QUANTUM ERROR DETECTION IN BOXES

BELLA FINKEL

Abstract. We review background material relevant to quantum error detection and give lower bounds on the dimension of quantum error-detecting codes in $\mathfrak{su}(2,\mathbb{C}) \oplus \mathfrak{su}(2,\mathbb{C})$-metric spaces.

Contents

1. Introduction

The problem of executing computations reliably in the presence of noise requires a rigorous information theoretic formulation. In the development of classical information theory, the characterization of noise that afflicts messages to be communicated [1] enabled the development of the first error-correcting codes [2, 3]. Computations that rely on uniquely quantum phenomena are subject to errors of a fundamentally different nature than classical information transfer [4, 5, 6], and therefore present a unique and relevant challenge for quantum computation. The development of techniques for fault-tolerant computation [7] and quantum error correction [8, 9, 10, 11] made viable the possibility of achieving successful quantum computation even in the presence of environmental noise. Such techniques inspired the description of quantum error correction in a general framework [12, 13]. This report focuses on the related problem of investigating error-detecting codes for particular systems not composed of qubits.

In error correction and detection, it is invaluable to have a notion of how to quantify the severity with which a message has been afflicted by errors. In classical computation, the Hamming metric provides such a notion [3]. In [14], Kuperberg and Weaver introduce a definition of a quantum metric space which generalizes that

Date: April 5, 2023.

of a classical metric to a non-commutative model. They define a quantum metric to be a $*$-algebra filtration $\{\mathcal{V}_t\}$ on the linear operators $\mathcal{L}(\mathcal{H})$ of a finite dimensional Hilbert space $\mathcal{H}$ with the identity contained in all subspaces $\mathcal{V}_t$ of the filtration. It is possible to construct quantum metric spaces in the sense of [14] from finite-dimensional representations of semisimple Lie algebras. Quantum metric spaces which emerge this way may be referred to as a $\mathfrak{g}$-metric spaces, or metric spaces of Lie type. In this report, we investigate the class of metric spaces where $\mathfrak{g}$ is a direct sum of copies of $\mathfrak{su}(2)$ acting on a tensor product of Hilbert spaces.

In Sections 2 and 3 we introduce the principles of quantum information most relevant to error correction and detection, then offer some background in classical error correction useful to keep in mind when investigating the quantum case. In Section 4 we review the definition of quantum metric spaces given by [14] and discuss the quantum metric space corresponding to the traditional error model of generalized Pauli matrices acting on systems of qubits. We discuss the class of quantum metric spaces of Lie type in Section 5, then review the condition for a quantum code to detect error in Section 6. In Section 7 we discuss the procedure for establishing quantum error-detecting codes for a system experiencing general noise given in [13], which we call the KLV method. We introduce the definition of a maximal super-Tverberg point and state a necessary and sufficient condition for such a point to emerge in commutative error subspaces for irreducible representations of the form $\mathfrak{su}(2) \oplus \mathfrak{su}(2) \circlearrowright \mathcal{H}_n \otimes \mathcal{H}_m$. We give optimal upper bounds on the dimensions of distance-two quantum error-detecting codes for quantum metric spaces constructed from the irreducible representation $\mathfrak{su}(2) \oplus \mathfrak{su}(2) \circlearrowright \mathcal{H}_n \otimes \mathcal{H}_m$ obtained using the KLV method. These can be interpreted as lower bounds on codes in these metric spaces.

2. Basics of quantum information

A quantum computer is one that relies on quantum superposition and interference for its function. The state space of any quantum system is a Hilbert space which may be finite or infinite-dimensional. When a quantum system's state space is finite-dimensional, it is a complex vector space $\mathcal{H}$ equipped with the Hermitian inner product. The state of such a quantum system is a unit vector $|\psi\rangle \in \mathcal{H}$. A single two-state quantum subsystem is the traditional fundamental unit of information in quantum computing. It is known as a qubit, and it is associated with the algebra $M_2(\mathbb{C})$. The state of a qubit has the general form $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. A state is said to be a superposition of the basis vectors $|0\rangle, |1\rangle$ if a and b are both nonzero. A qudit is a generalization of a qubit for a d-dimensional system, and is associated with the algebra $M_d(\mathbb{C})$. A system of qubits can successfully simulate any qudit. Therefore, qudit-based systems have the same computational power as qubit-based systems. Considering qudits rather than qubits is one way to formulate a more general theory of quantum information and error-detecting codes.

Measuring a state changes it to an eigenvector of the associated measurement operator. For this reason, it is said that measurement destroys quantum superposition. (This is why error detection and eavesdropping detection are equivalent in the quantum case.) Since measurement alters quantum states, quantum error correction is less straightforward than classical error correction. To successfully perform quantum error correction, we must restore the affected vector without performing a measurement which reveals the encoded state.

It is inevitable that a physical quantum computer will interact with its environment. Therefore, a quantum computer is properly understood as a subsystem of a larger system which includes the computer together with its environment. We can understand the environment as an auxiliary system which interacts with the computer via measurement, causing decoherence of quantum states. Decoherence is the destruction of information in the quantum computer subsystem that happens when objects which were previously in coherent quantum superpositions entangle with the environment. Denoting the Hilbert space associated with our quantum computer by $\mathcal{H}_{\text{comp}}$ and the Hilbert space associated with its environment by $\mathcal{H}_{\text{env}}$, we can write the computer-environment system by $\mathcal{H}_{comp} \otimes \mathcal{H}_{env}$.[1]

Efforts at achieving fault-tolerant computation strive to increase the probability that computation can be accurately completed even in the presence of error. For real computation to be carried out, there has to be some permissible level of decoherence that won't falsify results. Successful error correction is necessary to achieve fault-tolerant computation.

3. Classical error correction

It is useful to have in mind some classical background for comparison with the quantum case. Let X be a space of messages. A code is a subset $C \subseteq X$ which we choose so that it can detect and correct error. It is useful to equip a space of messages with a metric to classify error.

Definition 3.1 (Metric Space)**.** A metric space (X, d) is a set X possessing a distance function $d : X \times X \to \mathbb{R}$ such that

(1) $d(x, y) = 0 \iff x = y$
(2) $d(x, y) = d(y, x)$
(3) $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality).

In fact, by the following axioms, $d : X \times X \to \mathbb{R}_{\geq 0}$. The metric space most relevant to clasical information theory is Hamming space. In a Hamming space, $X = \{0, 1\}^n$ is the set of bit strings of length n, and distance $d(x, y)$ is defined as the number of bits that differ between the bit strings x and y. In a generalized Hamming space, we have the finite alphabet A and $X := A^n$ is the set of words of length n. Distance is defined as in an ordinary Hamming space.

Let X be a metric space and let $C \subseteq X$ be a code. A message $x \in X$ might be altered to $y \in X$ with probability $p(x, y)$. We want to select a large code C with a small probability of undetected and uncorrected error. An important simplification often applies. If X has a metric such that error is far less likely when distance is greater ($p(x', y') \ll p(x, y)$ when $d(x', y') > d(x, y)$), then choosing C simplifies to guaranteeing a minimum distance $d(C) := \min_{x,y \in C, x \neq y} d(x, y)$ between codewords. We can make the same simplification in the quantum case, where we satisfy ourselves

[1]This is a small example of a general principle in quantum mechanics that all evolution is unitary if our system is sufficiently large. It is a postulate of quantum mechanics that the evolution of a closed system is unitary. When an open system experiences non-unitary evolution, it does so because of interaction with an external system. To treat the interaction as being unitary, we can close the system by taking the tensor product of the two systems to make a composite system. (To contract the system, we instead use the partial trace map to remove a subsystem, a process sometimes called tracing out the subsidiary system.) We can keep taking bigger physical systems until we encompass the entire universe.

with finding an error-detecting code of a certain minimum distance. Say $d = d(C)$ is the minimal distance of C. Then it is possible to detect any error up to distance $s < d$: if something is not a codeword, then it is erroneous. If $d(x, y) \in \mathbb{Z}_{\geq 0}\ \forall x, y$, the detection distance is $d-1$. It follows from the triangle inequality that the error balls of radius r are disjoint for all $r < \frac{d}{2}$, and if the distances are integers the correction distance is $\lfloor \frac{d-1}{2} \rfloor$.

Let $G = \mathrm{Isom}(X)$ be the isometry group of a metric space X. We write the action of G on X as $G \circlearrowright X$. A homogeneous metric space is one where where the isometry group acts transitively on the metric space. When $\mathrm{Isom}(X) \circlearrowright X$ is transitive, X is a single orbit under this action. This case is the more interesting one for error correction in X based on minimum distance sets because the cardinality $|B(x, r)|$ of the radius-r error balls depends only on r and not on x. That is, the placement of the center of the balls does not matter.

4. Quantum metric spaces

"When examining various problems connected with error detecting and correcting codes it is often convenient to introduce a geometric model."
– R. W. Hamming, *Error Detecting and Error Correcting Codes*

Metric spaces serve a fundamental function in classical coding theory. The concept of error distance with respect to errors of the Pauli spin matrices acting on qubits is central in the traditional treatment of quantum error correction. It is natural, therefore, to ask for a definition of a non-commutative metric space which provides us with a means of evaluating how severely a quantum system has been affected by error. The definition of a quantum metric space (also called a W^*-metric space) introduced in [14] is such a generalization. We review some of the concepts used in the definition of a quantum metric space given in [14].

Definition 4.1 ($*$-algebra)**.** A $*$-algebra A is an algebra over $\mathbb{C}$ with the properties

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

for $x, y \in A, \lambda \in \mathbb{C}$.

Definition 4.2 ($*$-algebra filtration)**.** A $*$-algebra filtration on A is a function $d : A \to \mathbb{R}_{\geq 0}$ such that:

(1) $d(xy) \leq d(x) + d(y)$
(2) $d(x + y) \leq \max(d(x), d(y))$
(3) $d(\lambda x) = d(x)$ if $\lambda \neq 0$
(4) $d(x^*) = d(x)$
(5) $d(1) = 0$ (the identity element has degree zero).

Let $\mathcal{H}$ be a finite-dimensional Hilbert space and let $\mathcal{L}(\mathcal{H})$ be the space of bounded linear operators on $\mathcal{H}$. It is helpful to note that the $d \times d$ complex matrices $M(d) \cong \mathcal{L}(\mathcal{H})$, but because we can choose any orthonormal basis for $\mathcal{H}$ we give preference to the notation $\mathcal{L}(\mathcal{H})$. A quantum pseudometric on $\mathcal{L}(\mathcal{H})$ is an algebra filtration $\{\mathcal{V}_t\}$ invariant under the $*$-operation. The filtration $\{\mathcal{V}_t\}$ is of subspaces $\mathcal{V}_t$ with the properties that

(1) $\mathcal{V}_s \subseteq \mathcal{V}_t$ if $s \leq t$ (the subspaces nest)

(2) $\mathcal{V}_s\mathcal{V}_t \subseteq \mathcal{V}_{s+t}$
(3) $\mathcal{V}_t = \mathcal{V}_t^*$
(4) $I \in \mathcal{V}_0$

where the multiplication and $*$ operations acting on subspaces in (2) and (3) are interpreted using set arithmetic and $s, t \in \mathbb{R}$. If we have a quantum pseudometric

$$I \in \mathcal{V}_0 \subseteq \mathcal{V}_1 \subseteq \cdots \subseteq \mathcal{L}(\mathcal{H})$$

on $\mathcal{L}(\mathcal{H})$, then we can interpret it as a quantum metric on $\mathcal{M}$ by setting $\mathcal{M}$ to be the commutant of $\mathcal{V}_0$. The double commutant theorem implies that $\mathcal{M}$ is the commutant of $\mathcal{V}_0$ if and only if $\mathcal{V}_0$ is the commutant of $\mathcal{M}$. When

$$\mathcal{V}_0 = \text{span}\{I\},$$

we must have

$$\mathcal{M} = \mathcal{L}(\mathcal{H})$$

and the metric is considered to be fully quantum.

When t is a nonnegative integer, we can interpret an element $E \in \mathcal{V}_t$ as an error of distance at most t

$$\text{deg}E = \min_{E \in \mathcal{V}_t} t.$$

As is standard, we work under the simplification that for error operators $E, F \in \mathcal{L}(\mathcal{H})$, $\text{deg}E < \text{deg}F$ implies that F is significantly less likely to occur than E.

As a subspace in a quantum metric, $\mathcal{V}_0$ contains the identity matrix and is closed under addition, multiplication, and $*$. Therefore, $\mathcal{V}_0$ is a $*$-subalgebra of $\mathcal{L}(\mathcal{H})$. We can interpret $\mathcal{V}_0$ as the algebra of inconsequential errors–of errors which change only the global phase of a state. When $\mathcal{V}_0$ is as small as possible, we are in the non-degenerate and fully quantum case.

Let us discuss how the severity of errors is classified for n-qubit strings. Call a matrix of the form

$$\sigma_{\vec{a}} := \bigotimes_{i=1}^{n} \sigma_{a_1}^{(1)} \otimes \cdots \otimes \sigma_{a_n}^{(n)}$$

with $\vec{a} = (a_1 \dots a_n) \in \{I, X, Y, Z\}^{\times n}$ a generalized Pauli matrix (or a multi-Pauli operator). The set of multi-Pauli operators form a basis for $\bigotimes_{i=1}^{n} \mathcal{L}(\mathcal{H}_2)$. An error operator of distance t is a multi-Pauli operator with exactly t terms in its tensor product which are not the identity. A filtration can be defined on $\bigotimes_{i=1}^{n} \mathcal{L}(\mathcal{H}_2)$ by defining $\mathcal{V}_t$ to be the span of all multi-Pauli operators of distance less than or equal to t. This filtration is a quantum metric

$$\text{span}\{I\} = \mathcal{V}_0 \subseteq \mathcal{V}_1 \subseteq \cdots \subseteq \mathcal{V}_n = \bigotimes_{i=1}^{n} \mathcal{L}(\mathcal{H}_2)$$

that is appropriately referred to as "quantum Hamming space." Quantum Hamming space is one example of a Lie graph metric.

5. Constructing quantum metric spaces of Lie type

The class of quantum metric spaces of Lie type includes all constructions from a finite dimensional representation $\rho : \mathfrak{g}_{\mathbb{C}} \to \mathcal{L}(\mathcal{H})$ of a complex semisimple Lie algebra $\mathfrak{g}_{\mathbb{C}}$. Our discussion will focus on constructions from representations of the complexification of $\mathfrak{su}(2)$. For a more general review of $\mathfrak{g}$-metric spaces, see [15].

We often want to study the representations of a matrix Lie group G through its Lie algebra $\mathfrak{g}$. In general, the Lie algebra of a matrix Lie group is only real. Therefore, we would like to have a way to associate a complex Lie algebra $\mathfrak{g}_{\mathbb{C}}$ to $\mathfrak{g}$. This is of interest to us because in quantum mechanics, we often have occasion to study the action of the Lie group $SU(2)$. When we study the angular momentum of a quantum system, we are looking for representations where $\mathfrak{su}(2)$ acts on the system's state space. While $\mathfrak{su}(2)$ and $\mathfrak{sl}(2,\mathbb{R})$ are not isomorphic, their respective complexifications $\mathfrak{su}(2)_{\mathbb{C}}$ and $\mathfrak{sl}(2;\mathbb{R})_{\mathbb{C}}$ are both isomorphic to $\mathfrak{sl}(2,\mathbb{C})$. Moreover, it gives us efficient access to the representation theory of the Lie algebra if we are able to work over an algebraically closed field. In order to describe the complexification of a Lie algebra, it helps to first have a definition for the complexification of a real vector space.

Definition 5.1 (Complexification of a vector space)**.** Let V be a vector space. Then the complexification of $\mathfrak{g}$ is denoted $\mathfrak{g}_{\mathbb{C}}$, and is defined to be the space spanned by the linear combinations of the form

$$x_1 + ix_2$$

for $x_1, x_2 \in \mathfrak{g}$ with

$$i(v_1 + iv_2) = -v_2 + iv_1$$

defined to ensure the compatibility of scalar multiplication with field multiplication.

The complex vector space can be defined equivalently as the tensor product $\mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$. Note that $\mathfrak{g}$ is a real subspace of $\mathfrak{g}_{\mathbb{C}}$. This notion, together with the extension of the bracket operation on $\mathfrak{g}$ to that on $\mathfrak{g}_{\mathbb{C}}$, gives us a definition for the complexification of a real Lie algebra.

Proposition 5.2. *Let $\mathfrak{g}$ be a finite-dimensional real Lie algebra with $\mathfrak{g}_{\mathbb{C}}$ its complexification as a vector space. Then the bracket operation on $\mathfrak{g}$ extends uniquely to $\mathfrak{g}_{\mathbb{C}}$ such that $\mathfrak{g}_{\mathbb{C}}$ becomes a complex Lie algebra called the complexification of $\mathfrak{g}$.*

Proof. This proposition can be demonstrated by checking the uniqueness of the extension using the bilinearity of the bracket operation

$$[x_1 + ix_2, y_1 + iy_2] = ([x_1, y_1] - [x_2, y_2]) + i([x_1, y_2] + [x_2, y_1]).$$

This expression demonstrates that the bracket on $\mathfrak{g}_{\mathbb{C}}$ is real bilinear and skew-symmetric. That the bracket is complex linear in the first factor implies its complex linearity in the second factor, since the bracket is real skew-symmetric. It is a straightforward argument from the real case to check that the Jacobi identity holds. □

This abstract definition of the complexification of a Lie algebra follows through for a matrix Lie algebra as we might expect.

Proposition 5.3. *Let $\mathfrak{g} \subset M_d(\mathbb{C})$ be a real Lie algebra such that for all nonzero elements x, the matrix ix is not in $\mathfrak{g}$. Then the abstract complexification $\mathfrak{g}_{\mathbb{C}}$ given by Definition 5.1 is isomorphic to the subset*

$$\{X + iY | X, Y \in \mathfrak{g}\} \subseteq M_d(\mathbb{C}).$$

Proof. The map $\Phi : \mathfrak{g}_{\mathbb{C}} \to M_d(\mathbb{C})$ taking $x + iy \in \mathfrak{g}_{\mathbb{C}}$ to $X + iY \in M_d(\mathbb{C})$ is a homomorphism of Lie algebras. By our assumption that for all nonzero elements x, the matrix ix is not in $\mathfrak{g}$, it is also an isomorphism. □

This proposition justifies the correspondence between the complexification of $\mathfrak{su}(d)$ and the complex special linear Lie algebra

$$\mathfrak{su}(d)_{\mathbb{C}} \cong \mathfrak{sl}(d;\mathbb{C}).$$

That is, the complex linear span of $\mathfrak{su}(d)$ equals that of $\mathfrak{sl}(d;\mathbb{R})$.

We are most interested in quantum metric spaces of Lie type coming from the Lie algebra $\mathfrak{su}(d)$. Let $\mathfrak{g}_{\mathbb{R}}$ be a real semisimple Lie algebra and let $\rho : \mathfrak{g}_{\mathbb{R}} \to \mathcal{L}(\mathcal{H})$ be a linear representation such that $\rho_{\mathfrak{g}}$ is anti-Hermitian. Note that $\rho(\mathfrak{g}_{\mathbb{R}})$ is traceless because $\mathfrak{g}_{\mathbb{R}}$ is semisimple. The representation ρ extends to a representation of the complex Lie algebra $\mathfrak{g}_{\mathbb{C}}$. We can build a quantum metric by taking

$$\begin{aligned}\mathcal{V}_0 &= \operatorname{span}\{I\}\\ \mathcal{V}_1 &= I \oplus \mathfrak{g}_{\mathbb{C}}\\ \mathcal{V}_t &= \mathcal{V}_1^t\end{aligned}$$

where the $\mathcal{V}_t$ are taken to be the linear span of the tensor product of t or fewer errors from $\mathcal{V}_1$. Schur's Lemma implies that if ρ is an irreducible representation of $\mathfrak{g}$, then there exists a t for which $\mathcal{V}_t = \mathcal{L}(\mathcal{H})$.

Consider the real Lie algebra $\mathfrak{su}(2)_{\mathbb{C}}$ of the traceless 2×2 complex anti-Hermitian matrices. The Lie algebra $\mathfrak{su}(2)_{\mathbb{C}}$ has a basis $\{i\sigma_X, i\sigma_Y, i\sigma_Z\}$. The standard basis of $\mathfrak{sl}(2,\mathbb{C})$ ($\mathfrak{sl}(2,\mathbb{C}) \cong \mathfrak{su}(2)_{\mathbb{C}}$) is comprised of the matrices

$$E = \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix},\ F = \begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix},\ H = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

which have commutation relations $[H,E] = 2E$, $[H,F] = -2F$, $[E,F] = H$. The operators E, F, H generate $\mathfrak{su}(2)_{\mathbb{C}}$, and relate to the basis elements of $\mathfrak{su}(2)_{\mathbb{C}}$ given above by

$$E = \frac{\sigma_X + i\sigma_Y}{2}, \quad F = \frac{\sigma_X - i\sigma_Y}{2}, \quad H = \sigma_Z.$$

If we have $\mathcal{V}_0 = \operatorname{span}\{I\}$ and take $\mathcal{V}_1$ to consist of the identity matrix along with the standard basis of $\mathfrak{sl}(2)$

$$\mathcal{V}_1 = \operatorname{span}_{\mathbb{C}}\{I, E, F, H\}$$

then $\mathcal{V}_1 \cong \mathfrak{gl}(2,\mathbb{C})$.

Let $\mathcal{H}$ be a finite-dimensional quantum state space upon which $\mathfrak{su}(2)$ acts irreducibly. It is a fact from the representation theory of $\mathfrak{su}(2)$ that for some non-negative integer n, $\mathcal{H}$ has an orthonormal basis of vectors

$$\{|-n\rangle, |-n+2\rangle, \ldots, |n-2\rangle, |n\rangle\}$$

with simple, explicit forms for the matrices $\rho(E)$, $\rho(F)$ and $\rho(H)$. The action of H on $\mathcal{H}$ is diagonal, and E and F act as raising and lowering operators, respectively, on the weight spaces associated with the basis vectors of $\mathcal{H}$. The $\mathfrak{g}$-module $\mathcal{H}$ has highest weight n and dimension $n+1$.[2]

Note that we can also construct irreducible representations from existing ones. If $\mathfrak{g}_1 \circlearrowright \mathcal{H}_1$ and $\mathfrak{g}_2 \circlearrowright \mathcal{H}_2$ are irreducible representations, then $\mathfrak{g}_1 \oplus \mathfrak{g}_2$, the direct sum of $\mathfrak{g}_1, \mathfrak{g}_2$ as vector spaces has an irreducible representation

$$\mathfrak{g}_1 \oplus \mathfrak{g}_2 \circlearrowright \mathcal{H}_1 \otimes \mathcal{H}_2.$$

[2]An explanation of these statements in terms of the representation theory of $\mathfrak{sl}(2,\mathbb{C})$ can be found in §6.4–7.2 of [16].

In Section 8, we will use this fact to explore error spaces where $\mathfrak{su}(2)^{\oplus n}$ acts on a tensor product of Hilbert spaces of various dimensions.

6. Introduction to quantum error-detecting codes

Let $\mathcal{H}$ be a finite-dimensional Hilbert space. A quantum code $\mathcal{C}$ is a complex subspace of $\mathcal{H}$ defined by an idempotent, self-adjoint projector $P_{\mathcal{C}}$ for which $\text{im}P_{\mathcal{C}} = \mathcal{C}$. We can think of $P_{\mathcal{C}}$ as a boolean that asks if a certain configuration is in the subset and $\text{im}P_{\mathcal{C}}$ as the subset (which is a subspace in these circumstances) of configurations to which the answer is "yes."

Definition 6.1 (Minimum distance)**.** The minimum distance of a code $\mathcal{C}$ is the largest t for which $E \in \mathcal{V}_s$, $s < t$ (equivalently, $\deg E < t$) implies that there exists a linear function $\epsilon : \mathcal{V}_s \to \mathbb{C}$ such that

$$P_{\mathcal{C}} E P_{\mathcal{C}} = \epsilon(E) P_{\mathcal{C}} \ \forall E \in \mathcal{V}_s. \tag{6.2}$$

Equation 6.2 is the general error detection condition. A subspace $\mathcal{C}$ associated with the projection $P_{\mathcal{C}}$ which satisfies the above condition is an error-detecting code. This definition holds for any error space.

We can not expect a quantum process to occur or not to occur in a binary. Since quantum errors are one sort of quantum process, they must in general be expressed in terms of a quantum superposition. An arbitrary error operator is a linear combination of error which is strictly detectable and no error at all

$$E = F + \epsilon(E) I \tag{6.3}$$

where $E \in \mathcal{V}_t$ is the error we want to describe, ϵ is the function introduced in Equation 6.2, $F \in \mathcal{V}_t$ is a specific error which is strictly detected, and I is the identity matrix. In terms of the projector $P_{\mathcal{C}}$, we have the cases where

$$P_{\mathcal{C}} |\psi\rangle = \psi \Leftrightarrow |\psi\rangle \in \mathcal{C}$$

and

$$P_{\mathcal{C}} |\psi\rangle = 0 \Leftrightarrow |\psi\rangle \perp \mathcal{C}.$$

The latter case captures the situation where $P_{\mathcal{C}} E P_{\mathcal{C}} = 0$ and we are guaranteed to have successfully detected the error. We can view the case where $E = I$ as the opposite situation; clearly $IP |\psi\rangle = P |\psi\rangle \in \mathcal{C}$. These two cases act like a basis for a general error operator in the error space.

Equation 6.3 invites the use of the term "slope" as a moniker for the linear function ϵ. The slope is a measure of how much of a particular error is the identity– how much of the error is actually non-error. In order to guarantee the detection of E, we have to subtract the portion of E which is proportional to the identity in the superposition sense. The code $\mathcal{C}$ detects errors only if there is a satisfactory function ϵ for the relevant error space. In the next section, we review a method for constructing quantum error-detecting codes for general noise developed in [13]. In Section 8, we'll employ this method to obtain lower bounds on the size of $\mathfrak{su}(2) \oplus \mathfrak{su}(2)$ error-detecting codes.

7. Realizing Quantum Error-Detecting Codes through Discrete Geometry

A 2000 paper [13] by Knill, Laflamme, and Viola (KLV) introduces an approach to constructing quantum error-detecting codes for a system subject to an arbitrary

space of error. For short, we will refer to this procedure as the KLV method. A central result of [13] concerns the existence of good error-detecting codes for a general error space. Given a Hilbert space $\mathcal{H}$ of dimension N and a set of errors $\mathcal{V}_t$ with dimension D, the KLV method constructs a quantum error-detecting code guaranteed to have dimension at least $\left\lceil \frac{N}{D} \right\rceil \frac{1}{D+1}$.

The KLV method proceeds as follows. Given the state space of a quantum system $\mathcal{H}$ and a space of errors $\mathcal{V}_t$, create a classical intermediate code $\mathcal{B} \subset \mathcal{H}$ for which the error of a desired distance is commutative. In other words, create a d-dimensional classical code $\mathcal{B} = \text{span}\{|\psi_1\rangle, \ldots, |\psi_d\rangle\}$ with orthonormal basis states $|\psi_1\rangle, \ldots, |\psi_d\rangle$ and an error space

$$\mathcal{V}_t = \text{span}\{I, E_1, \ldots, E_k\}, \mathcal{V}_t^* = \mathcal{V}_t$$

satisfying

$$P_{\mathcal{B}} E_\ell P_{\mathcal{B}} = \epsilon(E_\ell) P_{\mathcal{B}} \; \forall l \in [1, k]$$

and for which $P_{\mathcal{B}} E P_{\mathcal{B}}$ commutes with $P_{\mathcal{B}} F P_{\mathcal{B}}$ for all $E, F \in \mathcal{V}_t$. Choosing a basis, we can say that an intermediate code $\mathcal{B}$ is a classical error-detecting code if $P_{\mathcal{B}} E P_{\mathcal{B}}$ is diagonal for all $E \in \mathcal{V}_t$. By arguing from a greedy algorithm, [13] find that classical codes of dimension at least $\left\lceil \frac{N}{D} \right\rceil$ can always be obtained.

Going from the intermediate classical code $\mathcal{B}$ to a quantum error-detecting code $\mathcal{C}$ requires taking a subcode of $\mathcal{B}$ such that an ϵ can be found satisfying Equation 6.2. KLV introduce this as a convex sets problem. Recall that to each $|\psi_m\rangle$ there is an associated linear function ϵ_m, with the vector representation

$$\vec{\epsilon}_m(E) = \begin{bmatrix} \langle\psi_m| E_1 |\psi_m\rangle \\ \vdots \\ \langle\psi_m| E_k |\psi_m\rangle \end{bmatrix}.$$

That is, the ϵ_m act as *weights* for the error space, and we have an associated a weight diagram where the points are the states in $\mathcal{B}$.

To establish the existence of a suitable ϵ, [13] partition the basis states of $\mathcal{B}$ so that the convex closure of the parts is nonempty. For this, [13] invoke Tverberg's theorem [17] to obtain a lower bound on the dimension of a quantum error-detecting code given any quantum system and space of errors.

Theorem 7.1 (Tverberg's theorem)**.** *For any set of* $(d+1)(r-1)+1$ *points in a* d*-dimensional Euclidean space, there exists a partition of the points into* r *subsets such that the intersection of the convex hulls of all of the subsets is nonempty.*

The slope can be taken as any of the points in the convex closure so that the parts form states in the quantum error-detecting code $\mathcal{C}$. States in a subset together are put into a linear combination in $\mathcal{C}$. For this reason, the dimension of $\mathcal{C}$ is equal to the number of parts in this partition.

Since the construction in [13] is for an arbitrary error space, they construct their intermediate classical code via a greedy algorithm. When the error space comes from a Lie algebra, the weight diagram of the error space is exactly that associated with the Lie algebra. In the latter case, we find the abelian subcode $\mathcal{B}$ in the weight diagram as a discrete, classical packing problem–we find a subset of the weight diagram for which no two basis vectors are neighbors within the code distance and take it as our classical intermediate code $\mathcal{B}$. Then, we search for a common slope ϵ in the convex hull of a partition of the states in $\mathcal{B}$. Quantum metric

spaces of Lie type possess additional symmetry not assumed in [13]; therefore, it is often possible to obtain quantum codes larger than those guaranteed by Tverberg's theorem.

8. Error detection in boxes

By "error detection in boxes" we refer to the class of quantum metric spaces constructed from the irreducible representations of the form $\mathfrak{su}(2)^{\oplus k} \circlearrowright \mathcal{H}_{n_1} \otimes \cdots \otimes \mathcal{H}_{n_k}$ where n_i denotes the highest weight of the $\mathfrak{su}(2)$ representation. When $k = 2$, these irreducible representations have weight diagrams which are rectangles; when $k = 3$, the weight diagrams are rectangular prisms; in k dimensions, the weight diagram is an k-dimensional box. Here, we examine the metric spaces constructed from the irreducible representations $\mathfrak{su}(2) \oplus \mathfrak{su}(2) \circlearrowright \mathcal{H}_n \otimes \mathcal{H}_m$ with highest weight n and m, respectively. Given an irreducible representation $\mathcal{H}_n \otimes \mathcal{H}_m$, we state the greatest possible dimension of a distance-two error-detecting code $\mathcal{C}$ constructed using the KLV method.

For $\mathfrak{su}(2) \oplus \mathfrak{su}(2) \circlearrowright \mathcal{H}_n \otimes \mathcal{H}_m$, we have additional symmetry that always lets us construct quantum error-detecting codes that beat the lower bound established by [13]. Tverberg's theorem guarantees that for any set of $(d+1)(r-1)+1$ points in a Euclidean space of dimension d, there exists a partition of the points into r parts such that the convex hull of the parts is nonempty. If there is additional symmetry between the points, it is possible form a partition with more than r parts. Call such a partition a super-Tverberg partition, and the points(s) in the intersection of the convex hulls of the parts a super-Tverberg point. In what follows, we find it useful to introduce a term for a point lying in the intersection of the convex hulls of the parts of a partition in which all parts have size at most two. We call such a point a *maximal super-Tverberg point.* A maximal super-Tverberg point is one which lies at the common intersection of the line segments formed by taking the points in each part as the endpoints of the line segments. The notion of a maximal super-Tverberg point is useful for defining when we have symmetry in $\mathcal{B}$ that allows us to take the greatest possible number of subsets in the partition giving the final code $\mathcal{C}$.

In all that follows, we consider the quantum metric spaces constructed from the irreducible representations $\mathfrak{su}(2) \oplus \mathfrak{su}(2) \circlearrowright \mathcal{H}_n \otimes \mathcal{H}_m$. All of our results concern distance-two codes constructed with the KLV method. It is helpful to have the following fact in mind.

Remark 8.1. Tile $\mathbb{R}^2$ by 1-norm balls with one ball centered at the origin. Any $n \times m$ grid of points from the integer lattice can be taken to represent the weight diagram for $\mathcal{H}_n \otimes \mathcal{H}_m$. Selecting the points in the intermediate code to be the center points of the 1-norm balls forms $\mathcal{B}$ with the optimal dimension. That is, when we choose states in $\mathcal{B}$ in this way, we can always go on to form a quantum error-detecting code of the greatest possible dimension.

When m and n have the same parity, we can always form the optimal KLV construction by taking $\mathcal{B}$ with the largest possible number of states in this pattern and taking the pairs of points which join to form line segments intersecting in the center as the parts in the partition. The largest intermediate code includes $\left\lceil \frac{nm}{2} \right\rceil$ points that can be partitioned into pairs (with the potential addition of one extra maximal super-Tverberg point) yields a final code with dimension $\left\lceil \frac{nm}{4} \right\rceil$. For

$\mathfrak{su}(2) \oplus \mathfrak{su}(2) \circlearrowright \mathcal{H}_{2n} \otimes \mathcal{H}_{2m}$ and $\mathfrak{su}(2) \oplus \mathfrak{su}(2) \circlearrowright \mathcal{H}_{2n+1} \otimes \mathcal{H}_{2m+1}$ if we form a classical intermediate code to detect one error, the best we can do by following the KLV method gives us a code $\mathcal{C}$ with

$$\dim\mathcal{C} = \frac{1}{2}\dim\mathcal{B} = \frac{1}{4}\dim(\mathcal{H}_n \otimes \mathcal{H}_m).$$

(We can only do worse intentionally by creating our intermediate code in a different pattern or choosing larger parts in our partitions.) If we compare the code we get from $\mathfrak{su}(2)\oplus\mathfrak{su}(2) \circlearrowright \mathcal{H}_n\otimes\mathcal{H}_m$ to the code we get from an irreducible representation where one or both of m and n is greater and m and n have the same parity, the dimension of the code is always larger in the latter case. However, if we compare to the code we get from an irreducible representation where one or both of m and n is greater and m and n have opposite parities, we do not necessarily succeed in increasing the dimension of the final code; for example, if we start with $\mathfrak{su}(2) \oplus \mathfrak{su}(2) \circlearrowright \mathcal{H}_n \otimes \mathcal{H}_1$, where n is odd, and then look at $\mathfrak{su}(2) \oplus \mathfrak{su}(2) \circlearrowright \mathcal{H}_{n+1} \otimes \mathcal{H}_1$, we will always only be able to obtain a final code with dimension equal to that in the former case.

For use in the proof of Theorem 8.3, we introduce the following Lemma.

Lemma 8.2. *For all n, m greater than two, the convex hull of all points in the largest distance-two intermediate code $\mathcal{B}$ is one of the three shapes (Figure 5a, Figure 5b, Figure 5c) depending on the parities of m and n.*

Proof. Let the subscripts n, m denote the highest weight of the representation. Begin by examining $\mathcal{H}_3 \otimes \mathcal{H}_3$. The weight diagram and a largest intermediate code for $\mathcal{H}_3 \otimes \mathcal{H}_3$ are shown in Figure 1.

When we examine other values of n and m, we add rows and columns to the weight diagram. Because we are creating the intermediate code of the highest dimension, we are constrained by the checkerboard pattern as we take points in the new rows and columns into the intermediate code. We do not lose generality switching whether we alter n or m; therefore, there are three ways by which we can change n and m

(1) Add to n a nonnegative even integer. Add to m a nonnegative even integer.
(2) Add to n a nonnegative odd integer. Add to m a nonnegative odd integer.
(3) Add to n a nonnegative odd integer. Add to m a nonnegative even integer.

Performing (1) leaves the shape of the convex hull of all points in the intermediate code unchanged, since every other row of the checkerboard has the same pattern. See, for example, the intermediate code for $\mathcal{H}_5 \otimes \mathcal{H}_3$ shown in Figure 2.

Performing (2) gives us a weight diagram with an odd number of points, and so there are two ways we can choose which checkerboard of points becomes our intermediate code, and the dimension of one of these choices is one larger than the other. For the purposes of proving our proposition we need only consider the larger code, but in the spirit of the proof of Theorem 8.3 (and because it is this pattern is useful for generalizing to larger $\mathfrak{su}(2)^{\oplus n} \circlearrowright \mathcal{H}_{n_1} \otimes \cdots \otimes \mathcal{H}_{n_k}$) we display convex hull of the points in the code we get for either choice in Figure 3.

Consider finally what happens to the weight diagram of Figure 1 in (3). Adding to m a nonnegative even integer does not alter the shape of the convex hull of $\mathcal{B}$ from that of Figure 1. Adding an odd integer to n causes the rightmost column in the resulting weight diagram to be offset from that in 1, giving the shape in Figure 5c.

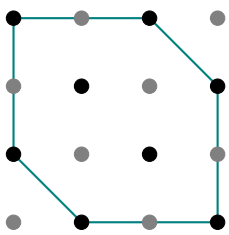


FIGURE 1. The weight diagram for $\mathcal{H}_3 \otimes \mathcal{H}_3$. Points corresponding to states in $\mathcal{B}$ are shown in black. The convex hull of the points in the intermediate code is drawn in teal.

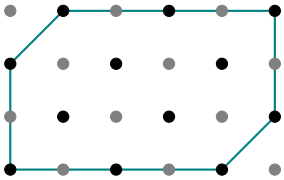
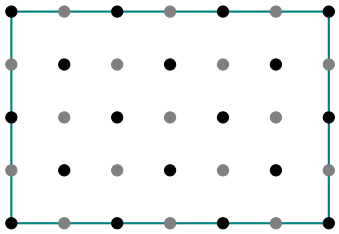
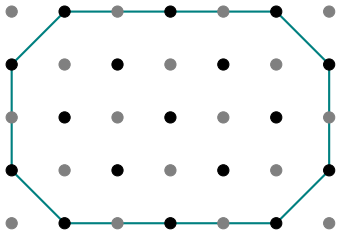


FIGURE 2. The weight diagram $\mathcal{H}_5 \otimes \mathcal{H}_3$. Points corresponding to states in $\mathcal{B}$ are shown in black. The convex hull of the points in the intermediate code is drawn in teal.



(A) The weight diagram for $\mathcal{H}_6 \otimes \mathcal{H}_4$. Points corresponding to states in $\mathcal{B}$ are shown in black. The convex hull of the points in the intermediate code is drawn in teal.



(B) The weight diagram for $\mathcal{H}_6 \otimes \mathcal{H}_4$ with the smaller $\mathcal{B}$ taken. The convex hull of the points in the intermediate code is drawn in teal. Although this $\mathcal{B}$ is smaller, it is possible to obtain a final code $\mathcal{C}$ of the same dimension taking this $\mathcal{B}$ as if we took the $\mathcal{B}$ shown in 3a.

FIGURE 3. Weight diagrams for $\mathcal{H}_6 \otimes \mathcal{H}_4$ with the two $\mathcal{B}$ from which we can obtain a $\mathcal{C}$ of greatest possible dimension.

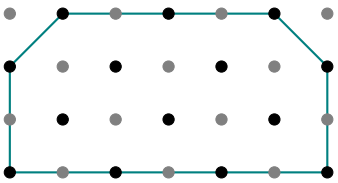
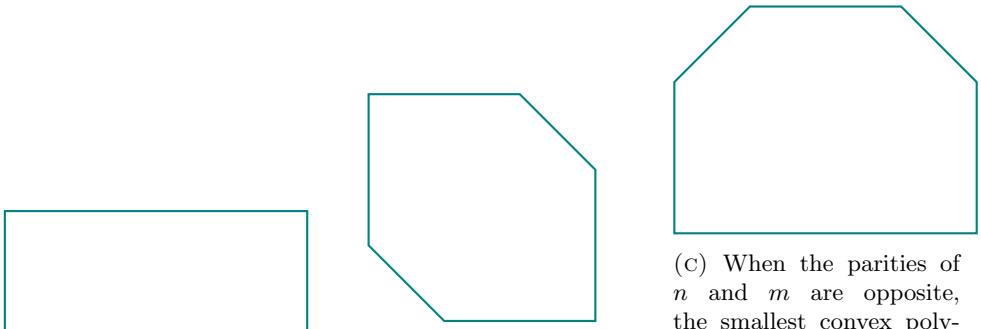


FIGURE 4. The largest intermediate code for $\mathcal{H}_6 \otimes \mathcal{H}_3$. Points in $\mathcal{B}$ are shown in black, and points in the weight diagram but outside of $\mathcal{B}$ are shown in gray. The convex hull of the points in the intermediate code is drawn in teal.



(A) When n and m are both odd, the smallest convex polygon containing all points in the $\mathcal{B}$ of maximum dimension is an $n \times m$ rectangle.

(B) When n and m are both even, the smallest convex polygon containing all points in the $\mathcal{B}$ of maximum dimension is an irregular hexagon. The top and bottom horizontal sides have length $n-1$ and the left and right vertical sides have length $m-1$.

(C) When the parities of n and m are opposite, the smallest convex polygon containing all points in the $\mathcal{B}$ of maximum dimension is a trapezoid with the length of the top horizontal side equal to $n-2$, the length of the bottom horizontal side equal to n, and the length of the left and right vertical sides equal to $m-1$.

FIGURE 5. The three shapes that the convex hull of $\mathcal{B}$ may take on.

□

Figure 2, Figures 3a and 3b, and Figure 4 give examples of $\mathcal{B}$ for specific choices of m and n. The convex hull of the points in the largest distance-two intermediate code for $n, m \leq 2$ is just a matter of reducing sides in the shapes 5*a*, 5*b*, 5c to a point.

Theorem 8.3. *There exists a partition of a distance-two intermediate classical code $\mathcal{B}$ of maximal dimension in a weight diagram of $\mathcal{H}_n \otimes \mathcal{H}_m$ which produces a maximal super-Tverberg point if and only if m and n have the same parity.*

Proof. Given a point x in $\mathbb{R}^2$, all line segments intersecting x are described by revolving a point y around x by 180° to get a point z, then connecting y and z. Given a point y in a set of points in $\mathbb{R}^2$, we can construct a line segment through x with endpoint y if and only if there exists a point z in the set which is the image of y under a 180° revolution about x. There exists a maximal super-Tverberg point inside of the convex hull of $\mathcal{B}$ if and only if the image of each point $y \in \mathcal{B}$ under a 180° rotation is also in $\mathcal{B}$.

If m and n have the same parity, then the convex polygon enclosing all points in the intermediate code has either the shape 5a or 5b. Notice that 5a and 5b are invariant under 180° rotations. If m and n have the same parity, then the set of points in $\mathcal{B}$ is invariant under 180° revolutions about the center. Taking the endpoints of the line segments constructed via these revolutions as the parts of the partition forming $\mathcal{C}$ gives a maximal super-Tverberg point.

If m and n have opposite parities, then convex hull of the points in the intermediate code has the shape 5c. Notice that 5c is not invariant under 180° rotations.

If m and n have opposite parities, then for all candidate maximal super-Tverberg points x in the convex hull of $\mathcal{B}$ there exists a point $y \in \mathcal{B}$ such that the image of y under 180° revolution about x is not in $\mathcal{B}$.

□

For distance-two error-detecting codes, the $\mathcal{B}$ in which we can always build a maximal super-Tverberg point are precisely those for which the convex hull of the points in $\mathcal{B}$ is invariant under 180° rotations.

Theorem 8.4 (Bounds on code dimensions)**.** *Let n and m denote the dimensions of the representations $\mathcal{H}_n$ and $\mathcal{H}_m$. There exist distance-two error-detecting codes $\mathcal{C}$ for $\mathcal{H}_n \otimes \mathcal{H}_m$ of dimension at least $\lceil \frac{nm}{4} \rceil$ when n and m have the same parity and $\lceil \frac{n(m-1)}{4} \rceil$ when n and m have opposite parities.*

Proof. Let n and m denote the dimensions of the representations $\mathcal{H}_n$ and $\mathcal{H}_m$. This differs from the notation used previously, where n and m were used for the highest weights of the representations $\mathcal{H}_n$ and $\mathcal{H}_m$.

We use the construction given by the KLV method to obtain these lower bounds. If n and m are both odd or both even, then the $\mathcal{B}$ of the largest dimension has $\dim\mathcal{B} = \lceil \frac{nm}{2} \rceil$ and $\dim\mathcal{C} = \lceil \frac{nm}{4} \rceil$ If n and m have opposite parities, then the largest possible $\mathcal{C}$ has $\dim\mathcal{C} = \lceil \frac{n(m-1)}{4} \rceil$.

The case where n and m are both even, or where n and m are both odd and we take the larger intermediate code, gives us $\dim\mathcal{B} = \lceil \frac{nm}{2} \rceil$ points which can be paired to form a partition consisting of parts of size two. If n and m are both odd and we take the smaller intermediate code, then there are $\dim\mathcal{B} = \lfloor \frac{nm}{2} \rfloor - 1$ points which can be paired to form $\lfloor \frac{nm}{4} \rfloor$ parts of size two and one and one point in $\mathcal{B}$ lying on the maximal super-Tverberg point which can be put into a part by itself. Thus, in both cases we achieve $\dim\mathcal{C} = \lceil \frac{nm}{4} \rceil$.

If n and m have opposite parities, then for all points x in the convex hull of $\mathcal{B}$ there is at least one state in $\mathcal{B}$ which is not mapped to a point in the code when rotated about x by 180°. If a point is not mapped to another point in the code under 180° rotation, then it must necessarily belong to a part containing three or more points or form a line segment with the super-Tverberg point. (Points which are mapped to another point in the code under 180° rotation can belong to a part containing three or more points accidentally, but they do not do so necessarily.) The number of points not mapped to another point in the code under 180° rotation is equal to the number of points which do not add to the dimension of the final code. The points which are not mapped to another point in the code under 180° rotation are exactly the points lying on the side of the trapezoid 5c. Therefore, the maximum possible dimension of $\mathcal{C}$ for when n and m have opposite parities is the dimension of $\mathcal{C}$ for $\mathcal{H}_n \otimes \mathcal{H}_{m-1}$, that is, $\dim\mathcal{C} = \lceil \frac{n(m-1)}{4} \rceil$.

□

9. Conclusions

In [13], the authors comment that one goal in the process of constructing good quantum error-correcting codes is to maximize the dimension of the intermediate minimum-distance classical code. Tverberg's theorem provides the conditions under which increasing the dimension of $\mathcal{B}$ increases the lower bound on the dimension

of the final code $\mathcal{C}$ for general noise. Theorem 8.4 provides these conditions for $\mathfrak{su}(2,\mathbb{C}) \oplus \mathfrak{su}(2,\mathbb{C})$-metric spaces for distance-two error-detecting codes.

When m and n have opposite parities, there are often multiple partitions yielding a code of dimension given in Theorem 8.4. While not obviously relevant for discerning code dimensions, it is an interesting problem to determine when an optimal partition is unique and find an algorithm for obtaining the optimal partitions exhaustively.

The KLV method has been shown to be sub-optimal for constructing quantum error-detecting codes in $\mathfrak{su}(2)$-metric spaces (Rui Okada, personal communication). The question of whether there are code constructions which give better lower bounds than those of Theorem 8.4 deserves to be investigated.

Acknowledgments

I thank Greg Kuperberg for his mentorship of this REU project and for giving his time to discuss and criticize this work. I am grateful to Sanchayan Dutta and Rui Okada for offering us their time and expertise and to fellow participants Yuanyuan Shen, Ian Shors, Jonathan Webb, and Ruochuan Xu. Many thanks go to Javier Arsuaga and Greg Kuperberg for their work organizing the UC Davis Mathematics REU program.

References

[1] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948.
[2] Golay M. J. E. Notes on digital coding. *Proc. IEEE*, 37:657, 1949.
[3] R. W. Hamming. Error detecting and error correcting codes. *The Bell System Technical Journal*, 29(2):147–160, 1950.
[4] Rolf Landauer. Is quantum mechanics useful? *Philosophical Transactions: Physical Sciences and Engineering*, 353(1703):367–376, 1995.
[5] W. G. Unruh. Maintaining coherence in quantum computers. , 51(2):992–997, February 1995.
[6] I. L. Chuang, R. Laflamme, P. W. Shor, and W. H. Zurek. Quantum Computers, Factoring, and Decoherence. *Science*, 270(5242):1633–1635, December 1995.
[7] Peter W. Shor. Fault-tolerant quantum computation. *IEEE Computer Society Press*, pages 56–65, May 1996.
[8] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, Oct 1995.
[9] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.
[10] Artur Ekert and Chiara Macchiavello. Quantum error correction for communication. *Phys. Rev. Lett.*, 77:2585–2588, Sep 1996.
[11] Andrew Steane. Multiple-Particle Interference and Quantum Error Correction. *Proceedings of the Royal Society of London Series A*, 452(1954):2551–2577, November 1996.
[12] Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Phys. Rev. A*, 55:900–911, Feb 1997.
[13] Emanuel Knill, Raymond Laflamme, and Lorenza Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84:2525–2528, Mar 2000.
[14] G. Kuperberg and N. Weaver. *A von Neumann Algebra Approach to Quantum Metrics/Quantum Relations*. Memoirs of the American Mathematical Society. American Mathematical Society, 2012.
[15] Christopher Bumgardner. Codes in W-metric Spaces: Theory and Examples. 2012.
[16] James Humphreys. *Introduction to Lie Algebras and Representation Theory*. Graduate Texts in Mathematics. Springer New York, 1994.
[17] H. Tverberg. A Generalization of Radon's Theorem. *Journal of the London Mathematical Society*, s1-41(1):123–128, 01 1966.