Good Families of Quantum Low-Density Parity-Check Codes and a Geometric Framework for the Amplitude-Damping Channel

by

Reina Riemann

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 2011

© Reina Riemann, MMXI. All rights reserved.

The author hereby grants to MIT permission to reproduce and distribute publicly paper and electronic copies of this thesis document in whole or in part.

Author

Department of Electrical Engineering and Computer Science

Certified by

Peter W. Shor
Morss Professor of Applied Mathematics
Thesis Supervisor

Accepted by

Terry Orlando
Chairman, Electrical Engineering and Computer Science Department
Committee on Graduate Theses
Good Families of Quantum Low-Density Parity-Check Codes
and a Geometric Framework for the Amplitude-Damping
Channel

by

Reina Riemann

Submitted to the Department of Electrical Engineering and Computer Science
on January, 2011, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Abstract

Classical low-density parity-check (LDPC) codes were first introduced by Robert Gallager in the 1960’s and have reemerged as one of the most influential coding schemes. We present new families of quantum low-density parity-check error-correcting codes derived from regular tessellations of Platonic 2-manifolds and from embeddings of the Lubotzky-Phillips-Sarnak Ramanujan graphs.

These families of quantum error-correcting codes answer a conjecture proposed by MacKay about the existence of good families of quantum low-density parity-check codes with nonzero rate, increasing minimum distance and a practical decoder.

For both families of codes, we present a logarithmic lower bound on the shortest noncontractible cycle of the tessellations and therefore on their distance. Note that a logarithmic lower bound is the best known in the theory of regular tessellations of 2-manifolds. We show their asymptotic sparsity and non-zero rate. In addition, we show their decoding performance with simulations using belief propagation.

Furthermore, we present a general geometrical model to design non-additive quantum error-correcting codes for the amplitude-damping channel. Non-additive quantum error-correcting codes are more general than stabilizer or additive quantum error-correcting codes, and in some cases non-additive quantum codes are more optimal.

As an example, we provide an 8-qubit amplitude-damping code, which can encode 1 qubit and correct for 2 errors. This violates the quantum Hamming bound which requires that its length start at 9.

Thesis Supervisor: Peter W. Shor
Title: Morss Professor of Applied Mathematics
Acknowledgments

I acknowledge valuable criticism and collaboration with CSAIL members and affiliates and in particular from my advisor Peter Shor.
# Contents

1 Introduction 9

2 Definitions 14

2.1 Graph Theoretical Definitions 14
2.2 Linear Group Definitions 16
2.3 Number Theoretical Definitions 17

3 Good Families of Quantum Low-Density Parity-Check Codes 19

3.1 Background 19
3.2 Topological Quantum Error-Correcting Codes 21

4 Platonic Quantum Low-Density Parity-Check Codes 23

4.1 Platonic Surfaces 23
4.2 Platonic Quantum Low-Density Parity-Check Codes 24
  4.2.1 Platonic $\pi_7$ Code 25
  4.2.2 Family of Platonic Quantum Low-Density Parity-Check Codes 25
  4.2.3 Asymptotic Rate for the Platonic Family of Quantum LDPC Error-Correcting Codes 25
  4.2.4 Asymptotic Sparsity Analysis for the Platonic Family of Quantum LDPC Error-Correcting Codes 28
4.2.5 Shortest Noncontractible Cycle Bound, \( snc \sim \log(p) \), for the Dual Platonic Surfaces \( \pi_p' \) .................. 28

4.2.6 Empirical Calculations of the Shortest Noncontractible Cycle for the Dual Platonic Surfaces \( \pi_p' \) .................. 33

4.3 Belief-Propagation Decoding ............................... 36

5 Ramanujan Quantum Error-Correcting Codes .......................... 39

5.1 LPS Ramanujan Graphs Properties ................................ 41

5.2 Ramanujan Surfaces .......................................... 47

5.3 Ramanujan Quantum Error-correcting Codes ........................... 48

5.3.1 Asymptotic Rate for the Ramanujan Quantum LDPC Error-
Correcting Codes .............................................. 48

5.3.2 Sparsity Analysis for the Ramanujan Quantum LDPC Error-
Correcting Codes ........................................... 50

5.3.3 Ramanujan Surface Shortest Noncontractible Cycle \( snc \) .... 51

5.4 Belief-Propagation Decoding ................................... 53

6 A General Geometric Framework for the Amplitude Damping Chan-
nel ................................................................. 56

6.1 The Quantum Hamming Bound .................................. 57

6.2 General Geometrical Framework ................................. 60

6.2.1 Four qubit amplitude-damping error-correcting code example . 60

6.2.2 Singlet-state error-detecting code ............................ 61

6.2.3 General singlet-state family of codes ......................... 61

6.3 Orthogonality Framework ......................................... 61

6.3.1 Eight qubit amplitude-damping code .......................... 63

6.4 Generalizations .................................................. 65

7 Conclusions .......................................................... 66
List of Figures

4.2.1 Platonic graph $\pi_7'$ adjacency matrix. The vertical and horizontal axis represent ordered vertices of the graph. $nz$ is the number of non-zero elements in the matrix, which is twice the number of edges in the graph. 26

4.2.2 Farey Tree ............................... 29

4.2.3 The vertical axis represents the number of vertices in the graph. The horizontal axis represents the parameter $n$. The star line shows $n^2$ and the solid line shows the Fibonacci number of the empirical shortest non-contractible cycle of the platonic graphs as a function of $n$. ... 34

4.3.1 Simulation results for the quantum error-correcting codes derived from Platonic surfaces. The $Y$ coordinate is the code rate. The $X$ coordinate represents the flip probability $f_m$ at which the probability of block decoding error is $10^{-4}$ (0.9999 threshold). All simulation labels start at Platonic $n = 6$. For more information about the labels, read the section simulation results. The smooth curve shown in blue is the Shannon limit, and the dotted curve shown in blue is the Gilbert-Varshamov bound. ......................................... 38

5.1.1 Ramanujan graph $X^{5,13}$ adjacency matrix. On close-up, the blocks appear randomly sparsely filled. ...................................... 44

5.1.2 Ramanujan graph $X^{5,17}$ adjacency matrix. On close-up, the blocks appear randomly sparsely filled. ...................................... 46
5.2.1 Ramanujan graph $X^{2,3}$ .................................................. 49
5.2.2 Embedded Ramanujan graph $X^{2,3}$ ........................................ 49
5.3.1 The vertical axis represents the prime $q$. The horizontal axis represents the length of the cycle. The stars show the empirical length of the shortest non-contractible cycle of the Ramanujan graph $X^{p,q}$ as a function of $q$, when $\left(\frac{p}{q}\right) = -1$. The solid line shows the theoretical lower bound for the girth of $X^{p,q} \geq 4 \log_p q - \log_p 4$. .................. 52
5.4.1 Experimental simulation decoding results for the Ramanujan quantum error-correcting LDPC codes. The $Y$ coordinate is the code rate. The $X$ coordinate represents the flip probability $f_m$ at which the probability of decoding block error is $10^{-4}$ (0.9999 threshold). For the Platonic codes, the simulation labels start at Platonic $n = 6$. For the Ramanujan codes, the simulation labels start at 5 – 13. The smooth curve shown is the Shannon limit, and the dotted curve shown is the Gilbert-Varshamov bound. ................................. 55
List of Tables

4.1 Table with the distance (shortest non-contractible cycle), genus and number of encoding qubits for the platonic quantum low-density parity-check error-correcting codes. .................................................. 35

5.1 Table with the distance (shortest non-contractible cycle), underlying group, order of the underlying group, number of graph edges or encoding qubits, for the Ramanujan quantum error-correcting codes. .......... 55
Chapter 1

Introduction

Quantum Computers, first proposed by Feynman in the 1980's, hold the potential to revolutionize information processing. For example, Grover's database search and Shor's factoring algorithm are more efficient than known classical algorithms.

The foundational unit of quantum information is the qubit, a two-dimensional quantum system, whose basis is represented by $|0\rangle$ and $|1\rangle$. In Dirac notation, $|\psi\rangle$, is a pure quantum state. A general quantum state is a complex vector in a Hilbert space:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where $|\alpha|^2 + |\beta|^2 = 1$.

Quantum information channels are models describing the evolution of quantum information over time or space. Analogous to the binary symmetric channel, the quantum binary channel describes the probability of flipping the $|0\rangle$ and $|1\rangle$ basis. The quantum phase-flip channel describes the probability of changing its phase.

Furthermore, experimental noise processes have led to the description of the amplitude-damping channel. This channel describes noise processes due to the energy
dissipation from a quantum system, e.g. the behavior of an atom emitting a photon or of a photon subject to scattering in a cavity [32]. These photonic processes are a promising direction in the realization of scalable quantum computers.

The development of quantum error-correcting codes is fundamental to the development of quantum computers. Most quantum error-correcting codes known are stabilizer or additive codes, which can be described in terms of group theory or of binary vector spaces [24]. In terms of group theory, stabilizer codes are the positive joint eigenstate of an abelian subgroup of tensor products of Pauli error matrices, \( \{ \sigma_x, \sigma_y, \sigma_z, I \} \), where:

\[
\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\]

Note that elements of the stabilizer group have to commute with each other. Otherwise they stabilize the trivial space.

In terms of binary vector spaces, a stabilizer code is described by two binary matrices whose rows represent generators, and whose columns represent different qubits. One of the matrices is associated with \( \sigma_x \), the other with \( \sigma_z \) and entries in both matrices are associated with \( \sigma_y \). The binary vector view of stabilizer codes emphasizes connections between classical and quantum error-correcting codes.
A quantum low-density parity-check (LDPC) error-correcting code is a stabilizer quantum error-correcting code when the associated stabilizer matrices are sparse [31]. Classical low-density parity-check (LDPC) codes were first introduced by Robert Gallager in the 1960’s [23], and have reemerged as one of the most influential coding schemes [34]. The local parity-check dependencies of the codes and their sparsity implies low decoding complexity when using local iterative message-passing decoding algorithms. LDPC and LDPC-like codes decoded with message-passing decoders are used in practice such as in internet and mobile media broadcast, optical networking, among other applications.

Following the same reasoning physical implementations of quantum computers using quantum LDPC error-correcting codes would require sparse local physical interactions. Therefore, the study of quantum LDPC codes can impact the development of scalable quantum computers. It is promising that DiVicenzo [15] has envisioned that quantum computing architectures could be further developed with topological quantum error-correcting codes.

In this thesis, we also analyze more general classes of quantum error-correcting codes, nonadditive quantum error-correcting codes, lack the restrictions of the stabilizer, also called additive, quantum error-correcting codes. Carefully designed nonadditive quantum error-correcting codes can be more optimal than similar stabilizer codes, surpassing standard theoretical bounds. For example, the four-qubit amplitude-damping error-correcting code corrects for one error, and is more optimal than the quantum Hamming bound would predict [18]. In this thesis, we provide a general geometric framework to correct for multiple amplitude-damping errors and develop amplitude-damping error-correcting codes. The amplitude-damping channel describes noise processes that have been observed experimentally due to the energy dissipationn from a quantum system, such as photons in optical cavities and wave packets traveling through space [32]. These photonic processes are another promising
direction in the realization of scalable quantum computers.
Overview

In next chapter, we give definitions and introduce the notation used in this thesis. In the third chapter, we introduce good families of quantum error-correcting codes, review related work, and give an introduction to topological quantum error-correction. In the fourth chapter, we present good families of low-density parity-check error-correcting codes derived from Platonic Surfaces and in the fifth chapter, from Ramanujan Surfaces. For both families, we prove their asymptotic logarithmic distance, calculate their empirical distance, show their asymptotic sparsity and non-vanishing rate, and do experimental decodings with belief propagation. In the sixth chapter, we present a new general geometrical framework for the amplitude-damping channel. This framework gives a characterization useful to build amplitude-damping codes that correct for multiple amplitude-damping errors. In the seventh chapter, we provide our insights and conclusions.
Chapter 2

Definitions

2.1 Graph Theoretical Definitions

In this section we introduce the topological graph-theoretic definitions used in the quantum error-correcting code families of codes that we present in this thesis.

**Definition 1.** Let $G = (V, E)$, where $G$ is a graph, $V$ is a set of vertices, and $E$, a set of edges.

**Definition 2.** If a graph $G$ can be drawn on a 2-dimensional surface or manifold $M$ without edge crossing, then it is said to be *embedded* on this manifold. An embedding of a graph is a tessellation of the *manifold*. The difference between $M$ and the embedded graph is a collection of open discs called faces.

The families of quantum error-correcting codes introduced in chapter 3, 4, and 5 are derived from embeddings of graphs on 2-dimensional surfaces.
Definition 3. The genus of a graph $G$ is the smallest genus of a 2-dimensional manifold $M$ in which the graph can be embedded.

The genus of the surfaces on which these graphs are embedded is related to the number of qubits that can be encoded as explained in the next section, topological quantum error-correcting codes.

Definition 4. A planar graph is a graph that can be embedded in a surface of genus 0, i.e. the plane.

Definition 5. The girth of a graph is the length of its shortest cycle.

Definition 6. The shortest noncontractible cycle of a graph of genus $g$ is the length of the shortest cycle or closed path that is not a face of the induced tessellation. A face is one of the open discs derived from the difference between the two-dimensional manifold $M$ and the embedded graph.

Definition 7. An embedding of a graph is a tessellation of a manifold.

Furthermore, the shortest noncontractible cycle of a graph is related to the number of errors that the quantum-error correcting code can correct as we explain in the next section, topological quantum error-correcting codes.
For additional definitions and background see [17].

2.2 Linear Group Definitions

Our topological families of quantum error-correcting codes are derived from topological graph embeddings, and the knowledge of these additional linear group definitions is needed in the next chapters. In particular, in Chapter 3 and 4 the Platonic and Ramanujan quantum error-correcting codes are defined and the underlying groups are factor groups of the general linear group, $GL$, or the special linear group, $SL$, formally defined in this section.

**Definition 8.** $GL(2,F)$ is the general linear group of $2 \times 2$ invertible matrices over a field $F$ with matrix multiplication as the group operation.

**Definition 9.** $D$ is the set of nonzero diagonal scalar matrices over a field $F$, i.e.

$$D = \left\{ \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \mid x \in F \right\}.$$  

It is the center of $GL(2,F)$. $D$ is a maximal subgroup of commutative elements with $GL(2,F)$. It is a normal subgroup of $GL(2,F)$. Normal subgroups can be used to form quotient or factor groups.

**Definition 10.** $PGL(2,F)$ is the projective general linear group. It is a factor group of $GL(2,F)$.

$$PGL(2,F) = GL(2,F)/D$$

16
Note that the order of $PGL(2,\mathbb{Z}_q)$ is $q(q^2 - 1)$.

**Definition 11.** $SL(2,\mathcal{F})$ is the special linear group of $2 \times 2$ invertible matrices with determinant 1 over a field $\mathcal{F}$ with matrix multiplication as the group operation.

**Definition 12.** $SD$ is the set of nonzero diagonal scalar matrices with unit determinant.

$\Gamma = PSL(2,\mathcal{F})$ is the projective special linear group, also known as the group of linear fractional transformations. It is defined analogously to $PGL(2,\mathcal{F})$.

### 2.3 Number Theoretical Definitions

Relevant number theoretical definitions for the construction of the Lubotzky – Phillips – Sarnak Ramanujan graphs:

**Definition 13.** $x$ is a **quadratic residue** modulo $q$, if there is a $y$ s.t. $y^2 \equiv x \mod q$. If there is no such $y$, then $x$ is a quadratic non-residue.

**Definition 14.** For $x \in \mathbb{Z}$ and $q$ odd positive prime, the Legendre symbol $\left( \frac{x}{q} \right) = 1$, if $x$ is a quadratic residue $\mod p$, and $\left( \frac{x}{q} \right) = -1$, if $x$ is a quadratic non-residue $\mod p$. Note that the following multiplication rule applies: $\left( \frac{xy}{q} \right) = \left( \frac{x}{q} \right) \left( \frac{y}{q} \right)$.
**Definition 15.** The ring of integral quaternions, $\mathbb{H}(\mathbb{Z})$, is defined as follows [13]:

$$
\mathbb{H}(\mathbb{Z}) = \{a_0 + a_1i + a_2j + a_3k : \\
a_0, a_1, a_2, a_3 \in \mathbb{Z}, \\
i^2 = j^2 = k^2 = -1, \\
i j = k, jk = i, ki = j, \\
ji = -k, kj = -i, ji = -k\}$$

**Definition 16.** Define the following homomorphism between the integer quaternions $\mathbb{H}(\mathbb{Z})$ and $PGL(2, \mathbb{Z}_q)$:

$$(a_0 + a_1i + a_2j + a_3k) \rightarrow c \begin{pmatrix}
   a_0 + a_1i & a_2 + a_3i \\
   -a_2 + a_3i & a_0 - a_1i
\end{pmatrix}
$$

where $i^2 = -1 \ mod \ q$. 
Chapter 3

Good Families of Quantum
Low-Density Parity-Check Codes

And do we also remember saying that the children of the good parents were to be brought up, while those of the bad secretly dispersed among the inferior citizens; and while they were all growing up the rulers were to be on the look-out, and to bring from below in turn those who were worthy – Plato

In this chapter we define good families of quantum low-density parity-check error-correcting codes, review related work, and give an introduction to topological quantum error-correcting codes.

3.1 Background

From a theoretical perspective, a good family of error-correcting codes corrects errors in proportion to the blocklength of the codes and has a practical decoder
For example, classical Low-Density Parity-Check codes (LDPC), first introduced by Gallager in the 1960’s [23], approach the Gilbert-Varshamov bound and have a practical decoder.

The existence of good quantum error-correcting codes was shown nonconstructively by Calderbank and Shor in 1996 [11]. In 2001, Ashikhmin introduced a family of asymptotically good quantum codes based on algebraic geometry without any proposed practical decoder [2]. In 2003, MacKay [31] introduced some promising individual examples of quantum LDPC codes. MacKay’s codes are dual-containing stabilizer codes, whose matrix representation is sparse. Several theoretical questions were raised by this work including a conjecture about the existence of families of sparse-graph quantum error-correcting codes with asymptotic non-zero rate, increasing minimum distance and a practical decoder. We answer this conjecture by presenting such families in this thesis.

We present families of good sparse quantum error-correcting codes with asymptotic logarithmic distance. We show their asymptotic sparsity and non-vanishing rate, and experimental results showing their decoding performance with belief propagation. These codes are derived from sparse graphs, induced by tessellations of topological surfaces, and are therefore a type of low-density parity-check (LDPC) codes. Note that while most known LDPC codes usually have constant weight matrices, there are classes of LDPC codes derived from irregular sparse graphs [30].

The families of codes that we present in chapter 4 and 5 are generalizations of Kitaev’s codes [27] to surfaces of genus $g$ that encode $2g$ qubits, as explained in chapter 4. Kitaev’s codes are a class of stabilizer codes derived from lattices on surfaces of single genus, or tori, with asymptotical zero rate. We note that Freedman in 2002, before MacKay’s conjecture in 2003, had independently from our work already discovered a different family of topological quantum error-correcting codes, with asymptotic logarithmic distance [21, 22]. These codes were mentioned in the context of a differe-
ential geometry conjecture by Gromov [25]. They were not studied in the context of quantum LDPC codes, and their properties and performance were not analyzed. Also previously, Dennis in 2001 introduced a family of topological quantum code constructions derived from random high-genus surfaces [14]. Nevertheless, a result by Makover [7] implies that their distance does not increase asymptotically. Furthermore, these codes were also not studied in the context of LDPC codes.

3.2 Topological Quantum Error-Correcting Codes

Topological codes are a class of stabilizer codes associated with tessellations of manifolds. Kitaev’s toric codes are defined by an $L \times L$ square grid on the torus. The encoding qubits are associated with edges of this grid. The related stabilizer quantum error-correcting code check operators are associated with faces and vertices are:

$$Z^{\text{face}} = \prod_{e \in \text{face}} Z_e$$

$$X^{\text{vertex}} = \prod_{e \in \text{vertex}} X_e$$

Note that the vertex and face operators commute because they either act on disjoint qubits or on an even number of qubits in common. By Euler’s equation, these toric codes encode 2 qubits. Since the number of logical qubits remains constant as the number of encoding qubits increases, the rate of a toric family of codes asymptotically vanishes.

In order to generalize toric codes to higher genus surfaces, we study tessellations of an orientable 2-manifold of genus $g$. See Chapter 2 for relevant topological graph-theoretic definitions. Using Euler’s equation $2g$ qubits are encoded. Furthermore,
a noncontractible cycle in the tessellation or dual tessellation commutes with the stabilizer group of the code because it is a cycle. Nevertheless, it is not contained in the stabilizer group. See Chapter 2 for relevant group-theoretic definitions. Therefore, the distance of the code is the length of the shortest non-contractible cycle in the tessellation.
Chapter 4

Platonic Quantum Low-Density Parity-Check Codes

In this chapter we present a family of Platonic Quantum Low-Density Parity-Check codes derived from Platonic Surfaces, which generalize the Platonic Solids. We provide a logarithmic lower-bound on the shortest noncontractible cycle of the tessellation, subdivide the tessellations, derive their asymptotic sparsity and non-vanishing rate, and present experimental simulations of their decoding performance with belief propagation.

4.1 Platonic Surfaces

Platonic Graphs $\pi_n$ are characterized by regular tessellations of 2-manifolds, which are called Platonic Surfaces $S_n$. The mathematical foundation is given in [6].
Definition 17. Platonic Graphs $\pi_n$ are determined by vertices and edges. A vertex of $\pi_n$ is defined by a pair of integers $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ such that $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} -a \\ b \end{smallmatrix}\right)$. The pair is taken projectively, that is, $gcd(a, b) = 1$. An edge joins two vertices, $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} c \\ d \end{smallmatrix}\right)$ iff 

$$
\det \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \pm 1 \mod n.
$$

Furthermore note that the Platonic Graphs have the two-step property [6], that is, any two vertices have exactly two paths of length two, associating $\pi_n$ to a unique triangulated topological 2-manifold. Also note that $n$ does not have to be a prime number. When $n \geq 6$, we obtain a tessellation of a surface of genus $\geq 1$.

The first few Platonic graphs are the tetrahedron $\pi_3$, the octahedron $\pi_4$, and the icosahedron $\pi_5$. The Dual Platonic graphs, $\pi'_n$, have a vertex for each triangular face in $\pi_n$, and an edge between two vertices iff the respective $\pi_n$ faces are adjacent. The first few dual Platonic Graphs are the tetrahedron $\pi'_3$ (self-dual), the cube $\pi'_4$, and the dodecahedron $\pi'_5$.

For $p$ prime, the graph $\pi_p$ has $\frac{p^2 - 1}{2}$ vertices. Let $v_p$ be the number of vertices of $\pi_p$, then there are $\frac{v_p p}{2}$ edges $e_p$, and $\frac{v_p p}{3}$ faces $f_p$. For $\pi'_n$, there are $v'_p = f_p$, $e'_p = e_p$, and $f'_p = v_p$. The genus $g_p$ of the associated Platonic surface is given by: $g_p = 1 + \frac{v_p (p-6)}{12}$. Similar formulas can be obtained for $\pi_n$, when $n$ is not prime.

4.2 Platonic Quantum Low-Density Parity-Check Codes

In this section we give an example of a quantum code derived from the Platonic Surface $\pi_7$, and an infinite family of good LDPC codes derived from Platonic Surfaces. We calculate their asymptotic rate, analyze their sparsity and provide a lower bound on their distance, the length of the shortest non-contractible cycle, as well as empirical calculations of these lengths.
4.2.1 Platonic $\pi_7$ Code

The Platonic quantum code derived from $\pi_7$ has $\frac{p^2-1}{2} = 24$ vertices $v_p$, $\frac{v_pP}{3} = 56$ faces, and $\frac{v_pP}{2} = 84$ edges, and that it follows that the $g = 3$ is the genus of the surface. Therefore, it has quantum rate 1/14. For $\pi_7'$, there are 56 vertices, 24 faces, and 84 edges. Its shortest non-contractible cycle is of length 8. One such cycle is for example:

$$
\begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix},
\begin{bmatrix}
1 & 1 \\
0 & 1
\end{bmatrix},
\begin{bmatrix}
2 & 1 \\
1 & 2
\end{bmatrix},
\begin{bmatrix}
2 & 3 \\
3 & 2
\end{bmatrix},
\begin{bmatrix}
5 & 3 \\
3 & 5
\end{bmatrix},
\begin{bmatrix}
5 & 1 \\
1 & 8
\end{bmatrix},
\begin{bmatrix}
6 & 1 \\
1 & 6
\end{bmatrix},
\begin{bmatrix}
6 & 0
\end{bmatrix}
$$

4.2.2 Family of Platonic Quantum Low-Density Parity-Check Codes

In general, we derive a family of quantum LDPC codes from the dual Platonic graphs $\pi_p'$, analyze their rate, and their distance by providing a theoretical bound on the length of the shortest non-contractible cycle, and also empirical calculations of these lengths.

4.2.3 Asymptotic Rate for the Platonic Family of Quantum LDPC Error-Correcting Codes
Figure 4.2.1: Platonic graph $n_7$ adjacency matrix. The vertical and horizontal axis represent ordered vertices of the graph. $nz$ is the number of non-zero elements in the matrix, which is twice the number of edges in the graph.
We calculate the non-vanishing asymptotic rate of the check-operators of the dual Platonic quantum LDPC error-correcting codes.

The $Z^{face}$ check operator of dual Platonic quantum LDPC error-correcting codes have rate approaching $1$, for $p$ odd prime.

\[
\lim_{p \to \infty} \frac{e_p' - (f_p' - 1)}{e_p'} = \frac{\varepsilon^3_{34} - \left( \frac{\varepsilon^3_{24} - 1}{2} \right)}{\varepsilon^3_{43}} = 1
\]

The $X^{vertex}$ check operator of a dual Platonic quantum LDPC error-correcting code has rate approaching $\frac{1}{3}$, for $p$ odd prime.

\[
\lim_{p \to \infty} \frac{e_p' - (v_p' - 1)}{e_p'} = \frac{\varepsilon^3_{43} - \left( \frac{\varepsilon^3_{62} - 1}{2} \right)}{\varepsilon^3_{43}} = \frac{1}{3}
\]

The average combined rate of the $X^{vertex}$ and $Z^{face}$ operators approaches $\frac{2}{3}$, for $p$ odd prime.

\[
\lim_{p \to \infty} \frac{2e_p' - (f_p' + v_p' - 2)}{2e_p'} = \lim_{p \to \infty} 1 - \frac{f_p' + v_p' - 2}{2e_p'} = \lim_{p \to \infty} 1 - \frac{1}{p} - \frac{1}{3} + \frac{1}{p^{1-p}} = \frac{2}{3}
\]
4.2.4 Asymptotic Sparsity Analysis for the Platonic Family of Quantum LDPC Error-Correcting Codes

We calculate the asymptotic sparsity of the check-operators of the dual Platonic quantum LDPC error-correcting codes.

Let $w_f$ be the weight of the $Z$-face check operators of a dual Platonic quantum LDPC error-correcting code, and let $e_p$ be the corresponding number of encoding qubits for prime $p$, then $\frac{w_f}{e_p}$ converges to a $c.p^{-2}$.

\[
\lim_{p \to \infty} \frac{p}{e_p} = \\
\lim_{p \to \infty} \frac{p}{\frac{e_p}{2}} = \\
\lim_{p \to \infty} \frac{p}{\frac{e_p}{4}} = \\
c.p^{-2}
\]

Let $w_v = 3$ be the weight of the $X$-vertex check operators of a dual Platonic quantum LDPC error-correcting code, and let $e_p$ be the corresponding number of encoding qubits for prime $p$, then $\frac{w_v}{e_p}$ converges to zero.

\[
\lim_{p \to \infty} \frac{3}{e_p} = \\
0
\]

4.2.5 Shortest Noncontractible Cycle Bound, $snc \sim \log(p)$, for the Dual Platonic Surfaces $\pi'_p$.  

28
In this section we show that the shortest non-contractible cycle of the family of dual platonic graphs \( \pi'_p \) grows logarithmically in the size of their genus. We derive the bound by regarding these graphs as quotient of \( T_3 \), the infinite cubic tree. Vertices of \( T_3 \) are labeled with unordered triplets and mapped to vertices of the platonic graphs \( \pi \), or to faces of the dual graphs \( \pi' \) respectively. The labeling in \( T_3 \), with unordered triplets of irreducible rational numbers \( \left( \begin{array}{c} a \\ b \\ c \\ d \\ f \end{array} \right) \) is known as a Farey Tree, which has many interesting properties [3, 4].

**Definition 18.** \( T_3 \) is defined recursively by generalizing the labels of the following rooted binary tree \( B \). The root of \( B \) is \( \left( \begin{array}{c} 0 \\ 1 \\ 2 \\ 1 \\ 1 \end{array} \right) \). For a vertex \( \left( \begin{array}{c} a \\ b \\ c \\ d \\ f \end{array} \right) \) in \( B \), its left child is \( \left( \begin{array}{c} a \\ b+c \\ c \\ d+b \\ f \end{array} \right) \), and its right child is \( \left( \begin{array}{c} c \\ d \\ c+f \\ d+f \\ e \end{array} \right) \). \( B_n \) is obtained from \( B \) by adding \( n \) to the pairs, that is \( \left( \begin{array}{c} a \\ b \\ c \\ d \\ f \end{array} \right) \) is relabeled as \( \left( \begin{array}{c} a+n \\ b \\ c \\ d \\ f \end{array} \right) \). \( B_0 \) is \( B \), and \( T_3 \) is obtained by attaching the root of \( B_n \) to \( \left( \begin{array}{c} 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{array} \right) \).

In [4] the girth of a family of 3-regular graphs, the triplets \( T(p) \), is analyzed by mapping each pair \( \left( \begin{array}{c} a \\ b \end{array} \right) \) to \( a \cdot b^{-1} \mod p \). If \( b=0 \), then \( a \cdot b^{-1} \mod p \) is mapped to \( \infty \). We obtain the dual Platonic graphs \( \pi' \) from \( T_3 \) under the equivalence \( \left( \begin{array}{c} a \\ b \end{array} \right) \sim \left( \begin{array}{c} a \\ -b \end{array} \right) \mod p \). \( T(5) \) is Petersen’s graph, and \( \pi'(5) \) is the dodecahedron.

Using properties and symmetries of \( T_3 \), we show that the shortest non-contractible cycle \( snc \) in the graph \( \pi'_p \), for \( p \) prime, is bounded by \( p^2 \leq \text{Fibonacci}(snc+2) \) for large \( p \). This implies that \( \text{girth} \sim \log(p) \) for large \( p \), which is smaller than the size of the faces, \( p \), on the surfaces. Therefore, \( snc \sim \log(p) \).

**Theorem 19.** The shortest noncontractible cycle bound \( snc \) for the Dual Platonic Surfaces \( \pi'_p \), is \( \sim \log(p) \).
Proof

We provide relevant lemmas about $B$ [3] and prove a lemma about a needed symmetry of the tree.

Lemma. For any vertex $\left( \binom{a}{b} \binom{c}{d} \binom{e}{f} \right)$ in the rooted binary tree $B$,

$$b \cdot c - a \cdot d = d \cdot e - c \cdot f = 1.$$ 

Corollary

For each pair $\left( \binom{a}{b} \right)$,

$$\gcd(a, b) = 1.$$

Lemma. The largest $b$ in a pair $\left( \binom{a}{b} \right)$ at level $r$, is $Fibonacci(r + 2)$.

In addition, we observe that there is a symmetry of the tree $B$ that preserves the level of the vertices and induces a reflection on the tree. The symmetry is given by $\left( \binom{b-a}{b} \right)$ on each pair. In the following lemma we use $x$, as short for $\left( \binom{a}{b} \right)$, and $(1 - x)$ as short for $\left( \binom{b-a}{b} \right)$.

Lemma. Let $\left( \binom{x}{y} \binom{z}{} \right)$ be a vertex $v$, then the involution $i$ that takes $v$ to $\left( \binom{1-z}{1-y} \binom{1-x}{} \right)$ is a reflection of the tree $B$.

Proof. We prove this lemma by induction. Note that the root of $B$, $\left( \binom{0}{1} \binom{1}{2} \binom{1}{1} \right)$, is
a fixed point of the symmetry. Assume that the symmetry holds for all vertices in $B$
at levels less than $n$. Let $v = \left( \begin{array}{ccc} a & b & c \\ d & e & f \end{array} \right)$, be a vertex at level $n - 1$. Denote the
involution on $v$, as $i(v) = \left( \begin{array}{ccc} f & e & d \\ f & d & b \end{array} \right)$. Denote the left descendant of $v$
as $v_{\text{left}}$, and the right descendant as $v_{\text{right}}$. Then,

$$v_{\text{left}} = \left( \begin{array}{ccc} a & b & c \\ d & e & f \end{array} \right)$$

and

$$v_{\text{right}} = \left( \begin{array}{ccc} c & d & e \\ f & b & f \end{array} \right)$$

Under the involution, the results are:

$$i(v_{\text{left}}) = \left( \begin{array}{ccc} d & c & b + d - c - a \\ d & b + d & b \end{array} \right)$$

and

$$i(v_{\text{right}}) = \left( \begin{array}{ccc} f & e & d - c \\ f & b + f & d \end{array} \right)$$

which implies that $i(v_{\text{left}}) = (i(v))_{\text{right}}$, and $i(v_{\text{right}}) = (i(v))_{\text{left}}$.

\[\square\]

**Theorem 20.** Let $scn$ be the shortest non-contractible cycle in the graph $\pi'_p$, for $p$
prime, then $p^2 \leq \text{Fibonacci} \ (snc + 2)$ for large $p$. 

31
Proof. Since \( \pi'_p \) is vertex transitive, we consider only the cycles from vertex labeled \( ((1) (0) (1)) \). Note that a set of pairs \( ((c) (e) (f)) \) corresponds to a vertex in \( \pi'_p \) and a face \( \pi_p \). Each individual pair corresponds to a vertex in \( \pi_p \). There are six ways in which a vertex in \( T_3 \) can reduce to \( ((1) (0) (1)) \), that is all 6 permutations of the 3 pairs. In addition, the reflection symmetry lemma proved in 4.2.5 allows us to consider only 4 cases. Note that under this symmetry, the following cases are equivalent \( ((0) (1) (0)) \sim ((1) (0) (1)) \) and \( ((1) (0) (1)) \sim ((1) (1) (0)) \).

Case \( ((0) (1) (1)) \)

\[
\begin{pmatrix}
  a \cdot p + e \cdot p + 1 \\
  f \cdot p + b \cdot p + 1 + g
\end{pmatrix}
\]

In order for the middle pair \( (a \cdot p + e \cdot p + 1) \) to reduce to \( (0) \), \( g = -1 \). By applying the first lemma to the other two pairs in the triple, we get a contradiction.

Case \( ((0) (1) (0)) \)

We get a similar contradiction to the previous case.

Case \( ((1) (0) (1)) \)

A vertex that reduces to \( ((1) (0) (1)) \) must be of the form

\[
\begin{pmatrix}
  (a \cdot p \mp 1) \\
  b \cdot p
\end{pmatrix}
\begin{pmatrix}
  a \cdot p + e \cdot p \\
  b \cdot p + f \cdot p \mp 1
\end{pmatrix}
\begin{pmatrix}
  e \cdot p \mp 1 \\
  f \cdot p \mp 1
\end{pmatrix}
\]

For simplicity let \( c = a + e \) and \( d = b + f \). Then by applying the first lemma to the first two pairs, we get:
\[ b \cdot c \cdot p^2 - (a \cdot p \pm 1) \cdot (dp \mp 1) = 1 \]

which implies that
\[ \mp d = (a \cdot d - b \cdot c) \cdot p \mp a \]

Let \( a \cdot d - b \cdot c = g \). Then a vertex that reduces to \( (\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}) \) has the following form:

\[
\begin{pmatrix}
(a \cdot p \pm 1) & c \cdot p \\
b \cdot p & g \cdot p^2 \mp a \cdot p \mp 1
\end{pmatrix}
\begin{pmatrix}
e \cdot p \mp 1 \\
f \cdot p \mp 1
\end{pmatrix}
\]

Case(\( (\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}) \))
We get a similar reduction.

Therefore

\[ p^2 \leq \text{Fibonacci}(\text{girth} + 2) \]

which implies that \( \text{girth} \sim \log(p) \) for large \( p \), which is smaller than the size of the faces, \( p \), on the surfaces. Therefore, \( \text{snc} \sim \log(p) \).

### 4.2.6 Empirical Calculations of the Shortest Noncontractible Cycle for the Dual Platonic Surfaces \( \pi'_p \)

We calculate the empirical length of the shortest non-contractible cycle for the first 34 dual platonic graphs, \( \pi'_n \) [33]. In figure 4.2.2, we plot the bound derived in the previous section together with our empirical calculation results.
Figure 4.2.3: The vertical axis represents the number of vertices in the graph. The horizontal axis represents the parameter $n$. The star line shows $n^2$ and the solid line shows the Fibonacci number of the empirical shortest non-contractible cycle of the platonic graphs as a function of $n$. 
<table>
<thead>
<tr>
<th>Platonic n</th>
<th>distance ((snc))</th>
<th>genus</th>
<th>n</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>8</td>
<td>1</td>
<td>36</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>3</td>
<td>84</td>
</tr>
<tr>
<td>8</td>
<td>10</td>
<td>5</td>
<td>96</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
<td>10</td>
<td>162</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>13</td>
<td>180</td>
</tr>
<tr>
<td>11</td>
<td>10</td>
<td>36</td>
<td>330</td>
</tr>
<tr>
<td>12</td>
<td>10</td>
<td>25</td>
<td>288</td>
</tr>
<tr>
<td>13</td>
<td>12</td>
<td>50</td>
<td>546</td>
</tr>
<tr>
<td>14</td>
<td>12</td>
<td>49</td>
<td>504</td>
</tr>
<tr>
<td>15</td>
<td>12</td>
<td>73</td>
<td>720</td>
</tr>
<tr>
<td>16</td>
<td>12</td>
<td>81</td>
<td>768</td>
</tr>
<tr>
<td>17</td>
<td>15</td>
<td>133</td>
<td>1224</td>
</tr>
<tr>
<td>18</td>
<td>12</td>
<td>109</td>
<td>972</td>
</tr>
<tr>
<td>19</td>
<td>14</td>
<td>196</td>
<td>1710</td>
</tr>
<tr>
<td>20</td>
<td>14</td>
<td>169</td>
<td>1440</td>
</tr>
<tr>
<td>21</td>
<td>14</td>
<td>241</td>
<td>2016</td>
</tr>
<tr>
<td>22</td>
<td>14</td>
<td>241</td>
<td>1980</td>
</tr>
<tr>
<td>23</td>
<td>14</td>
<td>375</td>
<td>3036</td>
</tr>
<tr>
<td>24</td>
<td>14</td>
<td>289</td>
<td>2304</td>
</tr>
<tr>
<td>25</td>
<td>16</td>
<td>476</td>
<td>3750</td>
</tr>
<tr>
<td>26</td>
<td>14</td>
<td>421</td>
<td>3276</td>
</tr>
<tr>
<td>27</td>
<td>16</td>
<td>568</td>
<td>4374</td>
</tr>
<tr>
<td>28</td>
<td>18</td>
<td>529</td>
<td>4032</td>
</tr>
<tr>
<td>29</td>
<td>16</td>
<td>806</td>
<td>6090</td>
</tr>
<tr>
<td>30</td>
<td>16</td>
<td>577</td>
<td>4320</td>
</tr>
<tr>
<td>31</td>
<td>18</td>
<td>1001</td>
<td>7440</td>
</tr>
<tr>
<td>32</td>
<td>16</td>
<td>833</td>
<td>6144</td>
</tr>
<tr>
<td>33</td>
<td>18</td>
<td>1081</td>
<td>7920</td>
</tr>
</tbody>
</table>

Table 4.1: Table with the distance (shortest non-contractible cycle), genus and number of encoding qubits for the platonic quantum low-density parity-check error-correcting codes.
Interestingly, for \( \pi_{28} \), the length of the shortest non-contractible cycle is 18, and the girth of a graph is a lower bound on the length of the shortest non-contractible cycle of a graph. Since \( \pi_{28} \) has regular 28-gon faces, the girth 18 of this graph is the length of its shortest noncontractible cycle.

4.3 Belief-Propagation Decoding

We study the performance of the codes using belief propagation by simulating the 4-ary symmetric channel as two independent binary symmetric channels in order to make their performance comparable to MacKay’s sparse-graph quantum codes [31].

We model \( X^{\text{vertex}} \) and \( Z^{\text{face}} \) errors independently. Each decoding simulation either finds the correct decoding or a block error. Block error probability is calculated as a function of the flip probability \( f_m \) [31]. This is the probability with which we independently flip each bit. In particular, we show the flip probability \( f_m \) at which the probability of block decoding error is \( 10^{-4} \) (0.9999) by performing several simulated decodings.

We provide a summary of the performance of the Platonic codes and derived subfamilies in figure 4.3. The smooth curve shown in the figure is the Shannon limit, and the dotted curve is the Gilbert-Varshamov bound [24, 31].

All simulation labels start at Platonic \( n = 6 \). The red line represents the Platonic quantum codes without subtessellations. Their \( Z^{\text{face}} \) parity-check simulations starting at \( n = 6 \), are labeled \( \text{faces}6 \), and each additional matrix is denoted by a circle. Note that their rate approaches 1 as shown in theorem 4.2.3. Their \( X^{\text{vertex}} \) parity-check simulations are labeled \( \text{stars}6 \), and each additional matrix is denoted by a star. Their rate approaches \( \frac{1}{3} \) as shown in theorem 4.2.3.
Their $Z^{face}$ and $X^{vertex}$ average simulation performance is labeled as $comb6$, and each additional matrix is denoted by a dot. Their average rate approaches $\frac{2}{3}$ as shown in theorem 4.2.3. The average performance of the Platonic quantum codes without subtessellations is better than the Platonic quantum codes with subtessellations.

We also obtain subfamilies of Platonic codes by subtessellating the Platonic $n$-gons. Each face in $\pi'_n$ for $n \geq 6$ is subtessellated with pentagons in order to obtain better distance parameters. We obtain two subfamilies depending on the alignment of the subtessellations, both random and symmetric, and on the depth of the recursion. Symmetric subtessellations have neighboring $n$-gons whose subtessellations are aligned.

The black line represents Platonic quantum codes with randomly aligned pentagon subtessellations. Their $Z^{face}$ parity-check simulations are labeled as $rp6$, and each additional matrix is denoted by a circle. Their $X^{vertex}$ parity-check simulations are labeled $rp6$, and each additional matrix is denoted by a star.

Their $X^{vertex}$ and $Z^{face}$ average simulation performance starting at $n = 6$ is labeled $rp6$, and each additional matrix is denoted by a dot. Similarly, the purple line represents Platonic quantum codes with symmetrically aligned pentagon subtessellations, labeled as $ap6$, and the blue line represents codes with double-level pentagon subtessellations, labeled as $a2p6$.

We finally note that the average experimental decoding performance of the the Platonic quantum codes without subtessellations is better than the Platonic quantum codes with subtessellations.
Figure 4.3.1: Simulation results for the quantum error-correcting codes derived from Platonic surfaces. The $Y$ coordinate is the code rate. The $X$ coordinate represents the flip probability $f_m$ at which the probability of block decoding error is $10^{-4}$ (0.9999 threshold). All simulation labels start at Platonic $n = 6$. For more information about the labels, read the section simulation results. The smooth curve shown in blue is the Shannon limit, and the dotted curve shown in blue is the Gilbert-Varshamov bound.
Chapter 5

Ramanujan Quantum

Error-Correcting Codes

Ramanujan graphs are \((p + 1)\)-regular graphs whose second largest eigenvalue \(\lambda_1\) with respect to its adjacency matrix is less than or equal \(2 \sqrt{p}\). They achieve extremal properties such as large chromatic number, large girth, and exceptional expansion.

**Definition 21.** A graph \(G = (V,E)\) is an \((n,m,\delta)\)-expander graph if for every subset of at most \(m\) vertices expands by at least a fraction \(\delta\), where \(\delta\) is considered the expansion factor, that is, \(\forall S \subset V\) with \(|S| \leq n/2\), \(|N(S)| \geq \delta |S|\), where \(|N(S)|\) is the set of vertices in \(V \setminus W\) adjacent to a vertex in \(W\) [1, 39].

Ramanujan graphs have been used to build classical low-density parity-check (LDPC) error-correcting codes with efficient parameters and decoding properties [35, 41]. Sipser and Spielman use expander graphs to build classical LDPC codes, and use non-constructive expander-based arguments to analyze their good decoding performance [39]. In 2000, Rosenthal and Vontobel, first investigated the practical perfor-
mance of codes derived from Ramanujan graphs with remarkable results [35]. Most recently, Burshtein and Miller generalized expander-based arguments to prove the good decoding performance for various LDPC iterative message-passing decoding algorithms [10].

Several explicit constructions of Ramanujan graphs are known. In particular, there is a well-known algebraic construction of an infinite family of Ramanujan graphs due to Lubotzky, Phillips, and Sarnak (LPS) [29, 13].

**Definition 22.** For all primes $p, q ≡ 1 \mod 4$, $p ≠ q$, the Lubotzky-Phillips-Sarnak Ramanujan graphs $X^{p,q}$ are $(p+1)$-regular Cayley graphs of $PSL(2, \mathbb{Z}_q)$ when $\left(\frac{p}{q}\right) = 1$, and of $PGL(2, \mathbb{Z}_q)$ when $\left(\frac{p}{q}\right) = -1$ respectively, such that the second-largest eigenvalue of the graphs is at most $2\sqrt{p}$ [29, 13].

Note that Cayley graphs are undirected graphs derived from groups. Cayley graphs are formally defined below, and the relevant number theoretical definitions are given in the next section. For the LPS Ramanujan graphs, the underlying groups are either the projective special linear group, $PSL$, or the projective general linear group, $PGL$, whose definitions can be found in Chapter 2 under linear group definitions.

**Definition 23.** A **Cayley graph** is a graph $C = (G, S)$ where $G$ is a group, and $S$ is a set of generators. $C$ is an undirected $|S|$-regular graph. Each vertex of the graph corresponds to an element of the group $G$. There is an edge between two vertices, $g_1$ and $g_2$, if and only if $\exists s \in S$ such that $g_1.s = g_2$. The girth of a Cayley graph is the length of its shortest nontrivial identity relation.
We build an infinite family of good topological quantum LDPC quantum error-correcting codes with the LPS family of Ramanujan graphs. Our codes are derived from topological embeddings of Ramanujan graphs on 2-manifolds, and improves on our previous family of asymptotically good quantum LDPC codes with nonzero rate, increasing minimum distance, and a practical decoder. It further provides another example that answers MacKay's conjecture about the existence of such families of quantum LDPC codes.

5.1 LPS Ramanujan Graphs Properties

In this section, we provide known upper and lower bounds on the the girth of the LPS family of Ramanujan graphs $X^{p,q}$, and explain how to the generating sets of these graphs can be derived. See Chapter 2 for relevant number theoretical definitions for the construction of LPS Ramanujan graphs.

**Theorem 24.** If $\left( \frac{p}{q} \right) = -1$, the girth of the Ramanujan graph $X^{p,q} \geq 4\log p - \log q$.

Note that this is asymptotically the the largest known girth for a k-regular graph. The asymptotic girth for a random k-regular graph is $\log_{k-1} n$ [13, 36].

**Theorem 25.** If $\left( \frac{p}{q} \right) = -1$, the girth of the Ramanujan graph $X^{p,q} \leq 4 \log p - \log q + 2$. 

41
This a theoretical upper bound for the girth of Ramanujan graphs [5].

**Definition 26.** When $p \equiv 3 \ (mod\ 4)$, or $p \equiv 1 \ (mod\ 4)$, the generating set for $X^{p,q}$ is the set of integral quaternions, described earlier in this chapter in the section Number Theoretical definitions, $S_p$, of cardinality $p + 1$, and of norm $p$. These are the $p + 1$ integer solutions, according to a theorem by Jacobi [35], to $p = a_o^2 + a_1^2 + a_2^2 + a_3^2$ with $a_0 > 0$ and odd, and $a_1, a_2, a_3$ even.

**Ramanujan $X^{5,13}$ graph**

For $p = 5$, and $q = 13$, we build $X^{5,13}$ as follows:

We obtain the generators, $S_5$, given from the 6 integer solutions of norm 5 to $5 = a_o^2 + a_1^2 + a_2^2 + a_3^2$ with $a_0 > 0$ and odd, and the $a_1, a_2, a_3$ even:

$$S_5 = (a_0, a_1, a_2, a_3, a_4) = \begin{cases} (1, 2, 0, 0) \\ (1, -2, 0, 0) \\ (1, 0, 2, 0) \\ (1, 0, -2, 0) \\ (1, 0, 0, 2) \\ (1, 0, 0, -2) \end{cases}$$

Or in quaternion notation,
Furthermore, by using the quaternion homomorphism previously described and by observing that $5^2 \equiv -1 \mod 13$, we get,

$$S_5 = \{1 + 2i, 1 - 2i, -1j, 1 - 2j, 1 + 2k, 1 - 2k\}$$

Since $(\frac{5}{13}) = -1$, $X^{5,13}$ is a Cayley graph of $PGL(2,13)$. Since $|PGL(2,13)| = 2,184$, then $X^{5,13}$ has 2,184 vertices, and since the order of generating set $|S_5| = 6$, then $X^{5,13}$ is a 6 regular graph.

**Ramanujan $X^{5,17}$ graph**

For $p = 5$, and $q = 17$, we build $X^{5,17}$ as follows:

We obtain the generators, $S_5$, given from the 6 integer solutions of norm 5 to $5 = a_0^2 + a_1^2 + a_2^2 + a_3^2$ with $a_0 > 0$ and odd, and the $a_1, a_2, a_3$ even:
Figure 5.1.1: Ramanujan graph $X^{5,13}$ adjacency matrix. On close-up, the blocks appear randomly sparsely filled.
\[ S_5 = (a_0, a_1, a_2, a_3, a_4) = \{(1,2,0,0)\}
\{(1,2,0,0)\}
\{(1,-2,0,0)\}
\{(1,0,0,2)\}
\{(1,0,0,-2)\}\]

Or in quaternion notation,

\[ S_5 = \{1 + 2i, 1 - 2i, -1j, 1 - 2j, 1 + 2k, 1 - 2k\} \]

Furthermore, by using the quaternion homomorphism previously described and by observing that \(4^2 \equiv -1 \mod 17\), we get,

\[ S_5 = \left\{ \begin{pmatrix} 1 \pm 8 & 0 \\ 0 & 1 \mp 8 \end{pmatrix}, \begin{pmatrix} 1 \pm 2 \\ \mp 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 \mp 8 \\ \pm 8 & 1 \end{pmatrix} \right\} \]
Figure 5.1.2: Ramanujan graph $X^{5,17}$ adjacency matrix. On close-up, the blocks appear randomly sparsely filled.
In addition since \((\frac{5}{17}) = -1\), then \(X^{5,17}\) is a Cayley graph of \(PGL(2, \mathbb{Z}_{17})\). Since \(|PGL(2, \mathbb{Z}_{17})| = 4,896\), then \(X^{5,17}\) has 4,896 vertices, and since the order of the generating set \(|S_5| = 6\), then \(X^{5,17}\) is a 6 regular graph.

5.2 Ramanujan Surfaces

In general for a given connected graph, \(G\), a rotation scheme is an algebraic description of an embedding of a graph on a 2-dimensional manifold or surface. A rotation, for a vertex \(i \in V\), is a cyclic permutation of \(N(i)\), where \(N(i)\) is the set of all vertices adjacent to \(i\), and a rotation scheme for a graph consists of one such rotation for each vertex in the graph [17].

**Definition 27.** For a Cayley graph \(C = (G, S)\), where \(G\) is a group and \(S\) is a set of generators, each edge in the graph is labeled by an element of the generating set \(S\). An embedding of a Cayley graph on a 2-dimensional manifold or surface is homogeneous, by assigning a rotation of the generators \(S\) at the identity vertex, and using this ordering at all of the vertices of the Cayley graph [9, 8].

In an homogeneous embedding of the Ramanujan graph \(X^{p,q}\), for each vertex, there are \(p+1\) adjacent faces in the embedding. Let the length of each of these faces be denoted by \(f_i\), so we have \(f_{p+1}\) faces. Furthermore, each \(f_i\) is at most twice the order of an element of the underlying group \(G^{p,q}\) of the Ramanujan graph \(X^{p,q}\). This implies that each \(f_i\) must divide either \(2q\), \(2(q - 1)\) or \(2(q + 1)\) [9].

In addition, for the embedding of \(X^{p,q}\), we get that [9]:

47
\[ 2 - 2g = |G^{p,q}| \left[ \sum_{i=1}^{p+1} \frac{1}{f_i} - \frac{p - 1}{2} \right] \]

**Ramanujan \(X^{2,3}\) Example**

Following the cubic Ramanujan graph constructions by Chiu [12], for \(p = 2\) and \(q = 3\), we build the smallest such Ramanujan graph, \(X^{2,3}\), as follows:

The generators \(S_3\) in \(PGL(2, \mathbb{Z}_3)\) are:

\[
S_3 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}
\]

In addition, since \((\frac{2}{3}) = -1\), then \(X^{2,3}\) is a Cayley graph of \(PGL(2, \mathbb{Z}_3)\). Since \(|PGL(2, \mathbb{Z}_3)| = 24\), then \(X^{2,3}\) has 24 vertices, and since \(|S_2| = 3\), then \(X^{2,3}\) is a 3 regular graph. See Figure 5.2.1 for the Ramanujan graph \(X^{2,3}\) [12, 36], and Figure 5.2.2, for the homogeneous embedding of the Ramanujan graph \(X^{2,3}\) [9].

**5.3 Ramanujan Quantum Error-correcting Codes**

We derive a family of quantum LDPC codes from the Ramanujan surfaces of \(X^{p,q}\), analyze their rate, sparsity and distance.

**5.3.1 Asymptotic Rate for the Ramanujan Quantum LDPC Error-Correcting Codes**
Figure 5.2.1: Ramanujan graph $X^{2.3}$

Figure 5.2.2: Embedded Ramanujan graph $X^{2.3}$
We calculate the non-vanishing asymptotic rate of the check-operators of the Ramanujan quantum LDPC error-correcting codes.

The $Z^{face}$ check operators of the Ramanujan quantum LDPC error-correcting codes have rate approaching $1$.

\[
\lim_{q \to \infty} \frac{e_{p,q} - (f_{p,q} - 1)}{e_{p,q}} = 1
\]

\[
\lim_{q \to \infty} \frac{|G_{p,q}| \frac{p+1}{2} - (f_{p,q} - 1)}{|G_{p,q}| \frac{p+1}{2}} = \frac{p-1}{p+1}
\]

The $X^{vertex}$ check operators of the Ramanujan quantum LDPC error-correcting codes have rate approaching $\frac{p-1}{p+1}$.

\[
\lim_{q \to \infty} \frac{e_{p,q} - (v_{p,q} - 1)}{e_{p,q}} = 1
\]

\[
\lim_{q \to \infty} \frac{|G_{p,q}| \frac{p+1}{2} - (|G_{p,q}| - 1)}{|G_{p,q}| \frac{p+1}{2}} = \frac{p-1}{p+1}
\]

The average combined rate for the $X^{vertex}$ and $Z^{face}$ operators approaches $\frac{p}{p+1}$.

5.3.2 Sparsity Analysis for the Ramanujan Quantum LDPC Error-Correcting Codes

We calculate the asymptotically vanishing sparsity of the check-operators of the
Let $w_f$ be the weight of the $Z^{face}$ check operators of a Ramanujan quantum LDPC error-correcting code, and let $e_{p,q}$ be the corresponding number of encoding qubits for primes $p, q$, then $\frac{w_f}{e_p}$ converges to zero.

$$\lim_{q \to \infty} \frac{w_f}{e_{p,q}} \leq$$
$$\lim_{q \to \infty} \frac{2(q+1)}{|G_{p,q}|^{\frac{q+1}{2}}} = 0$$

Note that $w_f$ is at most twice the order of an element of the underlying group.

Let $w_v = p + 1$ be the weight of the $Z^{vertex}$ check operators of a Ramanujan quantum LDPC error-correcting code, and let $e_{p,q}$ be the corresponding number of encoding qubits for primes $p, q$, then $\frac{w_v}{e_{p,q}}$ converges to zero.

$$\lim_{q \to \infty} \frac{w_v}{e_{p,q}} =$$
$$\lim_{q \to \infty} \frac{p+1}{|G_{p,q}|^{\frac{p+1}{2}}} = 0$$

### 5.3.3 Ramanujan Surface Shortest Noncontractible Cycle ($snc$)

We calculate the empirical length of the shortest non-contractible cycle for the
Figure 5.3.1: The vertical axis represents the prime $q$. The horizontal axis represents the length of the cycle. The stars show the empirical length of the shortest non-contractible cycle of the Ramanujan graph $X^{p,q}$ as a function of $q$, when $\left( \frac{p}{q} \right) = -1$. The solid line shows the theoretical lower bound for the girth of $X^{p,q} \geq 4 \log_p q - \log_4 4$. 

52
first few 6-regular Ramanujan surfaces [33]. In Table I, we present these lengths (shortest non-contractible cycles). Note that the girth of a graph is a lower bound on the length of the shortest non-contractible cycle of a graph. Ramanujan graphs have asymptotically a logarithmic girth lower bound, which is the best known bound for regular graphs. Also note that a logarithmic lower bound is the best known shortest non-contractible cycle bound in the theory of regular tessellations of 2-manifolds [26].

5.4 Belief-Propagation Decoding

We study the performance of the codes using belief propagation by simulating the 4-ary symmetric channel as two independent binary symmetric channels in order to make their performance comparable to MacKay’s sparse-graph quantum codes [31].

We model $X^{\text{vertex}}$ and $Z^{\text{face}}$ errors independently. Each decoding simulation either finds the correct decoding or a block error. Block error probability is calculated as a function of the flip probability $f_m$ [31]. This is the probability with which we independently flip each bit.

We provide a summary of the performance of the Platonic codes and derived subfamilies in figure 4. In particular, we show the flip probability $f_m$ at which the probability of block decoding error is $10^{-4}$ by performing several simulated decodings. The smooth curve shown in the figure is the Shannon limit, and the dotted curve is the Gilbert-Varshamov bound [24, 31].

The simulation labels start at 5 – 13, denoting the embedded $X^{5,13}$ and are in addition presented for the embedded $X^{5,17}$, and $X^{5,29}$. Their $X^{\text{vertex}}$ parity-check simulations are denoted by a star. Their $Z^{\text{face}}$ parity-check simulations are denoted by a circle. And their $Z^{\text{face}}$ and $X^{\text{vertex}}$ average simulation performance is denoted
by a dot.

In addition we show both the Ramanujan and Platonic simulations in a single figure 5.4. For the Platonic codes, the simulation labels start at Platonic $n = 6$. The blue line represents the Platonic quantum codes without subtessellations. Their $Z^{\text{face}}$ parity-check simulations starting at $n = 6$, are labeled faces6, and each additional matrix is denoted by a circle. Their $X^{\text{vertex}}$ parity-check simulations are labeled stars6, and each additional matrix is denoted by a star. Their $Z^{\text{face}}$ and $X^{\text{vertex}}$ average simulation performance is labeled as comb6, and each additional matrix is denoted by a dot. Note that for a given flip probability $f_m$, the combined Ramanujan codes would have a higher rate than the Platonic codes.
| $X^{p=q}$ | distance (snc) | $G^{p/q}$ | $|G|$ | graph edges or encoding qubits |
|-----------|---------------|------------|-------|-----------------------------|
| 13        | 8             | $PGL(2, Z_{13})$ | 2,184 | 6,552                       |
| 17        | 8             | $PSL(2, Z_{17})$ | 2,448 | 4,896                       |
| 29        | 9             | $PGL(2, Z_{29})$ | 12,180 | 36,540                      |
| 37        | 10            | $PGL(2, Z_{37})$ | 50,616 | 151,848                     |
| 41        | 9             | $PSL(2, Z_{41})$ | 34,440 | 103,320                     |
| 53        | 12            | $PGL(2, Z_{53})$ | 148,824 | 446,472                    |

Table 5.1: Table with the distance (shortest non-contractible cycle), underlying group, order of the underlying group, number of graph edges or encoding qubits, for the Ramanujan quantum error-correcting codes.

Figure 5.4.1: Experimental simulation decoding results for the Ramanujan quantum error-correcting LDPC codes. The Y coordinate is the code rate. The X coordinate represents the flip probability $f_m$ at which the probability of decoding block error is $10^{-4}$ (0.9999 threshold). For the Platonic codes, the simulation labels start at Platonic $n = 6$. For the Ramanujan codes, the simulation labels start at $5 - 13$. The smooth curve shown is the Shannon limit, and the dotted curve shown is the Gilbert-Varshamov bound.
Chapter 6

A General Geometric Framework for the Amplitude Damping Channel

In this chapter we present a general geometrical framework to build quantum error-correcting codes for the amplitude-damping channel, ADC. The new geometrical model gives a characterization useful to build amplitude-damping codes which correct multiple amplitude-damping errors. For these codes, the conditions for exact quantum error correction [28] are not satisfied, requiring the more general framework that we present.

The amplitude-damping channel is characterized by the following error operators:

\[
E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\alpha} \end{bmatrix} \quad \text{and} \quad E_1 = \begin{bmatrix} 0 & \sqrt{\alpha} \\ 0 & 0 \end{bmatrix}
\]

Where \( \alpha \) is the probability of energy loss or dissipation. The error operator \( E_1 \) changes \( |1\rangle \) into \( |0\rangle \) with probability \( \alpha \), and eliminates \( |0\rangle \). The error operator \( E_0 \) damps the amplitude of \( |1\rangle \) and leaves \( |0\rangle \) unchanged.

These error operators are specific to the amplitude-damping channel and different
from the standard error operators. Therefore to build error-correcting codes for this noise process requires new tools and theories different from those derived for standard quantum error-correcting schemes. Recent papers address the problems related to adapting error-correcting schemes to the structure of the amplitude-damping error processes. This can be traced back to early work on approximate quantum error-correcting schemes [18].

We use nonadditive quantum error-correcting codes to construct a quantum error-correcting code that corrects for multiple amplitude-damping errors. Nonadditive codes are more general than stabilizer or additive codes, which are the positive joint eigenstate of an abelian subgroup of tensor products of Pauli matrices. Families of nonadditive quantum error-correcting codes for the standard Pauli description of errors have been constructed, which are more optimal than possible with additive codes [40].

In this chapter we provide a general geometric framework for the construction of nonadditive codes that correct for multiple amplitude-damping errors. The geometric framework that we present induces a notion of distance useful to build families of nonadditive quantum error-correcting codes for the amplitude-damping channel.

We construct an 8-qubit code, encoding one qubit and correcting for two amplitude-damping errors. Nine qubits would be required according to the Hamming bound. This code is more optimal than the equivalent stabilizer codes because it violates the usual Hamming bound. Previously [18], a 4-qubit code, encoding one qubit and correcting for one amplitude-damping error, was constructed, whereas 5 qubits would be required according to the Hamming bound for the Pauli description of errors.

6.1 The Quantum Hamming Bound
For a quantum error-correcting code using the Pauli basis of errors: $\sigma_x$, $\sigma_y$ and $\sigma_z$, encoding $k$ qubits into $n$, and correcting up to $t$ errors, the general quantum Hamming Bound is [32]:

$$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n$$

In the particular case when a code encodes one qubit into $n$ correcting for up to one error, the quantum Hamming bound is:

$$2(1 + 3n) \leq 2^n$$

which implies that $n \geq 5$ is necessary.

There is a known 5-qubit stabilizer code meeting the quantum Hamming bound that can correct for one Pauli error [32].

For the case when error-correcting encodes $k$ qubits into $n$, using 2 types of error, and correcting up to $t$ errors, the quantum Hamming Bound is:

$$\sum_{j=0}^{t} \binom{n}{j} 2^j 2^k \leq 2^n$$

And in the particular case when one qubit is encoded into $n$ and corrects up to one error, the quantum Hamming bound is:

$$2(1 + 2n) \leq 2^n$$

which is also satisfied when $n \geq 5$, and but not when $n \leq 4$.

Therefore, the first amplitude-damping error-correcting code constructed is [18]:
\[
|\bar{0}\rangle = \frac{1}{\sqrt{2}} [|0000\rangle + |1111\rangle]
\]
\[
|\bar{1}\rangle = \frac{1}{\sqrt{2}} [|0011\rangle + |1100\rangle]
\] (6.1.1)

This code encodes one qubit and corrects for one amplitude-damping error, violating the quantum Hamming bound for the standard description of Pauli errors for which at least five qubits are required to correct one error.

In addition note that for a code using only 1 type of error encoding \( k \) qubits into \( n \), and correcting up to \( t \) errors, the quantum Hamming Bound is:

\[
\sum_{j=0}^{t} \binom{n}{j} 1^j \cdot 2^k \leq 2^n
\]

which requires that \( n \geq 3 \).

There are a few other examples of individual non-additive quantum codes adapted to the amplitude-damping channel in the literature and a few families with constant distance [20, 38, 37].

Recently families of quantum error-correcting codes correcting for multiple errors for the amplitude-damping channel were first constructed using concatenated codes [16]. They emphasize the difficulties in systematically generalizing previous methods to build them, and the lack of known constructions of amplitude-damping codes correcting multiple amplitude-damping errors.
6.2 General Geometrical Framework

We introduce a general framework useful to build families of amplitude-damping error-correcting codes that correct for multiple amplitude-damping errors. When the four-qubit amplitude damping code [18] was introduced, the method of proof relied on showing that after any single amplitude-damping error, the resulting states were approximately orthogonal.

For a quantum code $C$ to correct all $k^{th}$ order amplitude-damping errors, an element of the superposition of a codeword must be nonzero after any error $e$, where $|e| \leq k$. Furthermore, for any element of the superposition of codewords, we have that $u - e = v - e$ implies $u = v$.

We introduce a notion of distance between two codewords, $c_1$ and $c_2$ in a code $C$, which we call the amplitude damping distance, $d_{ADC}(c_1, c_2)$, for codewords with positive coefficients. We also introduce the notion of amplitude damping distance of a code, $d_{ADC}(C) = k$, as the minimum $k$ such that for all $|e| \leq k$ and for all codewords, $c_i \in C$, $d_{ADC}(c_i, e) > 0$.

6.2.1 Four qubit amplitude-damping error-correcting code example

The four-qubit amplitude-damping error-correcting code given above 6.1.1 can correct for any one amplitude-damping error. The ket elements of $|0\rangle$ and or $|1\rangle$ are positive. From this amplitude-distance framework perspective, it has distance 2, that is, the minimum weight of an error that takes one ket from a given codeword into a ket from another codeword is of order two. Therefore, the code can correct for any 1
amplitude-damping error.

6.2.2 Singlet-state error-detecting code

The special singlet state $|\psi\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$ can detect any one amplitude-damping error because any one weight error will take $|\psi\rangle$ to the ground state $|00\rangle$. This code has amplitude-damping distance 1 from that state, and can therefore detect for any one error.

6.2.3 General singlet-state family of codes

More generally, any singlet state $|\psi\rangle = \frac{1}{\sqrt{2}} (|v\rangle + |\bar{v}\rangle)$, where $\bar{v}$ is the complement of $v$, and where the minimum weight to the corresponding ground state is $d$ will be able to detect any $d$ amplitude-damping errors.

6.3 Orthogonality Framework

More generally, we can take into account the orthogonality relations to create more compact codes. Let $ADC$ be the amplitude damping channel. Let $E_{0,j}$ be the $E_0$ operator previously defined acting on the $j^{th}$ qubit, and similarly let $E_{1,k}$ be the $E_1$ operator acting on the $k^{th}$ qubit.

Denote by $\delta$ a binary vector of length $n$, and denote its sub-indexes by $S$, such that the index entries $i \in S$ are one. Denote by $S_i$ one such index, where $j \in 2^n$, and
such that $|S_i| = k \leq l$.

**Theorem**

A code $C$ corrects all $l$-order errors in the amplitude damping channel iff for all general codewords $u, v \in C$, $\langle u - \delta_{S_i} | v - \delta_{S_j} \rangle = 0$. Furthermore, for each codeword, after the effect of each of the $l$-order errors, a ket of the elements of its superposition must be nonzero.

**Proof.** Let us have two codewords $|w_1\rangle$ and $|w_2\rangle$. Then the effect of the amplitude damping channel up to $l$ errors is:

\[
ADC(|w_1\rangle \langle w_2|) = E_{0,1} E_{0,2} \cdots E_{0,n} |w_1\rangle \langle w_2| E_{0,1}^\dagger E_{0,2}^\dagger \cdots E_{0,n}^\dagger + \sum_{j=1}^{n} \sum_{k\neq j} E_{1,j,k} |w_1\rangle \langle w_2| E_{1,j,k}^\dagger + O(\gamma^2)
\]

Rewrite $E_0$ and $E_1$ as follows $E_0 = (1 - \gamma/4)I + \gamma Z + O(\gamma^2)$ and $E_1 = \frac{\sqrt{\gamma(X + iY)}}{2}$ then
\[ ADC(|w_1\rangle\langle w_2|) = (1 - \gamma/4)^{2n}|w_1\rangle\langle w_2| \]
\[ + \frac{\gamma}{4}(1 - \gamma/4)^{2n-1} \sum_{j=1}^{n} (Z_j|w_1\rangle\langle w_2| + |w_1\rangle\langle w_2|Z_j) \]
\[ + \cdots \]
\[ + \frac{\gamma^{2l}}{4}(1 - \gamma/4)^{2n-2l} \sum_{j=1}^{n} (X + iY)^l|w_1\rangle\langle w_2|(X + iY)^l \]
\[ + O(\gamma^2) \]

Note that terms like \( Z_j|w\rangle \) takes \( |w\rangle \) to a subspace orthogonal to the code.

6.3.1 Eight qubit amplitude-damping code

This 8-qubit amplitude-damping code can encode 1 qubit and correct for 2 errors. Note that in order to correct two errors in an n-qubit code, according to the quantum Hamming bound using the Pauli basis, \( n \geq 9 \). This code uses only 8 qubits:

\[ |0\rangle = \frac{1}{\sqrt{5}} |00000000\rangle + \frac{1}{\sqrt{20}} \sum_c |11110100\rangle + \frac{1}{\sqrt{20}} \sum_c |10111100\rangle \]
\[ |\bar{1}\rangle = \frac{1}{\sqrt{5}} |11111111\rangle + \frac{1}{\sqrt{20}} \sum_c |11010000\rangle - \frac{1}{\sqrt{20}} \sum_c |10110000\rangle \]

Where \( c \) denotes all the cyclic permutations.

Remark. For \( |\psi\rangle = \frac{1}{\sqrt{2}} (a|0\rangle + b|\bar{1}\rangle) \),
\[
E_{0,1}E_{0,2}E_{0,3}E_{0,4}E_{0,5}E_{0,6}E_{0,7}E_{0,8}(\langle \psi \rangle) = \frac{1}{\sqrt{2}} \left[ a\left(\frac{1}{\sqrt{5}}|00000000\rangle + \frac{(1 - \alpha)^{5/2}}{\sqrt{20}} \sum_{\text{cyc}} |11110100\rangle \right) + \right.
\]
\[
+ \frac{(1 - \alpha)^{5/2}}{\sqrt{20}} \sum_{\text{cyc}} |10111100\rangle \right)
\]
\[
+ b\left(\frac{(1 - \alpha)^4}{\sqrt{5}} |11111111\rangle + \frac{(1 - \alpha)^{3/2}}{\sqrt{20}} \sum_{\text{cyc}} |11010000\rangle \right)
\]
\[
- \frac{(1 - \alpha)^{3/2}}{\sqrt{20}} \sum_{\text{cyc}} |10110000\rangle \right]
\]

so that

\[
\langle 0|E_{00000000}^\dagger E_{00000000}^\dagger |0\rangle \neq \langle 1|E_{00000000}^\dagger E_{00000000}^\dagger |1\rangle
\]

and therefore the conditions for exact quantum error correction [28] are not satisfied, requiring the more general framework that we have presented.
6.4 Generalizations

We have shown an example that generalizes the notion of distance for amplitude-damping codes with positive coefficients for the amplitude-damping channel. We have also shown a general orthogonality framework used to construct an error-correcting code that corrects for multiple amplitude-damping errors in a more optimal way than possible with the standard stabilizer quantum error-correcting codes. This geometric distance notion and general orthogonality framework is analogous to distance frameworks used in classical error-correcting codes, which have advanced the analysis of their error-correcting properties, including the study of optimality bounds.
Chapter 7

Conclusions

This thesis answers MacKay's conjecture about the existence of good families of quantum low-density parity-check error-correcting codes with nonzero rate, increasing minimum distance, and good decoding performance. We analyzed their sparsity; proved a logarithmic lower bound on their distance; showed the non-vanishing rate of their $X^{\text{vertex}}$ and $Z^{\text{face}}$ operators and of their average, and showed their performance with experimental simulated decodings using belief propagation.

With respect to the distance of the codes, it is a major open problem in the theory of Riemann surfaces to improve on the logarithmic lower bound of their systoles [26], the continuous analog of the shortest non-contractible cycles of a graph on a 2-manifold. Therefore, it seems unlikely that there exist families of topological quantum error-correcting codes derived from regular algebraic tessellations of 2-manifolds that have provably better than logarithmic distance properties. Nevertheless, it is possible that irregular or random tessellations might yield better short noncontractible distance bounds.

Quantum error-correction is foundational to the development of practical quantum computers. DiVicenzo [15] recently addresses that a promising direction in the
development of quantum computing architectures could be developed with topological surface quantum error-correcting codes [19]. In the first and second chapters, we have presented new constructions of quantum LDPC error-correcting codes derived from sparse tessellations of topological surfaces. Physical implementations of quantum computers using quantum LDPC error-correcting codes would require few sparse local physical interactions. Therefore, the study of quantum LDPC codes can impact the development of scalable quantum computers.

Another promising direction in the experimental development of practical quantum computers is the manipulation of optical photons. For example, qubits can be represented by whether a photon is in one of two optical cavities, or also as wave packets traveling through space in one of several different modes [32].

The amplitude-damping channel describes noise processes due to energy dissipation from a quantum system such as photon in optical cavities, and wave packets traveling through space. In the last chapter, we have introduced a new geometrical framework for the construction of amplitude-damping codes which correct for multiple amplitude-damping errors. Recent work [16] emphasizes the difficulties in systematically generalizing previous methods to build amplitude-damping codes correcting multiple amplitude-damping errors.
Bibliography


