \pm 1$. Since P is prime, it follows that $T = \pm P$. The argument applies for every axis, hence the lattice is periodic in every dimension with period P. □

With the above preliminaries complete, we now treat lattices from the perspective of generalized Clifford algebras.

5.2 Using Generalized Clifford Algebras for Lattices

5.2.1 Generalizing the Algebraic Framework for Generalized Clifford Algebras to Lattices in $\mathbb{Z}_P^d$

Let us again use the axioms as given in Chapter 2. Now suppose one has a code C in $\mathbb{Z}_P^d$. Then one has $2d$ generators, $c_1, c_2, \ldots, c_{2d-1}, c_{2d}$, which satisfy $c_a c_b = q c_b c_a$ if $a < b$, and $c_a^P = 1$. Furthermore, q is a primitive Pth root of unity, with $q^P = 1$ and $q^a \neq 1$ for any positive integer $a < P$. Let us start with a basis $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r$ of the code. The dual code has a basis $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_{d-r}$. The code and dual code are both P-ary codes. Define the product $c_{\mathbf{v}}$ in the algebra by

$$c_{\mathbf{v}} := c_2^{v^1} c_4^{v^2} \cdots c_{2d}^{v^d}, \tag{5.2.1}$$

where $\mathbf{v} = (v^1, v^2, \cdots, v^d)$. This definition is well-defined over $\mathbb{Z}_P^d$ because the generators each satisfy $c_a^P = 1$.

Up to phase factors, one can associate each codeword $\mathbf{v} = \sum_{i=1}^{r} \alpha_i \mathbf{v}_i$ with the ordered product $c_{\mathbf{v}_1}^{\alpha_1} c_{\mathbf{v}_2}^{\alpha_2} \cdots c_{\mathbf{v}_r}^{\alpha_r} |\Omega\rangle^{\otimes d}$, where $\alpha_i = 0, 1, \cdots, P-1$. In Chapter 2, we already defined the generalized Clifford algebra generators c_i in a matrix representation in terms of a fixed basis (see equations 2.2.1 and 2.2.2). From these equations, it is clear that

Proposition 5.2.1. *Let $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_r \in \mathbb{Z}_P^d$ be a set of linearly independent vectors, where P is positive integer at least two. The set $c_{\boldsymbol{v}_1}^{\alpha_1} c_{\boldsymbol{v}_2}^{\alpha_2} \cdots c_{\boldsymbol{v}_r}^{\alpha_r} |\Omega\rangle^{\otimes d}$ is an orthonormal basis for the subspace spanned by the codewords $|\sum_{i=1}^{r} \alpha_i \boldsymbol{v}_i\rangle$, with $\alpha_i = 0, 1, 2, \ldots, P-1$.*

Proof. This result follows simply from the fact that $|\sum_{i=1}^{r} \alpha_i \mathbf{v}_i\rangle$ is equal to $c_{\mathbf{v}_1}^{\alpha_1} c_{\mathbf{v}_2}^{\alpha_2} \cdots c_{\mathbf{v}_r}^{\alpha_r} |\Omega\rangle^{\otimes d}$ up to an overall phase factor $e^{i\varphi}$ (φ is real) by equation 2.2.1. □

Furthermore, this subspace is invariant under the action of the algebra generated by the $c_{\mathbf{v}_i}$'s.

Proposition 5.2.2. *The subspace spanned by the codewords $|\sum_{i=1}^{r} \alpha_i \boldsymbol{v}_i\rangle$, with $\alpha_i = 0, 1, 2, \ldots,$ $P-1$ is invariant under the action of the subalgebra (over $\mathbb{C}$) generated by $c_{\boldsymbol{v}_1}, c_{\boldsymbol{v}_2}, \ldots, c_{\boldsymbol{v}_r}$.*

Proof. By the closure properties of a vector space under addition and multiplication by a complex scalar, it suffices to check that the subspace is invariant under multiplication by a single $c_{\mathbf{v}_i}$. Without loss of generality, let us consider multiplication $c_{\mathbf{v}_1}$. From equation 2.2.1, $c_{\mathbf{v}_1} |\sum_{i=1}^{r} \alpha_i \mathbf{v}_i\rangle = e^{i\varphi} |\sum_{i=1}^{r} \alpha_i \mathbf{v}_i + \mathbf{v}_1\rangle$, where φ is real. Hence the vector subspace is fixed under multiplication by a single $c_{\mathbf{v}_i}$, and so it is invariant under the action of the entire subalgebra. □

Before we proceed, we state an important relation which allows us to work with the new $c_{\mathbf{v}}$ operators:

Proposition 5.2.3.

$$c_v c_w c_v^{-1} c_w^{-1} = q^{\sum_{i,j=1}^{d} \varepsilon_{ij} v^i w^j}, \tag{5.2.2}$$

where $\varepsilon_{ij} = 0$ if $i = j$, 1 if $i < j$, and -1 if $i > j$.

From this identity, one may deduce the commutant of the subalgebra generated by a $c_{\mathbf{v}}$ operator.

Corollary 5.2.4. *c_w commutes with c_v if and only if $\sum_{i,j=1}^{d} \varepsilon_{ij} v^i w^j = 0$ (mod P).*

Note that the condition $\sum_{i,j=1}^{d} \varepsilon_{ij} v^i w^j = 0$ (mod P) defines a single equation linear in **w**.

Written slightly differently, Proposition 5.2.4 becomes $c_{\mathbf{v}} c_{\mathbf{w}} = q^{\sum_{i,j=1}^{d} \varepsilon_{ij} v^i w^j} c_{\mathbf{w}} c_{\mathbf{v}}$. This can be generalized to the following identity, by iterated commutation:

Proposition 5.2.5.

$$c_{\boldsymbol{v}}^{a} c_{\boldsymbol{w}}^{b} = q^{ab \sum_{i,j=1}^{d} \varepsilon_{ij} v^i w^j} c_{\boldsymbol{w}}^{b} c_{\boldsymbol{v}}^{a}. \tag{5.2.3}$$

Proof. Bringing a single copy of $c_{\mathbf{w}}$ in front of $c_{\mathbf{v}}^{a}$ yields a factors of $q^{\sum_{i,j=1}^{d} \varepsilon_{ij} v^i w^j}$. So bringing b copies of $c_{\mathbf{w}}$ in front of $c_{\mathbf{v}}^{a}$ gives the phase factor $q^{ab \sum_{i,j=1}^{d} \varepsilon_{ij} v^i w^j}$. □

We define new braid-like operators B_{kl} given by

$$B_{kl} := \frac{1}{\sqrt{P}} \sum_{i=0}^{P-1} c_{\mathbf{v}_k}^{i} c_{\mathbf{v}_l}^{-i}. \tag{5.2.4}$$

In order for this sum to be well-defined mod P, we need the auxiliary result that $c_{\mathbf{v}_k}^{P} = 1$. This turns out to be true only if P is odd. This requirement is an extremely important *regularity condition*.

Proposition 5.2.6 (Regularity Condition)**.** *Suppose $x^P = y^P = 1$ and $xyx^{-1}y^{-1} = Q$, where Q is a Pth root of unity. If P is odd, then $(xy)^P = 1$.*

Proof. By repeated commutation and collecting powers of Q, one obtains that $(xy)^P = Q^{-P(P-1)/2} x^P y^P = Q^{-P(P-1)/2}$. This equals 1 if P is odd. □

Corollary 5.2.7. *$c_{v_k}^{P} = 1$ if P is odd.*

Proof. The proof follows by inducting over the length of the product c_{v_k} and repeatedly applying Proposition 5.2.6. More plainly, c_{v_k} is a product of elements whose Pth powers are 1, and whose pairwise commutator $xyx^{-1}y^{-1}$ is a Pth root of unity, hence its Pth power is also 1. □

In what follows, we will assume that P is odd, so that the braid-like operators are invariant under shifting of indices. By the form of the sum, the B_{kl} operators satisfy the following proposition.

Proposition 5.2.8. *Suppose P is odd.*

$$c_{\mathbf{v}_k} B_{kl} = B_{kl} c_{\mathbf{v}_l}^{-1}. \tag{5.2.5}$$

Proof. By shifting indices by 1 and applying Proposition 5.2.6. □

Corollary 5.2.9. *Suppose P is odd.*

$$c_{\mathbf{v}_k}^{-a} B_{kl} = B_{kl} c_{\mathbf{v}_l}^{a} \tag{5.2.6}$$

for any $a \in \mathbb{Z}_P$.

Proof. By multiple applications of Proposition 5.2.8 and the regularity condition of Proposition 5.2.6. □

Corollary 5.2.10. *Suppose P is odd.*

$$c_{\mathbf{v}_l}^{-a} B_{kl}^{\dagger} = B_{kl}^{\dagger} c_{\mathbf{v}_k}^{a} \tag{5.2.7}$$

for any $a \in \mathbb{Z}_P$.

Proof. It follows by taking the adjoint of equation 5.2.6. □

We now prove a commutation relation which is *not* dependent on the regularity condition.

Proposition 5.2.11. *Let P be any positive integer at least two. Then B_{kl} and $B_{kl}^{\dagger}$ commute with $c_{\mathbf{v}_k} c_{\mathbf{v}_l}^{-1}$.*

Proof. Since B_{kl} can be rewritten as a sum of terms of the form $z_{kl}(c_{\mathbf{v}_k} c_{\mathbf{v}_l}^{-1})^a$, where z_{kl} is a constant depending on k, l and a, it follows that it commutes with $c_{\mathbf{v}_k} c_{\mathbf{v}_l}^{-1}$. The same argument applies to $B_{kl}^{\dagger}$. □

Corollary 5.2.12. *Let P be any positive integer at least two. Then B_{kl} and $B_{kl}^{\dagger}$ commute.*

Proof. Each term in B_{kl} can be written as a power of $c_{\mathbf{v}_k} c_{\mathbf{v}_l}$ times a complex coefficient. Applying Proposition 5.2.11 for $B_{kl}^{\dagger}$, and linearity, it follows that $B_{kl} B_{kl}^{\dagger} = B_{kl}^{\dagger} B_{kl}$. □

We can use a direct approach to compute $B_{kl}^{\dagger} B_{kl}$. The following proposition shows that under a nondegeneracy condition for the basis vectors $\mathbf{v}_k$ of a code C, it follows the braid-like operators B_{kl}, $B_{kl}^{\dagger}$ are *unitary*. The nondegeneracy condition is that Q_{kl} be a primitive Pth root of unity. In the special case that P is prime, this means that $Q_{kl} \neq 1$. Furthermore, if $Q_{kl} = 1$, the B_{kl}'s are proportional to projection operators; in the prime case, this provides a converse statement, which is that B_{kl} is unitary only if $Q_{kl} \neq 1$.

Proposition 5.2.13. *Assume P is odd. Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{Z}_P^d$ be linearly independent vectors. Set*

$$Q_{kl} = q^{\sum_{i,j=1}^{d} \varepsilon_{ij} v_k^i v_l^j} \tag{5.2.8}$$

where v_k^i and v_l^j denote the ith and jth coordinates of $\mathbf{v}_k$ and $\mathbf{v}_l$, respectively.

If Q_{kl} is a ***primitive*** *Pth root of unity, then B_{kl}, $B_{kl}^{\dagger}$ are unitary. In the special case that P is prime, Q_{kl} is a primitive Pth root of unity if and only if $Q_{kl} \neq 1$. On the other hand, if $Q_{kl} = 1$, i.e. $c_{\mathbf{v}_k}$ and $c_{\mathbf{v}_l}$ commute, then B_{kl} is proportional to a projection, specifically, B_{kl} is self-adjoint ($B_{kl} = B_{kl}^{\dagger}$), and $B_{kl}^2 = \sqrt{P} B_{kl}$.*

Proof. Set $Q_{kl} = q^{\sum_{i,j=1}^{d} \varepsilon_{ij} v_k^i v_l^j}$, where v_k^i and v_l^j denote the ith and jth coordinates of $\mathbf{v}_k$ and $\mathbf{v}_l$, respectively. Then using the fact that $B_{kl}^\dagger$ and B_{kl} commute (by Corollary 5.2.12),

$$B_{kl}^\dagger B_{kl} = B_{kl} B_{kl}^\dagger = \frac{1}{P} \sum_{i,j=0}^{P-1} c_{\mathbf{v}_k}^{i} c_{\mathbf{v}_l}^{-i} c_{\mathbf{v}_l}^{j} c_{\mathbf{v}_k}^{-j} \tag{5.2.9}$$

$$= \frac{1}{P} \sum_{i,j=0}^{P-1} c_{\mathbf{v}_k}^{i} c_{\mathbf{v}_l}^{j-i} c_{\mathbf{v}_k}^{-j} \tag{5.2.10}$$

$$= \frac{1}{P} \sum_{i,j=0}^{P-1} Q_{kl}^{(j-i)j} c_{\mathbf{v}_k}^{i-j} c_{\mathbf{v}_l}^{j-i} \tag{5.2.11}$$

$$= \frac{1}{P} \sum_{a,j=0}^{P-1} Q_{kl}^{aj} c_{\mathbf{v}_k}^{-a} c_{\mathbf{v}_l}^{a} \tag{5.2.12}$$

by Proposition 5.2.5 and re-indexing using Proposition 5.2.6. We can first perform the sum over j. Taking first the special case that P is prime, there are two cases, $Q_{kl} = 1$ and $Q_{kl} \neq 1$, corresponding to $\sum_{i,j=1}^{d} \varepsilon_{ij} v_k^i v_l^j$ being 0 mod P or nonzero mod P. If $Q_{kl} \neq 1$, Q_{kl} is a primitive P-root of unity if P is prime. In the first case, $Q_{kl} = 1$, the resulting sum yields that B_{kl} is actually self-adjoint, since $c_{\mathbf{v}_k}$ commutes with $c_{\mathbf{v}_l}$, and so $B_{kl} = B_{kl}^\dagger$. Hence, summing over j yields a factor of P, and one obtains that

$$B_{kl}^2 = \sum_{a=0}^{P-1} c_{\mathbf{v}_k}^{-a} c_{\mathbf{v}_l}^{a} = \sqrt{P} B_{kl}. \tag{5.2.13}$$

if $Q_{kl} = 1$. If $Q_{kl} \neq 1$, then the sum over j is P if $a = 0$, and otherwise equal to 0, since $\sum_{j=0}^{P-1} Q_{kl}^{aj} = \frac{Q_{kl}^{aP}-1}{Q_{kl}^{a}-1} = 0$. Note that P being prime guarantees that $Q_{kl}^a \neq 1$ for $a \neq 0$.

In the case that P is not prime, suppose Q_{kl} is a primitive Pth root of unity. Then $Q_{kl}^{aj} = 1$ if and only if $aj = 0$ (mod P). Then $\sum_{j=0}^{P-1} Q_{kl}^{aj} = \frac{Q_{kl}^{aP}-1}{Q_{kl}^{a}-1} = 0$ if $a \neq 0$ and equals P if $a = 0$. Thus, only the constant term in the sum survives, which is 1. This again shows that $B_{kl}^\dagger B_{kl} = B_{kl} B_{kl}^\dagger = 1$.

If, on the other hand, for general P, we have that $Q_{kl} = 1$, then $B_{kl}^2 = \sqrt{P}B_{kl}$, by the same computation as in equation 5.2.13. □

Another proof of unitarity can be given using Proposition 5.2.8, combined with Corollary 5.2.4. This strategy requires a suitable generalization of Proposition 3.3.2, which stated that the generalized Clifford algebra generated by $c_1, c_2, \ldots, c_{2n-1}, c_{2n}$ has trivial center. This proposition was so crucial for obtaining results in Chapter 3 that we described it as a "golden" rule. So now we need a more generalized golden rule. The appropriate generalization of Proposition 3.3.2 is to replace the GCA generators $c_1, c_2, \ldots, c_{2d}$ with $c_{\mathbf{v}_1}, c_{\mathbf{v}_2}, \ldots, c_{\mathbf{v}_r}$, and impose a suitable nondegeneracy condition that depends on the full-rank property of an antisymmetric matrix (mod P) formed out of the vector basis $\mathbf{v}_i$.

Proposition 5.2.14 (Generalized Golden Rule). *Let $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_r \in \mathbb{Z}_P^d$ be a set of linearly independent vectors, where P is a positive integer at least two. Define the matrix $\boldsymbol{F}$ with the matrix elements*[1]

$$F_{kl} = \sum_{a,b=1}^{d} \varepsilon_{ab} \boldsymbol{v}_k^a \boldsymbol{v}_l^b. \tag{5.2.14}$$

Then the algebra generated by $c_{\boldsymbol{v}_1}, c_{\boldsymbol{v}_2}, \ldots, c_{\boldsymbol{v}_r}$ has trivial center if and only if $\boldsymbol{F}$ (mod P) is full rank in $\mathbb{Z}_P^d \times \mathbb{Z}_P^d$.

Proof. Any element x of the algebra may be represented in a canonical form by the expression $x = \sum_{i_1,i_2,\ldots,i_r=0}^{P-1} a_{i_1,i_2,\ldots,i_r} c_{\mathbf{v}_1}^{i_1} c_{\mathbf{v}_2}^{i_2} \cdots c_{\mathbf{v}_r}^{i_r}$. Furthermore, by Proposition 3.3.2, $x = y$ if and only if the coefficients in the normal form agree with each other. Suppose x lies in the center of the algebra generated by $c_{\mathbf{v}_1}, c_{\mathbf{v}_2}, \ldots, c_{\mathbf{v}_r}$. We assume $x \neq 0$ (otherwise, it commutes trivially with the whole algebra), so there is a tuple $(i_1, i_2, \cdots, i_r)$ such that $a_{i_1,i_2,\ldots,i_r} \neq 0$. Then setting $xc_{\mathbf{v}_1} = c_{\mathbf{v}_1}x$ and comparing coefficients yields that $a_{i_1,i_2,\ldots,i_r} Q_{21}^{i_1} Q_{31}^{i_2} \cdots Q_{r1}^{i_r} = a_{i_1,i_2,\ldots,i_r}$. Since $a_{i_1,i_2,\ldots,i_r} \neq 0$, it follows that $Q_{21}^{i_1} Q_{31}^{i_2} \cdots Q_{r1}^{i_r} = 1$. Thus, using equation 5.2.8, we obtain that

[1] Again, we are using the upper index to denote the coordinate of the corresponding vector $\mathbf{v}_k$.

$\sum_{l\neq 1} i_l \sum_{a,b=1}^{d} \varepsilon_{ab} v_1^a v_l^b = 0$ (mod P). Noting that $F_{kk} = 0$ by the asymmetry of ε_{ab}, we can write this equation as $\sum_{l=1}^{r} F_{1,l} i_l = 0$ (mod P). More generally, setting $xc_{\mathbf{v}_k} = c_{\mathbf{v}_k}x$, one obtains that

$$\sum_{l=1}^{r} F_{kl} i_l = 0 \text{ (mod P)} \tag{5.2.15}$$

for $k = 1, 2, \ldots, r$. The statement that the only solution mod P is given by $(i_1, i_2, \ldots, i_r) = (0, 0, \ldots, 0)$ is equivalent to the statement that $\mathbf{F}$ (mod P) is full-rank in $\mathbb{Z}_P^d \times \mathbb{Z}_P^d$.

□

It is interesting to observe that the full-rank condition for Proposition 5.2.14, in terms of the full-rank of a matrix depending on the code basis, is the appropriate generalization of the condition for Proposition 5.2.13. The following corollary demonstrates this fact.

Corollary 5.2.15. *Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{Z}_P^d$ be linearly independent vectors, where P is a positive integer at least two. Taking the special case $r = 2$, the full-rank property of $\mathbf{F}$(mod P) reduces to the condition that $c_{\mathbf{v}_1}$ and $c_{\mathbf{v}_2}$ do not commute with each other. Thus, the algebra generated by $c_{\mathbf{v}_1}$ and $c_{\mathbf{v}_2}$ has trivial center if and only if $Q_{12} \neq 1$, i.e. $F_{12} \neq 0$ (mod P).*

Proof. Taking $r = 2$, if $F_{12} = 0$ (mod P), then $F_{21} = -F_{12} = 0$ (mod P), and $\mathbf{F}$ (mod P) is certainly not full-rank. Conversely, if $\mathbf{F}$ (mod P) is not full-rank, then the only possibility is that $F_{12} = 0$ (mod P). □

Using the above framework, one can now adapt the approach presented by the dissertation author in Chapter 3 to show the unitarity of b_{kl}, to now show the unitarity of B_{kl}. Namely, we simply need to show that $B_{kl}^{\dagger} B_{kl}$ (alternately, the equal expression $B_{kl} B_{kl}^{\dagger}$) lies in the center of the algebra generated by $c_{\mathbf{v}_k}$ and $c_{\mathbf{v}_l}$, and that the constant term is 1.

Proposition 5.2.16. *Suppose P is odd. Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{Z}_P^d$ be linearly independent vectors, and suppose $Q_{kl} \neq 1$, where Q_{kl} is as defined above. Then $B_{kl}^{\dagger} B_{kl}$ (alternately, the equal expression*

$B_{kl}B_{kl}^\dagger$) lies in the center of the generalized Clifford algebra generated by $c_{\boldsymbol{v}_k}$ and $c_{\boldsymbol{v}_l}$ and its constant term is 1*.*

Proof. To prove that $B_{kl}^\dagger B_{kl}$ lies in the center of the generalized Clifford algebra generated by $c_{\mathbf{v}_k}$ and $c_{\mathbf{v}_l}$, we simply need to show that $B_{kl}^\dagger B_{kl}$ commutes with all elements of the form $c_{\mathbf{v}_k}^a c_{\mathbf{v}_l}^b$, and then use linearity to extend this to the statement that $B_{kl}^\dagger B_{kl}$ commutes with any element of the form $\sum_{a,b=1}^r \alpha_{ab} c_{\mathbf{v}_k}^a c_{\mathbf{v}_l}^b$, which is in fact the whole algebra generated by $c_{\mathbf{v}_k}$ and $c_{\mathbf{v}_l}$.

To show this fact, we first use the fact that any $c_{\mathbf{v}_k}^a c_{\mathbf{v}_l}^b$ can be written as $z(c_{\mathbf{v}_k} c_{\mathbf{v}_l}^{-1})^a c_{\mathbf{v}_l}^{a+b}$ where z is a constant. By Proposition 5.2.11, it follows that $(c_{\mathbf{v}_k} c_{\mathbf{v}_l}^{-1})^a$ commutes with both B_{kl} and $B_{kl}^\dagger$, and hence with their product. Thus, we only need to show that $c_{\mathbf{v}_l}$ commutes with $B_{kl}^\dagger B_{kl}$. Applying Corollary 5.2.9 and 5.2.10 of Proposition 5.2.8, it follows that $B_{kl}^\dagger B_{kl} c_{\mathbf{v}_l} = B_{kl}^\dagger c_{\mathbf{v}_k}^{-1} B_{kl} = c_{\mathbf{v}_l} B_{kl}^\dagger B_{kl}$, which shows that $c_{\mathbf{v}_l}$ commutes with $B_{kl}^\dagger B_{kl}$.

To show that the constant term is 1, observe that $B_{kl}^\dagger B_{kl} = B_{kl} B_{kl}^\dagger = \frac{1}{P} \sum_{i,j=0}^{P-1} c_{\mathbf{v}_k}^i c_{\mathbf{v}_l}^{-i} c_{\mathbf{v}_l}^j c_{\mathbf{v}_k}^{-j}$ yields that the constant term is 1 by plugging in $i - j = 0$. Note that no other terms contribute to the constant term since $\mathbf{v}_k$ and $\mathbf{v}_l$ are assumed to be linearly independent in $\mathbb{Z}_P^d$. □

Corollary 5.2.17. *Suppose P is odd. Let $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathbb{Z}_P^d$ be linearly independent vectors, and suppose $Q_{kl} \neq 1$, where Q_{kl} is as defined above. Then B_{kl} is unitary.*

Proof. This follows by application of the generalized golden rule, Proposition 5.2.14, to Proposition 5.2.16. □

5.3 Conclusion

Thus, we have shown that one can generalize the approach used in Ch. 3 for the full generalized Clifford algebra to subalgebras of the generalized Clifford algebra induced by lattices subject to a particular full-rank condition. We built new unitary operators B_{kl}, which we called braid-like due to their similar sum construction to the *bona fide* braid group elements from Ch.

3. We envision these unitary operators as the first step to designing building blocks of unitary operations that are intrinsic to the lattice structure.

References

[1] Artin, E. (1925). Theory of braids. *Hamburger Abh.*, 4, 47–72.

[2] Bartolomei, H., Kumar, M., Bisognin, R., Marguerite, A., Berroir, J. M., Bocquillon, E., Plaçais, B., Cavanna, A., Dong, Q., Gennser, U., Jin, Y., & Fève, G. (2020). Fractional statistics in anyon collisions. *Science*, 368(6487).

[3] Choi, M. D. (1975). Completely positive linear maps on complex matrices. *Linear Algebra Appl.*, 10, 285–290.

[4] Cobanera, E. & Ortiz, G. (2014). Fock parafermions and self-dual representations of the braid group. *Physical Review A - Atomic, Molecular, and Optical Physics*, 89(1).

[5] Coecke, B. & Duncan, R. (2008). Interacting quantum observables. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5126 LNCS.

[6] Coecke, B. & Duncan, R. (2011). Interacting quantum observables: Categorical algebra and diagrammatics. *New Journal of Physics*, 13.

[7] Cui, S. X., Ding, D., Han, X., Penington, G., Ranard, D., Rayhaun, B. C., & Shangnan, Z. (2020). Kitaev's quantum double model as an error correcting code. *Quantum*, 4, 331.

[8] Drinfeld, V. (1986). Quantum groups. In *Proceedings of the International Congress of Mathematicians (Berkeley, 1986)*, volume 1 (pp. 789–820).: American Mathematical Society.

[9] Fourier, J. (1827). Histoire de l'académie, partie mathématique (1824). *Mémoires de l'Académie des sciences de l'Institut de France*, 7.

[10] Goldschmidt, D. M. & Jones, V. F. (1989). Metaplectic link invariants. *Geometriae Dedicata*, 31, 165–191.

[11] Gottesman, D. (1997). Stabilizer codes and quantum error correction. PhD thesis.

[12] Gottesman, D. & Chuang, I. L. (1999). Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760), 390–393.

[13] Haagerup, U. (1978). An example of a non nuclear c*-algebra, which has the metric approximation property. *Inventiones mathematicae*, 50(3), 279–293.

[14] Hansen, E. R. (1975). *A table of series and products*. Prentice Hall.

[15] Jaffe, A. & Liu, Z. (2017). Planar para algebras, reflection positivity. *Communications in Mathematical Physics*, 352(1).

[16] Jaffe, A., Liu, Z., & Wozniakowski, A. (2018). Holographic software for quantum networks. *Science China Mathematics*, 61(4).

[17] Jaffe, A. M. & Liu, Z. (2018). Mathematical picture language program. *Proceedings of the National Academy of Sciences of the United States of America*, 115(1).

[18] Janusz, G. J. (1966). Primitive idempotents in group algebras. *Proceedings of the American Mathematical Society*, 17(2), 520–523.

[19] Jones, V. F. (1989). On a certain value of the Kauffman polynomial. *Communications in Mathematical Physics*, 125.

[20] Junge, M., Palazuelos, C., Parcet, J., & Perrin, M. (2017). Hypercontractivity in group von Neumann algebras. *Mem. Amer. Math. Soc.*, 249(1183), xii+83.

[21] Khesin, A. B., Lu, J. Z., & Shor, P. W. (2022). Publicly verifiable quantum money from random lattices. arXiv:2207.13135.

[22] Kitaev, A. Y. (2003). Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1), 2–30.

[23] Kwaśniewski, A. K. (2001). On generalized Clifford algebras and spin lattice systems. *Acta Physica Polonica B*, 32(5).

[24] Lin, R. (2021a). An algebraic framework for multi-qudit computations with generalized Clifford algebras. arXiv:2103.15324.

[25] Lin, R. (2021b). A graphical calculus for quantum computing with multiple qudits using generalized Clifford algebras. arXiv:2103.16081.

[26] Lin, R. (2021c). Certain linear combinations of exponential functions are positive under semidefinite linear constraints. arXiv:2112.00134.

[27] Lin, R. & Boretsky, J. (2022). Kraus-like decompositions. arXiv:2204.06741.

[28] Morinaga, K. & Nōno, T. (2019). On the linearization of a form of higher degree and its representation. *Hiroshima Mathematical Journal*, 16.

[29] Morris, A. O. (1967). On a generalized Clifford algebra. *Quarterly Journal of Mathematics*, 18(1).

[30] Morrison, K. E. (1998). A generalization of circulant matrices for non-abelian groups. Research report.

[31] Müger, M. (2003). From subfactors to categories and topology ii: The quantum double of tensor categories and subfactors. *Journal of Pure and Applied Algebra*, 180(1-2).

[32] Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-quantum lattice-based cryptography implementations: A survey. *ACM Comput. Surv.*, 51(6).

[33] Neshveyev, S. & Størmer, E. (2006). *Dynamical entropy in operator algebras*, volume 50 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. [Results in Mathematics and Related Areas. 3rd Series.] A Series of Modern Surveys in Mathematics*. Springer-Verlag, Berlin.

[34] Nielsen, M. A. & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press. Tenth anniversary edition.

[35] Popa, S. (1995). An axiomatization of the lattice of higher relative commutants of a subfactor. *Inventiones Mathematicae*, 120(1).

[36] Popovici, I. & Gheorghe, C. (1966). Algèbres de clifford généralisées. *C. R. Acad. Sci. Paris*, 262, 682–685.

[37] Prakash, S. (2020). Magic state distillation with the ternary golay code: Distillation with the ternary golay code. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 476(2241).

[38] Schoenberg, I. J. (1938). Metric spaces and positive definite functions. *Transactions of the American Mathematical Society*, 44(3), 522–536.

[39] Schwinger, J. (1970). *Particles, sources, and fields*, volume 1. Perseus Books Publishing, L.L.C.

[40] Stinespring, W. F. (1955). Positive functions on C^*-algebras. *Proc. Amer. Math. Soc.*, 6, 211–216.

[41] Temperley, H. & Lieb, E. (1971). Relations between the 'percolation' and 'colouring' problem and other graph-theoretical problems associated with regular planar lattices: some exact results for the 'percolation' problem. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 322(1549).

[42] Uhlmann, A. (1977). Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory. *Comm. Math. Phys.*, 54(1), 21–32.

[43] van den Berg, C. & Forst, G. (1975). *Potential Theory on Locally Compact Abelian Groups*. Springer.

[44] Wirth, M. (2022). Christensen-Evans theorem and extensions of GNS-symmetric quantum markov semigroups. arXiv:2203.00341.

[45] Yamazaki, K. (1964). On projective representations and ring extensions of finite groups. *J. Fat. Sci. University of Tokyo*, Set I(10), 147–195.

[46] Yang, C. N. (1967). Some exact results for the many-body problem in one dimension with repulsive delta-function interaction. *Physical Review Letters*, 19(23).