An algebro-geometric study of two models of quantum computation

by Raeez Lorgat


Submitted to the
Department of Electrical Engineering and Computer Science
in Partial Fulfillment of the Requirements for the Degree of
Master of Engineering in Electrical Engineering and Computer Science

at the
Massachusetts Institute of Technology

September 2017

© 2017 Raeez Lorgat. All rights reserved.

The author hereby grants to M.I.T. permission to reproduce and to distribute publicly paper and
electronic copies of this thesis document in whole and in part in any medium now known or
hereafter created.
AN ALGEBRO-GEOMETRIC STUDY OF TWO MODELS OF QUANTUM COMPUTATION

RAEZZ LORGAT

ABSTRACT. We investigate geometric aspects of two models of quantum computation: starting with i. the computational complexity of the particle excitations of topological phases of matter in the restricted model of a Topological Quantum Field Theory in the sense of Turaev before leading to ii. where in analogy with ideas of Nielsen et. al., we propose and study a geometric model for Grover's search algorithm. i. presents fundamental results in the mathematics and physics literature on conformal field theory as a model for quantum computation, phrased within the algebraic framework of the theory of tensor categories. Our main questions are 1. how does the computational power of these excitations change as a function of the genus of a fixed 2-dimensional space-time? and 2. independent of any particular space-time, what structural properties of a TQFT govern its computational power?

When restricted to a space-time with space-like degrees of freedom represented by a smooth surface of genus g, we answer the first question by observing a $q^g$-fold degeneracy in the ground state of the TQFT resulting from the presence of abelian anyons with exchange statistics a $q$-th root of unity. Such a resource is a topologically fault-tolerant quantum memory. The abelian character of the emergent particle statistics leads us to answer the second question via an algebraic realization of non-abelian anyonic excitations in the language of unitary modular tensor categories. Subsequently, ii. studies the quantum mechanical evolution of a particle within the Schröedinger wave-function formalism of quantum mechanics: our primary result is a purely geometric proof of the optimality of Grover's Search Algorithm on n qubits obtained via a study of the geometric structure of a homogenous space for the Unitary group of transformations acting on a single qubit.

Date: September 5, 2017.
AN ALGEBRO-GEOMETRIC STUDY OF TWO MODELS OF QUANTUM COMPUTATION

CONTENTS

List of Figures 4
List of Tables 4

Part 1. Introduction 5
1. On Models of Quantum Computation in the presence of symmetry 5

Part 2. Computation in the setting of infinite dimensional infinitesimal symmetry 7
1.1. Computing with Anyons 7
2. The Computational Power of a TQFT 10
2.1. Universality and Density of the Braid Group Representations 10
2.2. Universality of a Given UMTC 11
2.3. Classification of UMTCs of Low Rank 12
3. Toric Code and Abelian Anyons 14
3.1. Toric Code 14
3.2. Anyons and The Toric Code 16
3.3. Abelian Anyons on a Surface: A Generalization 17
4. Conclusion 19

Part 3. Computation in the setting of finite dimensional group symmetry 21
5. Introduction 21
6. The Computational Metric 22
7. Grovers Algorithm as a geodesic on Projective Space 24
8. Deformations of Grover's algorithm 26
9. Conclusion 30

Part 4. Appendices 31
A: The Braid Group 31
B: The Fibonacci Theory \( F \) 32
Appendix C: TQFT and Unitary Modular Tensor Categories

$\mathcal{C}$ is a Semi-Simple Ribbon Category with finitely many isomorphism classes of simple objects

Braid Group Representations and non-triviality of UMTCs

Unitarity, Modularity and TQFTs

References

LIST OF FIGURES

1. Particle world-lines tracing out a braid. 8
2. Fusion of multiple $\tau$ particles. 33
3. Braiding of two $\tau$ particles. 34
4. Braid Transposition. 38

LIST OF TABLES

1. Classification of low-rank Unitary Modular Tensor Categories. 14
AN ALGEBRO-GEOMETRIC STUDY OF TWO MODELS OF QUANTUM COMPUTATION

Part 1. Introduction

1. ON MODELS OF QUANTUM COMPUTATION IN THE PRESENCE OF SYMMETRY

In order to productively analyse any proposal for a process effecting a computation, we first need to establish a rigorous framework within which we may define the basic constituents of and measure the resulting effects of the proposed process. Such a framework is typically known as a model of computation.

This thesis investigates two particular models of quantum computation: one of an inherently finite dimensional nature and admitting a description in terms of the Schröedinger or Hamiltonian formalisms of quantum mechanics and another possessing infinitely many degrees of freedom and subject to a description within the formalism of conformal field theory with gauge symmetry.

From a purely mathematical point of view, our study of the two models is motivated by and fits naturally within the classification of Kac-Moody algebras. We recall[3] the notion of generalized cartan matrix \( A \), which is an \( n \times n \) square matrix \( A = (a_{ij}) \) with integer entries \( a_{ij} \in \mathbb{Z} \) satisfying

1. the diagonal entries \( a_{ii} = 2 \).
2. the non-diagonal entries \( a_{ij} \leq 0 \)
3. \( a_{ij} = 0 \) if and only if \( a_{ji} = 0 \);

Furthermore, such a matrix \( A \) is termed symmetrizable if \( A \) can be expressed as a product of matrices \( D \cdot S \) where \( D \) is a diagonal matrix and \( S \) is a symmetric matrix.

To any such matrix \( A \) one can construct an algebra \( g(A) \) known as the Kac-Moody algebra associated to \( A \). Such an object may be generated from a \( 3n \)-dimensional complex vector space \( g(A) \) with a basis

\[ e_i, f_i, h_i \]

and equipped with a non-commutative (non-associative) product known as the lie bracket

\[ [\cdot, \cdot] : g(A) \times g(A) \rightarrow g(A) \]
subject to a set of defining relations, which include

\[ [h_i, h_j] = 0, [e_i, f_i] = 0 \text{ if } i \neq j \]

\[ [h_i, e_j] = a_{ij} e_j, [h_i, f_j] = -a_{ij} f_j, \]

These algebras play fundamental roles in the study of symmetry throughout mathematics and physics; in particular, they may be interpreted as the structures governing the \textit{infinitesimal symmetries} present in the dynamics of classical and quantum theories of fields and mechanics.

As suggested by the presentation above, these algebraic objects are classified by the generalized Cartan matrix $A$, and the two given models we investigate fits into the specialized scenarios:

(1) where all the principle minors of $A$ are positive and $g(A)$ is subsequently finite dimensional, recovering, for example, the familiar examples of finite dimensional semi-simple lie algebras

(2) the principle minors of $A$ are non-negative and $g(A)$ is infinite dimensional, but is of \textit{polynomial growth}, a class known as the \textit{affine lie algebras}

Within the framework of Kac-Moody algebras, our investigations may equally be phrased in terms of the geometric representation theory of kac-moody algebras. The geometry analysed in each case forms a \textit{symmetric space} for the corresponding symmetry modeled by the algebra $g(A)$. However, we will refrain from going into the details of the generality of Kac-Moody algebras in this thesis, instead relying on their classification as motivation and context for the specialized scenarios we will investigate: i.e. in particular Part 3 investigates the geometry of the complex projective space as a symmetric space admitting an action of the group of invertible Unitary matrices; in turn, these symmetric spaces can be understood locally in terms of the lie algebras $su_n$; we say that the space is \textit{uniformized} by the given lie algebra. Our main result is consequently a purely geometric proof of the optimality of \textit{grover's search algorithm} in terms of the geometry of the homogenous space for the corresponding finite dimensional unitary group. In Part 2 we study
AN ALGEBRO-GEOMETRIC STUDY OF TWO MODELS OF QUANTUM COMPUTATION

the geometry of particle excitations on genus \( g \) surfaces, which are controlled by
the infinitesimal symmetry given by the family of infinite dimensional affine lie
algebras \( \hat{\mathfrak{g}} \); here the homogenous space is given (implicitly) by the space of all \( G \)-
bundles on the topological surface, and is known as the (global form of the) affine
grassmannian. In each of these cases our point of view is shaped by the representation theory of the associated kac-moody algebra appearing in the classification
given above.

Given that the algebraic study of symmetry forms our departure point, the content of this thesis may equally be presented as a change in point-of-view: instead of the usual combinatorial or algorithmic framework as the point of departure, we find it instead fruitful to frame our study in the context of representation theory.

The next two parts of this thesis are each structured as follows: we fix the symmetry present in our model of computation in the onset, and then subsequently investigate the resulting properties of the model. An indication of the benefit of this point of view can be seen for example in Part 3 where, in contrast to the usual approach, we derive a purely geometric proof of the optimality of the now-classical grover's search algorithm.

Part 2. Computation in the setting of infinite dimensional infinitesimal
symmetry

1.1. Computing with Anyons. A characteristic property of quantum particles is
the set indistinguishability of identical particles. All photons in the world share
the same dynamical behaviour: for any system composed of multiple identical
photons a permutation of the positions of any two photons cannot have any effect
on the dynamics of the system as a whole. It follows that \( S_n \), the symmetric group
on \( n \) elements acts on an ensemble of \( n \) identical particles as a symmetry of the
composite system; physically, we observe the system's wave function remain un-
changed save for an anomalous total phase. In this way Unitarity of our physical
theories shows the resulting transform of the wave function is an element of the
group $U(1)$ i.e. transforms by scalar multiplication by a complex phase $e^{i\theta}$.

It is well-known that particle exchanges in three-dimensional space transform in precisely two flavours, each corresponding to one of two 1-dimensional irreducible representations of $S_n$. If the particles are bosons (e.g. photons), then an exchange of two particles is represented by the identity symmetry: the wave function is invariant, and the particles obey Bose statistics. If the particles are fermions (e.g. electrons in a metal), then the action of exchange is represented on the wave function as a multiplication by $-1$ i.e. the wave function changes sign. Correspondingly, the particles obey Fermi statistics.

However, in a space-time restricted to two spatial dimensions we instead find a wealth of exotic particle statistics. The restricted topology of a surface imposes a topological change to the symmetry in exchanging two particles; the exchange symmetry group is no longer modeled by the symmetric group $S_n$, but instead by the braid group $B_n$ (See Appendix A), as depicted in Figure 1.1. Vertical displacement is in the time direction and the $n$ particles are subjected to movement exchanging their positions from $a_i$ to $b_i$. The braids are formed from the individual particle’s world-lines.

![Figure 1. Particle world-lines tracing out a braid.](image)

Contrary to $S_n$, the infinite group $B_n$ has infinitely many one-dimensional irreducible unitary representations, each corresponding to a choice of phase $e^{i\theta}$. We see that for $\theta = 0$ and $\theta = \pi$ we recover bosonic and fermionic particles, but for every other choice of $\theta$ we find a new particle. As these particles can obtain any change of phase upon permutation they have been dubbed anyons.
Furthermore, in certain topological quantum field theories (henceforth TQFTs) we find that the higher dimensional representations of $B_n$ manifest themselves in an even more exotic type of particle; in contrast to those anyons that transform according to a one dimensional unitary representation i.e. according to a phase $e^{i\theta}$ in the abelian group $U(1)$, these non-abelian particles transform according to a representation $V_d$ of $B_n$ in some non-abelian unitary group $U(d)$ where $d > 1$ is the dimension of the corresponding representation. Fixing $V_d$, a pair of anyons of type $V_d$ with movement confined to a surface trace out a topologically non-trivial braid formed by the particle's world-lines. This braid then corresponds via the representation to an element $U(d)$. These anyonic particles carry an intrinsic computational resource that is purely topological in nature. According to the unitary representation of $B_n$ that they are modeled by, each particle carries internal degrees of freedom, and this state can be transformed by appropriately braiding the particles by moving them in 2-dimensional space-time. We will restrict our study to this particular computational resource afforded by a TQFT.

**Remark (On our treatment of TQFTs).** In order to not move too far afield, we focus on the strictly 2-dimensional part of a $2+1$-dimensional TQFT i.e. its anyonic excitations and corresponding braiding statistics. Furthermore, since a Unitary Modular Tensor Category (UMTC) in the sense of Turaev corresponds uniquely to a TQFT, we will instead work with UMTCs. Appendices B and C contain an informal discussion of TQFT and UMTCs in general. For a complete treatment, see [16] and [17].

The rest of this part is divided into two sections: a review of the structure and classification of $2+1$-dimensional TQFTs as it relates to the computational power of the TQFT, followed by a discussion of a fault-tolerant quantum memory in the topological degeneracy held by abelian anyons braided on a genus $g$ surface. Here we find that changing the topology of the surface does not change the range of
computations possible, but instead adds $q^9$ degrees of freedom not accessible via local operations.

2. The Computational Power of a TQFT

2.1. Universality and Density of the Braid Group Representations. Given that each UMTC $\mathcal{C}$ (see Appendix C) models a topological state of matter, it follows that the computational power of the nonabelian statistics of an anyon native to a given $2+1$-dimensional TQFT modeled by $\mathcal{C}$ is governed by the algebraic structure of $\mathcal{C}$. Much like a choice of gate set in the standard Quantum Circuit Model may or may not afford efficient approximation of any quantum algorithm, the choice of UMTC governs the availability of a non-abelian anyon with braiding statistics supporting implementation of any quantum algorithm.

More precisely: given an object $V$ in $\mathcal{C}$, the structure of a UMTC affords a homomorphism from the group algebra of the braid group

$$CB_n \rightarrow \text{End}(V^\otimes n)$$

acting on braid group generators $\sigma_i$ (See Appendix A) as

$$\sigma_i \mapsto \text{Id}_V^\otimes i-1 \otimes \sigma_{V,V} \otimes \text{Id}_V^\otimes n-i-1$$

where $\sigma_{V,V}$ denotes the braiding homomorphism

$$V \otimes V \rightarrow V \otimes V.$$ 

Furthermore, naturality of the braiding homomorphism implies compatibility of braiding with the Hilbert Space structure on $\text{End}(V^\otimes n)$. It follows that the left action of $\text{End}(V^\otimes n)$ on itself induces a unitary representation

$$B_n \rightarrow U(\text{End}(V^\otimes n)).$$
Thus for a given anyon type modeled by $V$, choosing $m, n \in \mathbb{N}$ anyons to encode one and two qubits respectively yields braid group representations of $B_m$ and $B_n$ in $\text{End}(V^\otimes m)$ and $\text{End}(V^\otimes n)$. If each of these representations have their images dense in the special unitary group, then we can apply the Solovay-Kitaev theorem to approximate any desired unitary to $\epsilon$ precision in a braid word of length $\text{poly}(\log(\frac{1}{\epsilon}))$.

**Example 2.1.**

Freedman, Larsen and Wang characterize the images of the Jones representations of the Braid group in [11], deriving as corollary in [12] that the UMTC $C(sl_2, e^{\pi i \frac{15}{2}})$ consisting of highest weight representations obtained as a subquotient of the representation category of the Quantum Group $U_q sl_2$ specialized at $q = e^{\pi i \frac{15}{2}}$ is universal. This particular UMTC corresponds to the SU(2)-Chern-Simons-Witten TQFT at level 3, or equivalently the Fibonacci UMTC $\mathcal{F}$ described in Appendix B.

**Example 2.2.** For an example lacking universality, by Jones in [14] the SU(2)-Chern-Simons-Witten TQFT at level 2 has braid group representations with image factoring through a finite group. In this case, the corresponding UMTC is $C(sl_2, e^{\pi i \frac{14}{3}})$.

**2.2. Universality of a Given UMTC.** Due to the divergence in computational power of different UMTCs, it is natural to ask for necessary and sufficient conditions for universality of the computational in a TQFT arising from a UMTC. As of August 2017, this remains an open problem. Recent progress by Etingof, Rowell and Wang have led to a conjectural characterization of UMTCs with braid group representations having exclusively finite image [9]:

**Definition 1.** A UMTC $C$ has property $F$ if the associated representations of $B_n$ on the centralizer algebras $\text{End}(V^\otimes n)$ have finite image for all objects $V$ and all $n \in \mathbb{Z}$. 
In any UMTC $C$ we can associate to objects $X, Y \in \text{Obj}(C)$ and a map $f : X \to Y$ a number called the trace of $f$ denoted $\text{tr } f$. In particular, for the identity map $\text{Id}_V : V \to V$ we can define the dimension $\dim(V) = \text{tr } \text{Id}_V$. For example, for any $V \in \mathcal{V}_k$, $\dim(X) \in \mathbb{N}$ is the standard vector space dimension. Denoting by $\dim(C) = \sum_i \dim(V_i)^2$ the global quantum dimension of $C$, then the conjecture, verified for all known examples, is

**Conjecture 2.1.** A UMTC $C$ has property F if and only if $\dim(C) \in \mathbb{N}$.

Returning to our standard example:

**Example 2.3.** Recall that the Fibonacci UMTC $\mathcal{F}$ was shown to be universal in [11]. Here we have two anyons $1$ and $\tau$, with dimensions

$$\dim(1) = 1 \text{ and } \dim(\tau) = \frac{1 + \sqrt{5}}{2}.$$  

It follows that

$$\dim(\mathcal{F}) = \frac{5 + \sqrt{5}}{2},$$

in accord with $\mathcal{F}$ being universal and hence not having property F.

**2.3. Classification of UMTCs of Low Rank.** Recall the rank of a UMTC $C$ is the number of simple objects in $C$. In [8] Wang conjectured that UMTCs could be classified not only as representation categories of Quantum Groups, but also directly according to their rank. This conjecture was recently proven in [5] and is now called the Rank Finiteness Theorem:

**Theorem 2.2.** There are finitely many isomorphism classes of UMTCs of fixed rank $r$.

The theorem is directly analogous to a classical result of Landau’s: for a fixed number $n \in \mathbb{N}$, there are only finitely many finite groups $G$ with exactly $n$ irreducible complex representations. The proof follows from analysing the class equation

$$|G| = \sum_{i=1}^{n} [G : C(g_i)],$$
dividing by $|G|$ to yield the Diophantine equation

$$1 = \sum_{i=1}^{n} \frac{1}{x_i}$$

which has finitely many solutions in the positive integers thus implying a bound on $|G|$; it follows there are only finitely many such $G$ with $n$ irreducible complex representations. Similarly, for a rank $n$ UMTC $\mathcal{C}$, the proof of the rank finiteness theorem in [5] analyses the equation

$$\dim(\mathcal{C}) = \sum_{i=1}^{n} (\dim(V_i))^2$$

in order to produce a bound on $\dim(\mathcal{C})$ implying a finite possible set of fusion rules for $\mathcal{C}$; a further analysis then reveals finitely many UMTCs having a fixed fusion rule, implying the result.

The Rank Finiteness Theorem suggests the feasibility of a classification of UMTCs by rank. The process of classification can be understood from the axiomatic specification of a UMTC: each axiom imposes a polynomial constraint with $\mathbb{Z}$-coefficients, equating the classification of UMTCs with counting points on certain algebraic varieties (solution sets to polynomial equations). As of December 2015, UMTCs of rank 4 and lower have been classified via the Galois groups associated to them, while in rank 5 all that is known is a list of possible fusion rules. The difficulty of the problem in rank 5 and greater can be described in terms of the higher dimensionality of the algebraic and arithmetic varieties involved [8].

According to the classification in [8], there are 70 UMTCs of rank less than or equal to 4, 10 of which are prime. The rest can be obtained from these 10 by applications of (categorical) direct sum and symmetry transformations. Table 2.3 below describes these, noting that 9/10 of the prime UMTCs are known to arise from a Quantum Group; here we label them according to the construction in [15]. We also explicitly name two UMTCs discussed in this thesis Fibonacci and Toric
Code. Column 3, row 4 is the only UMTC not known to arise as a coset construction from the category of representations of a Quantum Group; see [8] for details.

<table>
<thead>
<tr>
<th></th>
<th>Trivial A</th>
<th>SU(2) _ A</th>
<th>SU(3) _ A</th>
<th>SU(4) _ A</th>
<th>Spin(16) Toric Code A</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TABLE 1.** Classification of low-rank Unitary Modular Tensory Categories.

The ith column classifies rank i UMTCs. In each box we record: [n] the number n of distinct theories in the isomorphism class; the lie group G and level k specifying the TQFT G_k by which the UMTC arises; whether the anyons are abelian (A) or non-abelian (NA); and [U] the presence of a universal braiding anyon.

**Remark.** An example of a topological phase of matter is seen in fractional quantum Hall liquids. These are electron systems confined to a disk and subjected to a perpendicular magnetic field at extremely low temperatures. Electrons in the disk, pictured classically as orbiting concentric annuli around the origin, organize themselves into a topological order. In this way the classification of UMTCs is akin to obtaining a periodic table of elements for the topological phases of matter.

3. **Toric Code and Abelian Anyons**

We now restrict our attention to abelian anyonic particle dynamics on a surface of genus g. To do this we first look at a model of qubits on a surface with genus g = 1 i.e. a torus. We then generalize this case to arbitrary genus.

3.1. **Toric Code.** The Toric code, introduced by Kitaev, is an example of a symplectic or stabilizer code. Stabilizer codes are quantum analogues of classical linear codes. In general such a code works by selecting a set of “check operators”, analogous to checksums, and encoding qubits in states belonging to the stabilizer space for each of the check operators. This allows for correction of a particular set of errors by first measuring a “syndrome” to determine the type of error—essentially
checking to see if the state is still in the stabilizer space. By measuring the syndrome, and not the information in the bits directly, we can reconstruct the error and reverse it without damaging our state.

Consider an \( r \times r \) lattice embedded on a torus. On each edge of the lattice we place a qubit (or a spin-\( \frac{1}{2} \) degree of freedom). We then have two types of check operators. The first type we will call “star operators”. These are operators

\[
A_s^x = \prod_{j \in \text{star}(s)} \sigma_j^x
\]

where \( \text{star}(s) \) for some vertex \( s \) is the set of edges, or equivalently qubits, adjacent to that vertex. The second type we will call “face operators”. These are defined by

\[
A_u^z = \prod_{j \in \text{boundary}(u)} \sigma_j^z
\]

where \( \text{boundary}(u) \) is the set of qubits around a given face \( u \). For the purposes of a stabilizer code, we now want to find what the stabilizer space of these operators looks like. We have \( 2r^2 \) qubits, and \( 2r^2 \) check operators. However, we have two relations among the check operators i.e.

\[
\prod_s A_s^x = I = \prod_u A_u^z.
\]

We conclude that the stabilizer space has dimension \( 2^2 = 4 \).

Furthermore, each operator only acts on 4 qubits, and each qubit is only acted on by 4 operators. In addition, because the operators all commute (star operators and face operators commute because a boundary and a star either share 0 or 2 qubits) we can apply the syndrome measurement in a constant depth circuit. We can check that the errors undetectable by this code are only those errors that encompass an entire cycle i.e. an element of the homology group of the torus. We can show this either by working with the state space directly or by understanding the Toric code in terms of anyonic particles.
3.2. Anyons and The Toric Code. Consider the same system as above—an \( r \times r \) lattice with a qubit on each edge embedded on a torus. When we view this as a physical system we are led to the Hamiltonian

\[
H = \sum_s (I - A^s_x) + \sum_u (I - A^u_z).
\]

The null space of this operator is exactly the stabilizer code space of the Toric code. Because the operator is non-negative, we then see that the stabilizer space of the code is precisely the space of minimal energy for this Hamiltonian. It follows that the excited states, having non-minimal energy, then form the orthogonal complement.

Now suppose we have the ground state \( |\xi\rangle \). We want to consider some minimal excited state \( |\nu\rangle \), and to this end we can consider the excited states as ordered by the number of conditions they violate. For the state \( |\xi\rangle \) we have that for all faces and vertices \( A^s_x |\xi\rangle = A^u_z |\xi\rangle = |\xi\rangle \). Due to the relations described above, the number of violated conditions of a given type (either face or star) must be even. Let us consider the simplest case of two violated conditions at vertices \( s \) and \( p \). Then we have at these vertices \( A^s_x |\nu\rangle = -|\nu\rangle \) and the same for \( p \). It is standard terminology to say that we have two quasiparticles at \( s \) and \( p \). First, we note that we can generate the state \( |\nu\rangle \) from the state \( |\xi\rangle \). We simply apply a product of \( \sigma^z_j \) for all \( j \) along a path from \( s \) to \( p \). We can also move quasiparticles along a path by applying products of \( \sigma^z_j \) along that path. Similarly, we can talk about quasiparticles on faces by considering violated conditions at faces. Again these can be created by products of \( \sigma^z_j \) for paths along the “dual lattice” i.e. the lattice given by thinking of faces as vertices, and connecting those vertices that correspond to adjacent faces.

We now consider what happens when these two types of particles interact. Suppose we have two vertex quasiparticles at \( s \) and \( p \), and two face quasiparticles at \( u \) and \( v \). We consider the action of moving one of our face quasiparticles around a closed loop containing the vertex \( p \). Moving this quasiparticle around a closed
loop is an application of star operators at every vertex inside the loop. All of these act as the identity except for the star operator at vertex \( p \) which flips the sign of our state. Moving one particle around another results in a phase change, even though the particles don’t directly interact!

Finally, because we are working on a torus and not a plane, there is another action we can consider. Consider 4 operators, \( Z_1, Z_2, X_1, X_2 \), where the \( Z_1, Z_2 \) operators are products of \( \sigma^z \) around the two different non-trivial loops of the torus, and \( X_1, X_2 \) are products of \( \sigma_x \) along non-trivial loops. The commutation relations between these operators are

\[
\begin{align*}
X_1X_2 &= X_2X_1 \\
Z_1Z_2 &= Z_2Z_1 \\
X_1Z_1 &= Z_1X_1 \\
X_2Z_2 &= Z_2X_2 \\
X_2Z_1 &= -Z_1X_2 \\
X_1Z_2 &= -Z_2X_1.
\end{align*}
\]

The operators \( X_1, Z_2 \) and \( Z_2, X_1 \) can each be thought of as acting as \( \sigma^x \) and \( \sigma^z \) operators on the two different qubits embedded by the Toric code—in other words they act on the 4-dimensional space of ground states of the Hamiltonian. One way to think about this is to consider creating a pair of vertex and a pair of face particles. If we move one of the vertex particles around a non-trivial cycle, and then annihilate it with the other vertex particle, essentially performing \( X_1 \) we get a phase change, since we have also moved the particle in a closed path around a face particle. However, \( X_1 \) has to commute with the operators that create face particles, and so if we first perform \( X_1 \) and then create a pair of face particles, we should get an already-flipped state. In other words, the ground state “remembers” the topological behaviour of past anyons.

3.3. **Abelian Anyons on a Surface: A Generalization.** What we have described above is simply a pair of particles such that when one is moved around the other the state vector acquires a phase flip of -1. It follows that these particles can be viewed as anyons with exchange statistics which are a fourth root of unity. Now
consider a more general case: anyons on a torus with exchange statistics given by some $e^{i\theta}$ where $\theta = \pi \frac{p}{q}$. These are also known as rational anyons, since the phase change given by their exchange is a rational multiple of $\pi$. We will restrict our study to rational anyons.

Rather than looking at operators of particles moving around one another, we instead look at two operators $C_1$ and $C_2$, which are analogous to our $X_i$ and $Z_i$ operators above. The operator $C_1$ is given by the creation of a pair of anyons, moving one around one non-trivial cycle of the torus, and then fusing the anyons and annihilating them. The operator $C_2$ is the analogous operator for the other non-trivial loop. As above, these will act non-trivially on the ground state of the torus, and again such action is a topological behaviour. We consider the commutator $[C_1, C_2] = C_2^{-1}C_1^{-1}C_2C_1$. Topologically what we have done is to move one particle in a loop around another, and this is equivalent to two exchanges. It follows that

$$[C_1, C_2] = e^{i2\theta}.$$

Consider some eigenvector $|\psi\rangle$ of $C_1$ with eigenvalue $e^{i\alpha}$ (since $C_i$'s are unitary their eigenvalues have this form). Then we have the relation

$$[C_1, C_2]|\psi\rangle = e^{i2\theta}|\psi\rangle$$

$$C_2 e^{i\alpha}|\psi\rangle = C_1 C_2 e^{i2\theta}|\psi\rangle.$$

Rearranging terms we can get

$$C_1(C_2|\psi\rangle) = e^{i(\alpha - 2\theta)}(C_2|\psi\rangle).$$

In other words $C_2$ acts as a shift operator on eigenvalues of $C_1$. Furthermore we see

$$[C_1, C_2]^q = e^{q(i2\pi \frac{p}{q})} = 1.$$
In summary, moving abelian anyons on a torus yields an additional q-fold degeneracy that does not exist when quasiparticles with the same exchange statistics move on a plane.

There is another way we can generalize this picture, and that is passing to surfaces of higher genus. Suppose then that the spatial degrees of freedom form a surface of genus \( g \). The above analysis depends only upon the existence of 2 non-trivial loops on the torus. A genus \( g \) surface has \( 2g \) non-trivial loops. We organize these loops into pairs—one pair for each hole in our surface (a genus \( g \) surface can be thought of as a connected sum of \( g \) tori, or a surface with \( g \) holes). To each of these loops we associate an operator \( C_i^j \) where the \( i = 1, 2 \) and \( j \) ranges from 1 to \( g \). Operators corresponding to loops in different pairs commute, and operators corresponding to the same loops commute. The only non-trivial commutator is \([C_1^1, C_2^1] = e^{i2\theta}\). We conclude then that on a surface of genus \( g \), we have \( g \) copies of the q-fold degeneracy from the topology of the torus. In other words our ground state space has a \( q^9 \)-fold degeneracy above and beyond what is present when abelian anyons are braided on a genus 0 surface.

As the analysis shows, these abelian anyons on a genus \( g \) surface may have a finite dimensional topological degeneracy, but their braiding does not allow the implementation of arbitrary unitary transforms. At best we find a stable ground state protected from local errors.

4. Conclusion

We discussed the computational power of a topological quantum field theory. We reviewed two basic questions: i. How does the topology of space-time affect the computational power of a TQFT and ii. independent of a particular space-time, what intrinsic structural properties of a TQFT govern its computational power? The observation that abelian anyons on a genus \( g \) surface generalizes the Toric code answers the first question: a non-trivial 2-D space-time topology provides an
exponential (in the genus $g$) degeneracy in the ground state of the TQFT, a resource that in principle could serve as a quantum storage robust to local error, but cannot be used to implement any transformation not already accessible to anyons with comparable statistics on a genus $g = 0$ surface. To answer the second question, we appealed to the algebraic model of anyonic quantum computation via the Tensor Category formalism. By relying on our intuition from classical group theory to guide our understanding of their quantum generalizations, we have seen how the correspondence between UMTCs and 3-dimensional TQFTs, affords an algebraic and number theoretic analysis of the computational regime modeled by any TQFT. Recent deep results in this direction such as the Rank Finiteness Theorem and classification of UMTCs of low rank are the fruits of this approach: we are able to derive an explicit periodic table of elements for topological states of matter, indexed by the nature of the anyonic excitations provided.

Several open questions present themselves: we still do not have a good characterization of when a UMTC/TQFT has a universal computational model. Furthermore, restricting to those cases where the computational model is not universal, we do not have a good characterization of what computational power they do provide: at best we have a conjectural characterization of when arbitrary braiding of anyonic excitations implements at most a finite subgroup of the unitary group. Basic obstructions to answering these questions are a lack of understanding the relationships between the objects involved. For example, it's expected—but not yet known—that there are UMTCs that do not arise from Quantum Groups; in practice all known UMTCs can be constructed via some procedure from a Quantum Group. This could be rephrased as a gap in our understanding of the representation theory of a general Quantum Group. Given how basic computational questions directly translate into open problems concerning these relatively young fields, we expect new advances to directly contribute towards a deeper understanding of quantum computation arising from a TQFT in the years to come.
Part 3. Computation in the setting of finite dimensional group symmetry

5. Introduction

Few general techniques are available for constructing efficient quantum circuits (for a review of the quantum circuit model from the standard point of view, different as espoused here, cf. [1]) implementing a given unitary operator. To this end, in [2] Nielsen develops a geometric method for bounding the circuit complexity of a given unitary operator. The basic observation notes that a quantum circuit may be thought of as a discrete path in the smooth manifold of invertible unitary operators $U(n)$. Minimal complexity circuits then could be thought of as discrete paths of shortest length. However, to make precise the idea of shortest length we require a means of measuring distances within $U(n)$ such that the distance between two unitary operators is proportional to the complexity of synthesizing one operator given the other. Such a metric is termed a computational metric.

In the theory of Riemannian Geometry and Lie Groups (for a comprehensive reference, see [4]), distances are measured via a Riemannian metric: an assignment of a symmetric bilinear form on the tangent space to each given point $p$ compatible with the Lie Group structure on $U(n)$

$\langle , \rangle_p : T_p U(n) \times T_p U(n) \rightarrow \mathbb{R}$

If the metric is chosen correctly, the circuit complexity of a given unitary operator $U$ is then proportional to the distance $d(I, U)$ where $I$ is the identity operator and $d$ is the distance function on $U(n)$ induced by the metric. In this way we equate the question of finding a minimal complexity circuit implementing $U$ to finding a path of minimal length connecting $I$ and $U$ in $U(n)$ under the appropriate metric. These paths are given modeled by geodesics, and can be expressed naturally as the solutions (obtained via the calculus of variations) to the so-called geodesic equations derived in terms of the metric.
We follow this discussion with a geometric proof of the optimality of Grover's algorithm. While outside of Nielsen et al's framework, the proof casts Grover's algorithm as a geodesic of a natural metric on Complex Projective space. As a principle homogenous space (i.e. a space on which the Unitary group acts transitively), there is expected to be a strong link between this and the aforementioned point of view. We also include a result on a family deformations of Grover's search algorithm encountered in this geometric setting.

The core of this section falls into three distinct sections: section 6 a discussion of the Riemannian metric correlating discrete quantum circuits to continuous paths on the Unitary group, section 7 a geometric proof of the optimality of Grover's search algorithm and section 8 a discussion of a family of deformations of Grover's search algorithm.

6. THE COMPUTATIONAL METRIC

For simplicity we restrict our discussion to the $2^{2n}$ dimensional Lie Group $SU(2^n)$ (the results can be extended to $U(2^n)$ with added technical work). $SU(2^n)$ is a smooth manifold with tangent space $su(2^n)$, i.e. given a point of $SU(2^n)$ a tangent vector can be thought of as a *Hamiltonian*, i.e. a traceless $2^n \times 2^n$ Hermitian matrix. In this way, a Riemannian metric on $SU(2^n)$ at a point $U$ in $SU(2^n)$ is a positive-definite bilinear form $(H, J) U$ mapping traceless Hermitian matrices to $\mathbb{R}$.

If $U(t)$ is a curve in $SU(2^n)$ generated by a Hamiltonian $H(t)$ by the Schrödinger equation

$$dU = iHU,$$

then the length of the curve is given by

$$\int \sqrt{(H(t), H(t))} dt.$$

This allows us to define a distance $d(U1, U2)$ between two unitary operators in $SU(2^n)$ as the minimal length curve connecting them with respect to any given
metric. We build the computational metric as follows: let $\mathcal{P}$ be the subspace of $n$-qubit Hamiltonians which contain only 1 and 2 body terms, i.e. their expansion in terms of sums and tensor products of Pauli Operators contains only terms of weight at most 2, such as

$$= \sigma_x \otimes I_{n1}, \sigma_y \otimes I_{n3} \otimes \sigma_z \otimes I.$$

Let $\mathcal{Q}$ denote the complementary space of Hamiltonians containing only 3 and more-body terms, then

$$su(2^n) = \mathcal{P} + \mathcal{Q}$$

as any hamiltonian can be uniquely decomposed into a sum

$$H = H_P + H_Q$$

Let $\mathcal{P}, \mathcal{Q}$ also denote the projections onto these subspaces, then we can define an inner product on $su(2^n)$ as

$$\langle H, J \rangle = \text{tr}(H \cdot \mathcal{P}(J)) + q \cdot \text{tr}(\mathcal{Q}(J))2n$$

Nielsen et al call the term $q$ is penalty parameter which when chosen sufficiently large causes a variation in the length

$$\langle H, J \rangle$$

viewed as a cost of moving an infinitesimal distance on $SU(2^n)$ in the direction specified by the Hamiltonian $H(t)$. A large $q$ thus penalizes a large cost to the choice of 3 or more qubit gates.

In [2] Nielsen proves the induced distance $d(I, U)$ from the identity element to any given $U$ in $SU(2^n)$ bounds $G(U)$: the minimal number of 1 and 2 qubit gates required to synthesize $U$, thus

$$d(I, U) \leq G(U)$$
It follows that the explicit construction and computation of the length of a geodesic from \(I\) to a given unitary operator \(U\) will prove a lower bound on the gate complexity of \(U\).

7. **Grover's Algorithm as a Geodesic on Projective Space**

We now digress to investigate a geometric formulation of the optimality of Grover's algorithm.

**Theorem 7.1.** Grover's algorithm acts by evolving its initialized state along a geodesic of the Fubini-Study metric on complex projective space.

As the Fubini-Study metric is the unique natural unitary-invariant metric on projective space, and evolution of a state via the action of Unitary matrix preserves the metric, consequently:

**Corollary 7.2.** Grover's algorithm solves the search problem in time-complexity optimal among all quantum algorithms.

**Proof.** To this end, assume our search function is encoded as a boolean-valued indicator function \(f\) with domain the symbols \(1 \ldots n\). Grover's algorithm initializes our system with a quantum state that is a uniform super-position over \(n\) qubits.

\[
|a\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle,
\]

If \(f(t) = 1\), then we can note the inner product

\[
\langle t|a\rangle = \frac{1}{\sqrt{N}} = \sin \frac{\theta}{2}
\]

allows us to express \(|a\rangle\) as

\[
\begin{bmatrix}
\cos \frac{\theta}{2} |x\rangle \\
\sin \frac{\theta}{2} |t\rangle
\end{bmatrix}
\]
Once $|a\rangle$ is initialized, Grover's algorithm calls $f$ in the form of a diffusion operator

$$I_t|x\rangle = (1)^f(x)|x\rangle,$$

iterated on the state $|a\rangle$ as the operator

$$U = I_aI_t = (12|a\rangle\langle a|)(12|t\rangle\langle t|).$$

With respect to $\theta$ we see $U$ takes the form of a real rotation

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

Thus $k$ iterations of the diffusion operator yields

$$|\psi(k)\rangle = U_k|a\rangle = \begin{bmatrix} \cos(k + \frac{1}{2}\theta)|s\rangle \\ \sin(k + \frac{1}{2}\theta)|t\rangle \end{bmatrix}.$$ 

The notation above makes it clear that the optimal $k = \frac{\pi}{4}\sqrt{N}$ yielding a running time complexity of $O(\sqrt{N})$.

Now, if we consider the unitary operators in the above circuit formulation of Grover's search as linear operators acting on the Hilbert space $\mathbb{C}^n$, then as non-trivial quantum states are equivalent to 1-dimensional complex subspaces (non-zero vectors up to a complex scalar), we may work instead directly in complex projective space. The polar form of a complex number

$$z = re^{i\theta}$$

yields natural projections

$$\mathbb{C}^n \setminus \{0\} \rightarrow S^{2n+1} \rightarrow \mathbb{P}^{n},$$

where the first projection is a quotient by the dilation $z = rz$ for $r \in \mathbb{R}_+$ (i.e. projects via normalization every non-zero vector onto the real unit hypersphere...
$S^{2n+1}$ when $\mathbb{C}^n$ is considered as a 2n dimensional real vector space), and the second projection identifies great circles on $S^{2n+1}$, i.e. equates any two points of $S^{2n+1}$ given by a rotation by an angle $\theta$.

The first projection restricts the standard (Euclidean) metric on $\mathbb{C}^n$ (i.e. the 2-norm) to the hypersphere $S^{2n+1}$, while the second projection induces a natural quotient metric on $\mathbb{P}^n$ called the Fubini-Study metric.

Now projective space has the characteristic property that through any two points there passes a unique projective line $\mathbb{P}^1$, and in the complex case this is the Riemann Sphere. As a Riemannian globally symmetric space of rank 1, the geodesics of $\mathbb{P}^1$ are all closed and all have equal length, hence are great circles of the Riemann sphere. It follows that for some vectors $\psi_1, \psi_2$ of unit norm in $\mathbb{C}^n$, a geodesic of $\mathbb{P}^{n+1}$ is of the form

$$|\psi(u) = \cos \frac{u}{2}|\psi_1) + \sin \frac{u}{2}|\psi_2)$$

Returning to Grover’s algorithm, recall $k$ iterations of the diffusion operator yields

$$|\psi(k) = U_k|a = \begin{pmatrix} \cos(k + \frac{1}{2} \theta)|s) \\ \sin(k + \frac{1}{2} \theta)|t) \end{pmatrix}$$

Let $|\psi_1) = |s, |\psi_2) = |t)$ and $u = 2(k + 1)\theta$ then we see that Grover’s algorithm evolves the initial state $|a)$ along a geodesic of the Fubini-Study metric:

$$|\psi(u) = \cos \frac{u}{2}|\psi_1) + \sin \frac{u}{2}|\psi_2)$$

8. **Deformations of Grover’s Algorithm**

Now we investigate a natural generalization suggested by the geometry given above. Connecting any two points in state space $\mathbb{P}^n$ there is a unique projective line $\mathbb{P}^1$ and its preimage under the natural projections outlined in section 3 above
produces a unique complex plane

\[ \mathbb{C}^2 \subset \mathbb{C}^n. \]

This inspires us to consider products of pairs of linear combinations of orthogonal projections. In more detail, we consider unitary operators \( U_1, U_2 \) such that each is a linear combination of orthogonal projections, i.e., for orthogonal pairs of projections \( (A_i, B_i)_{i=0,1} \) each characterized by

\[
A_i^2 = A_i, \quad B_i^2 = B_i, \quad A_i + B_i = I
\]

then

\[ U_i = \alpha_i A_i + \beta_i B_i \]

where the \( \alpha_i \) and \( \beta_i \) are complex numbers. Then the operator we are interested in is the family of products

\[
(U_2 U_1)_{\alpha_1, \beta_1, \alpha_2, \beta_2}
\]

parameterising a family of Unitary Operators, and hence a family of Quantum Algorithms.

For our first example, for \( A_1 = |x\rangle \langle x|, B_1 = 1 - A_1 \) and

\[
A_2 = \frac{1}{\sqrt{N}} \begin{bmatrix}
1 & \ldots & 1 \\
\vdots & \ddots & \vdots \\
1 & \ldots & 1
\end{bmatrix}
\]

and \( B_2 = 1 - A_2 \) then since \( A_2 = |x_2\rangle \langle x_2| \) with \( x_2 = \frac{1}{\sqrt{N}} \)

then the parameters

\[
\alpha_1 = \alpha_2 = -1 = -\beta_1 = -\beta_2
\]
which means

\[ U_1 = 1 - 2A_1 \]
\[ U_2 = 1 - 2A_2 \]

(note that \( U_2 \) coincides with the diffusion operator introduced in section 3) reproduces the original Grover's search as iterated applications of

\[ (U_2U_1)_{1,-1,1,-1}, \]

and for all other values of the parameters produces a deformed version of the algorithm.

In order to analyse these deformations we restrict our attention to the \( \mathbb{C}^2 \) on which all non-trivial behaviour occurs, i.e. we consider the span of vectors \( |x_0 \rangle \) and \( \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x \rangle \).

On this basis we have

\[ U_1 = \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix} \quad \text{and} \quad U_2 = \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} + \frac{\beta_2 - \alpha_1}{N} \begin{bmatrix} 1 & \sqrt{N-1} \\ \sqrt{N-1} & -1 \end{bmatrix}. \]

Now we have four complex parameters, but we can fix two of them by fixing the choice of phase in each \( U_i \). We set

\[ \alpha_1 = \beta_2 = -1 \]

then

\[ (U_2U_1)_{\alpha_2,\beta_1} = \frac{1}{N} \begin{bmatrix} 1 + \alpha_2(1-N) & -\beta_1(1+\alpha_2)\sqrt{N-1} \\ (1+\alpha_2)\sqrt{N-1} & \beta_1(1+\alpha_2-N) \end{bmatrix}. \]
Similarly, we fix initial conditions by assuming the input vector is the same as in our original Grover's search i.e.

\[ |x_{1n} \rangle = \frac{1}{\sqrt{N}} |x_0 \rangle + \sqrt{\frac{N-1}{N}} \sum_{x \neq x_0} \frac{1}{\sqrt{N-1}} |x \rangle. \]

Now we'd like to compute the probability amplitude of finding the desired state as a function of the parameters, and we do so via spectral decomposition of \((U_2U_1)_{\alpha_2,\beta_1}\). If \(e^{i\lambda_j}\) are the associated eigenvalues with eigenvectors \(|\lambda_j\rangle\) then the spectral theorem yields

\[ \langle x_0 | (U_2U_1)_{\alpha_2,\beta_1} | x_{1n} \rangle = e^{in\lambda_1} \left( \frac{1}{\sqrt{N}} + e^{in(\lambda_2-\lambda_1)} \langle x_0 | \lambda_2 \rangle \langle \lambda_2 | x_{1n} \rangle \right). \]

Finally

\[ \det(U_2U_1)_{\alpha_2,\beta_1} = \beta_1 \alpha_2 \text{ and } \text{tr}(U_2U_1)_{\alpha_2,\beta_1} = -(\beta_1 + \alpha_2) + \frac{1}{N} (1 + \beta_2)(1 + \alpha_1) \]

so it follows that the eigenvalues

\[ e^{i\lambda_j} = \frac{\text{tr}(U_2U_1)_{\alpha_2,\alpha_1}}{2} + \sqrt{-\det(U_2U_1)_{\alpha_2,\alpha_1} + \frac{\text{tr}(U_2U_1)_{\alpha_2,\alpha_1}}{2}} \]

and the eigenspaces \(|\lambda_j\rangle\) are spanned by

\[
\begin{bmatrix}
(\beta_1 - \alpha_2)N + (1 - \beta_1)(1 + \alpha_2) + \sqrt{4\det(U_2U_1)_{\alpha_2,\beta_1} \pm (\beta_1 - \alpha_2)N + (1 - \beta_1)(1 + \alpha_2)}^2} \\
2(1 + \alpha_2)\sqrt{N-1} \\
1
\end{bmatrix}
\]

Now denote by \(N_{opt}\) the value of \(n\) where the above probability of finding the desired state is maximized, then we have derived that as \(n \to \infty\) we have the difference in eigenvalues

\[ \lambda_2 - \lambda_1 \to_{n \to \infty} \frac{4}{\sqrt{N}} \text{Real} \sqrt{\alpha_2} \]

leading to a parametrization

\[ \alpha_1 = e^{i\phi} \]
that
\[ N_{\text{opt}} \to_{n \to \infty} \left[ \frac{\pi}{4} \cos \frac{\phi}{2} \right] \sqrt{N}. \]

So we conclude that this family of deformations can be thought of as a family of search algorithms with efficiency a function of the real parameter \( \phi \). This family has all elements of order \( O(\sqrt{N}) \), and achieves optimality at \( \phi = 0 \) where the algorithm deforms into Grover's search. Note that the worst behaviour occurs when \( \phi \to \pi \) which coincides with \( (U_2 U_1) \) being the identity operator. Thus, we can view this family in the framework of Nielsen et al as a smooth path in the unitary group connecting the trivial algorithm to Grover's search.

9. CONCLUSION

Though the Nielsen et al. approach in principle allows us to introduce the calculus of variations to the task of proving quantum circuit lower bounds, to-date no new lower bounds proofs have resulted from this approach. The reasons are many-fold: the geometry of the Lie Groups \( U(n) \) and \( SU(n) \) is poorly understood (even for \( n \) as low as 3), inhibiting insight into the metrics we place on them, or the ways in which these metrics and their geodesics may be deformed. Furthermore, the computational metric as defined is far from a natural construction: there is no obvious way to derive it from or relate it to the known structure theories of \( U(n) \). Most structurally interesting, however, is a consequence of Razborov-Rudich: if classical pseudorandom generators exist, then there can be no classical algorithm running in time polynomial in \( 2^n \) which produces an accurate approximation to the length of a geodesic under the computational metric, as such an algorithm would allow us to efficiently distinguish between circuits of differing complexity. Since a circuit at random has high complexity, thus, we would show pseudorandom generators do not exist.
Still, the approach bears conceptual value: Lie Groups such as $U(n)$ and $SU(n)$ have rich theories that are ubiquitous across mathematics and physics; any theoretical bridge to computation: classical or quantum would prove fruitful, and Nielsen et al.'s approach highlights one such bridge: the identification of circuit complexity of a quantum algorithm with the notion of tensor rank of a non-commutative Hamiltonian. This bridge may provide further progress yet.

Finally, in contrast to the more general approach of finding geodesics on the space of all unitary operators, we have also shown how Grover's search algorithm on $n$ items can be viewed as a geodesic of a natural metric on $\mathbb{P}^{n-1}$. It remains to be seen whether the two approaches can be unified into a single framework, but in contrast to the arbitrary nature of the computational metric introduced in the Nielsen et al. approach, the Fubini-Study metric descends from the standard inner product on $\mathbb{C}^n$ via a natural projection map; consequently much more is understood about the Fubini-study metric. Given that a deformation of the Fubini study metric will yield a deformation of Grover's algorithm, an immediate question is to further investigate the natural families of quantum circuits arising from deforming Grover's search algorithm.

Part 4. Appendices

A: The Braid Group

The braid group $B_n$ on $n$ strands, is a generalization of the symmetric group $S_n$ on $n$ symbols. It has an intuitive presentation as braids of $n$ strings. Formally it is presented by $n-1$ generators $\sigma_i$ which corresponds to crossing the $i^{th}$ strand over the $i+1^{th}$ strand. For example, the braid
is given by generators
\[ \sigma_1 \sigma_2 \sigma_1^{-1}. \]

Such a sequence of generators is called a **braid word**. This set of generators has a set of relations:
\[ \sigma_i \sigma_j = \sigma_j \sigma_i \quad \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \]
where \(|i - j| > 2\). Such relations are easy to see if you draw out the corresponding diagrams.

**B: THE FIBONACCI THEORY \( \mathcal{F} \)**

We now introduce one of the simplest non-trivial TQFTs which we denote \( \mathcal{F} \), known as the Fibonacci theory in the literature (See pp. 21 in [10]). The purpose of explicitly describing \( \mathcal{F} \) here is to provide a concrete example to help motivate the abstract language of UMTCs used in this thesis.

We specify \( \mathcal{F} \) by the structure of the anyonic excitations it supports in any 2-dimensional slice of space-time, as well as the resulting exchange statistics. In this model, there are only two different types of anyons, the vacuum (or absence of an anyon) denoted \( \mathbb{1} \) and the non-abelian anyon \( \tau \). Part of the data specifying a TQFT is what is known as a **fusion rule**, which specifies what happens when two particles are brought together. Fusion can be considered as identifying the two anyons as a composite particle and identifying the resulting statistical behaviour of the ensemble. For example, fusing two fermions results in a boson. In the case of \( \mathcal{F} \):

\[ \tau \times \tau = \mathbb{1} + \tau, \]
\[ \tau \times \mathbb{1} = \tau, \]
\[ \mathbb{1} \times \tau = \tau, \]
\[ \mathbb{1} \times \mathbb{1} = \mathbb{1}. \]
These rules should be read, for example in the first row, as stating that fusing two \( \tau \) particles results in a state space consisting of two outcome states: the first state being the annihilation of both particles (the outcome being the vacuum) and the second state being the formation of another \( \tau \) particle. The fact that this fusion space has dimension higher than 1 and so allows for degeneracy in the fusion Hilbert space is equivalent to \( \tau \) being a non-abelian anyon, a fact that has only recently been proved; see [6].

\[ \begin{array}{c}
\tau \tau \tau \tau \tau \\
1 \text{ or } \tau
\end{array} \]

**Figure 2.** Fusion of multiple \( \tau \) particles.

The computational power of \( F \) is now made apparent in the process of fusing \( n \) anyons of type \( \tau \). Consider a line of \( \tau \) particles as depicted in figure 2 and proceed to fuse these particles in a step-wise fashion. We begin by fusing the first two particles, and then continue by fusing the outcome with the remaining particles incrementally. To each step \( i \) we assign an index \( e_i \) that indicates the outcome of the fusion at that step as being either 1 or \( \tau \). The states \( |e_1, e_2, \ldots, e_{n-3}\rangle \) belong to what is called the fusion Hilbert space of the \( \tau \) anyons, denoted \( \mathcal{H}_n \). In principle, there are \( 2^{n-3} \) possible outcomes of \( e_i \)'s, but not all are allowed by the fusion rules. For \( n = 1 \), we deal with the impossible case of the vacuum turning into a \( \tau \) anyon, so

\[ \dim(\mathcal{H}_1) = 0. \]

For \( n = 2 \) we see \( \tau \) as input and output going through a trivial process so

\[ \dim(\mathcal{H}_2) = 1. \]
Next, the possible outcomes are 1 or r, giving

$$\dim(\mathcal{H}_3) = 1,$$

but at the very next step we see that there are two possible ways of yielding a r from two different processes and so

$$\dim(\mathcal{H}_4) = 2.$$

Continuing this way we see that

$$\dim(\mathcal{H}_5) = 3,$$

and so on, yielding the sequence

$$0, 1, 1, 2, 3, 5, 8, 13, \ldots$$

which grows proportionally to $\phi^n$ where $\phi = \frac{1+\sqrt{5}}{2}$. Thus the fusion state space $\mathcal{H}_n$ of internal degrees of freedom of $n$ anyons of type $\tau$ grows exponentially with $n$. In order for this to be a viable computational resource, we ideally want to be able to implement arbitrary unitary transforms on $\mathcal{H}_n$. As mentioned in the previous section, this is accomplished by braiding two $\tau$ anyons around one another as in Figure 2.3.

![Figure 2.3](image)

**Figure 3.** Braiding of two $\tau$ particles.

The process of doing so is a unitary transform on those basis vectors in the fusion space spanning possible fusion outcomes $c$ according to the fusion rules governing $\alpha$ and $\beta$ in the particular TQFT. Hence, this braiding matrix is part of what specifies a TQFT. In the case of $\mathcal{F}$ again, we find that exchanging any two $\tau$
anyons acts as the matrix

\[ R_{\tau,\tau} = \begin{pmatrix} e^{\frac{2\pi i}{5}} & 0 \\ 0 & e^{\frac{2\pi i}{5}} \end{pmatrix}. \]

Given an exponential state space, rules for braiding, and rules for fusing, we can now see that in order to encode a logical qubit as in the standard Quantum Circuit Model, we might employ four \( \tau \) anyons. There are two distinguishable ways these anyons can be fused that can encode the qubit states: \( |0\rangle = |\tau, \tau \rightarrow 1\rangle \) and \( |1\rangle = |\tau, \tau \rightarrow \tau\rangle \). The possible logic gates are accomplished by forming arbitrary braids amongst these four qubits, with behaviour governed by \( R_{\tau,\tau} \). Fusing and reading the outcome then correspond to a measurement in the Quantum Circuit Model.

As our goal is to study the general computational power of a given TQFT, we find it fruitful to abstract the data presented here in the form of an algebraic model of anyons given by Tensor Categories as described in [16]. As described in Section 2, not only does the language of tensor categories simplify the description of a TQFT, but it also affords us algebraic and number-theoretic tools to analyse the computational power carried by any given TQFT.

APPENDIX C: TQFT AND UNITARY MODULAR TENSOR CATEGORIES

In the example furnished in Appendix B, a model of computation arose from a TQFT after specifying:

- a set of objects corresponding to the available types of anyons
- rules for fusing these objects pairwise
- rules for braiding these objects pairwise

We now capture this data in an algebraic structure known as a Unitary Modular Tensor Category. We include the concise definition for readers familiar with tensor categories, but for those not, immediately after we turn to recast the definition
in terms of two familiar objects: i. the category $V_k$ of finite dimensional vector spaces over the field $k$ and ii. the TQFT $F$.

**Definition 2.** A **Unitary Modular Tensor Category** (abbreviated UMTC) is a semi-simple ribbon category $C$ satisfying the following properties:

- $C$ has only a finite number of isomorphism classes of simple objects.
- $C$ is modular i.e. has non-degenerate $S$-matrix.

We refer the interested reader to [16] for a detailed exposition of the terminology used here. Modularity, though important for the dictionary between TQFTs and UMTCs, will not play an immediate technical role in any of our subsequent discussions, so we omit covering it here. Instead, for our purposes we now quickly describe the structure of two UMTCs: $V_k$ and $F$.

$C$ is a **Semi-Simple Ribbon Category with finitely many isomorphism classes of simple objects.** That $C$ is a category means that $C$ can be thought of as a collection of objects $\text{Obj}(C)$. For example, in the category $V_k$ of finite dimensional vector spaces over the field $k$, $\text{Obj}(V_k)$ is the set of isomorphism classes of vector spaces over $k$ of finite dimension; i.e. one object for each $n \in \mathbb{N}$. In the case of $F = \{1, \tau\} \subseteq \text{Obj}(F)$, but the full collection of objects includes additional objects that can be constructed from these two, as soon shall be seen.

That $C$ is a Semi-Simple Ribbon Category means that $C$ has natural duals, natural tensor products, and a natural braiding structure on $\text{Obj}(C)$. In the case of $V_k$, we see for any $V, W \in \text{Obj}(V_k)$ these constructions are the familiar dual vector spaces:

$$V \rightarrow V^*$$

tensor product

$$V \otimes W$$
and braiding map coinciding with commutativity of tensor product
\[ V \otimes W = W \otimes V. \]

In \( \mathcal{F} \) the natural duals on Obj(\( \mathcal{F} \)) are particle-to-antiparticle correlation
\[ 1 = \bar{1} \]
and
\[ \tau = \bar{\tau} \]
i.e. both \( 1 \) and \( \tau \) are their own antiparticle (i.e. are self-dual). Tensor product then corresponds to fusion e.g.
\[ \tau \times \tau \in \text{Obj}(\mathcal{F}) \]
is the composite particle with behaviour governed by the collective statistical behaviour of two \( \tau \) particles, and finally a natural braiding map given by
\[ R_{\tau,\tau} : \tau \times \tau \to \tau \times \tau. \]

Finally, that \( C \) is semi-simple means each tensor product of objects can be decomposed into a direct sum of a distinguished class of simple objects. Here simple should be taken in the sense of an irreducible representation, prime number etc. — a simple object is one that cannot be decomposed into a direct sum of smaller objects. For example, in \( \mathcal{V}_k \), any vector spaces \( V \) and \( W \) of dimensions \( m \) and \( n \) decomposes as
\[ V \otimes W = \bigoplus_{i=1}^{mn} k. \]
Analogously, the fusion rules of \( \mathcal{F} \) specify the decomposition of the fusion of two \( \tau \) particles:
\[ \tau \times \tau = 1 + \tau. \]
The simple objects of $\mathcal{V}_k$ clearly consist exclusively of the one dimensional vector space $k$, while the simple objects of $\mathcal{F}$ are $\{1, \tau\}$.

**Braid Group Representations and non-triviality of UMTCs.** The preceding section should have conferred the sense that UMTCs are in a sense categories that behave like the category of vector spaces, while at the same time UMTCs capture the basic data of anyonic statistics in a TQFT. While both of these form examples of a UMTC, they can be seen to lie on opposite ends of a vast spectrum of complexity in a UMTC: the former is in a certain sense trivial, while the latter is very interesting. To make this precise, consider the braiding maps in $\mathcal{V}_k$

$$V \otimes W \rightarrow W \otimes V$$

given by the familiar map $a \otimes b \rightarrow b \otimes a$, then this map squares to the identity. It follows that if in our TQFT we think of $V$ and $W$ as anyonic excitations, each with their worldlines (See Figure 4), then $V \otimes W$ would model the fused particle i.e. the composite subsystem consisting of the two particles. The braiding map then

![Figure 4. Braid Transposition.](image)

models the action on the fusion space when we twist one particle about the other; following this logic through, if we try to represent the braid group generator $\sigma_{V,W}$ that crosses the two strands corresponding to the worldlines of $V$ and $W$ (see appendix A), since this braid map squares to the identity, we have in effect limited ourselves to a highly constrained representation of the braid group $B_2$. It follows that a UMTC such as $\mathcal{V}_k$ does not model any interesting anyonic exchange statistics. Conversely, $\mathcal{F}$ has braid map $R_{\tau,\tau}$ that yields a highly non-trivial braid group representation (as referenced in Section 2, this representation is computationally universal).
The above discussion illustrates that in order to find UMTCs modeling non-trivial TQFTs, we have to go outside the scope of classical algebra. One way to realize this principle is via the correspondence between certain TQFT and suitable categories of representations of a Quantum Group. For a survey of ways to obtain UMTCs in this way, see [13].

**Unitarity, Modularity and TQFTs.** Together with Unitarity which guarantees a given hermitian structure on $\text{End}(V)$ for any object $V \in C$, the Modularity condition (which we have not treated here) guarantees that to each UMTC we can uniquely associate a TQFT; the precise construction of a field theory from the abstract algebraic description of a tensor category is beyond the scope of this thesis. We instead refer the interested reader to now-standard reference [16].

**REFERENCES**


DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139

E-mail address: raez@mit.edu