CARLETON UNIVERSITY

SCHOOL OF
MATHEMATICS AND STATISTICS

HONOURS PROJECT

TITLE: Quantum Error-Correcting Codes

AUTHOR: Alexandre Conlon

SUPERVISOR: Jason Crann

DATE: December 19, 2018

QUANTUM ERROR-CORRECTING CODES

ALEXANDRE CONLON

Abstract. This paper is an introduction to quantum error-correcting codes. It begins by laying the mathematical framework with which it then develops fundamental concepts in quantum information theory. Following this, it proves important results to the study of quantum error correction. The discussion then centres on a paper by Calderbank et al. [1], which presents a geometric formalism to produce quantum error-correcting codes via a group theoretic framework. Finally, the paper demonstrates that quantum error correcting codes can be constructed from classical error-correcting codes and inherit a portion of their error-correcting properties.

1. Introduction

Quantum physics is renowned for its property of wave-particle duality, famously demonstrated by the *double slit* experiment where it shows that observing (interacting with) a particle which exhibits a wave-like behaviour will induce a particle-like behaviour in the particle immediately after the observation (interaction).

Quantum computers work by exploiting the wave-like behaviour of particles. However, this wave-like behaviour is subject to involuntary observations (interactions) by its environment during computations which may cause errors. In fact, this is a major hurdle in the construction of a reasonably sized quantum computer. So far, we have only managed to construct quantum computers which are small enough to efficiently model classical computers. This motivates the study quantum error correction so that we may one day build a larger quantum computer which can out perform our current classical ones.

We begin by covering the mathematical concepts we require in order to introduce basic ideas in quantum theory, such as *quantum states* and *entanglement*. We assume the reader is familiar with elementary linear algebra and group theory, however we assume no prior knowledge of quantum theory. We then present concepts of quantum information theory, such as the *qubit* and *quantum channels*. Next, we focus our attention to quantum codes and discuss the conditions in which errors are correctable on quantum codes. Following this, we describe a geometric formalism for producing quantum codes, and we show that quantum error-correcting codes can be built from classical error-correcting codes. Finally, we present two examples of quantum error-correcting codes, the first of which is constructed from a classical error-correcting code, and the second is the *five qubit* code.

2. Mathematical Preliminaries

Definition 2.1 (Trace)**.** The *trace* of an $n \times n$ matrix A is the sum of its diagonal entries $\{A_{ii}\}_{i=1}^{n}$, and is denoted

$$tr(A) \coloneqq \sum_{i=1}^{n} A_{ii}.$$

Definition 2.2 (Sesquilinear Inner-Product)**.** For a finite-dimentional complex vector space H, the function $\langle \cdot, \cdot \rangle : H \times H \to \mathbb{C}$ is a *sesquilinear inner-product* over H if

i) $\langle \psi + \phi, \psi' + \phi' \rangle = \langle \psi, \psi' \rangle + \langle \psi, \phi' \rangle + \langle \phi, \psi' \rangle + \langle \phi, \phi' \rangle$
ii) $\langle \alpha\psi, \beta\phi \rangle = \bar{\alpha}\beta \langle \psi, \phi \rangle$

For all $\psi, \phi, \psi', \phi' \in H$ and for all $\alpha, \beta \in \mathbb{C}$, where $\bar{\alpha}$ is the complex conjugate of α.

Any sesquilinear inner product on H induces a norm via $\|\psi\| = \sqrt{\langle \psi, \psi \rangle}$.

Definition 2.3 (Hilbert space)**.** A *Hilbert space* is a finite-dimensional vector space H equipped with a sesquilinear inner-product.

For Hilbert spaces H, K, let $\langle \cdot, \cdot \rangle_H : H \times H \to \mathbb{C}$ and $\langle \cdot, \cdot \rangle_K : K \times K \to \mathbb{C}$ be the inner products over H and K respectively, and let $\mathcal{L}(H, K)$ denote the space of linear maps $A : H \to K$. The *adjoint* of an element $A \in \mathcal{L}(H, K)$ is the unique operator $A^* \in \mathcal{L}(K, H)$ satisfying

$$\langle \phi, A^*\psi \rangle_H = \langle A\phi, \psi \rangle_K, \text{ for every } \phi \in H, \psi \in K.$$

When $H = K$, an operator $A \in \mathcal{L}(H) \coloneqq \mathcal{L}(H, H)$ is *self-adjoint* if $A = A^*$, and *normal* if $AA^* = A^*A$.

Definition 2.4 (Positive operator)**.** Let H be a Hilbert space. Then $A : H \to H$ is a *positive operator* if $\langle \psi, A\psi \rangle \geq 0$, for all $\psi \in H$.

Definition 2.5 (Conjugate linear)**.** Let H and K be Hilbert spaces. Then the map $A : H \to K$ is *conjugate linear* if

$$A(\lambda\psi + \phi) = \bar{\lambda}A(\psi) + A(\phi)$$

for all $\lambda \in \mathbb{C}$ and $\psi, \phi \in H$.

Throughout this paper, we are interested in the structure preserving maps between Hilbert spaces called unitary maps (Hilbert-space-isomorphisms).

Definition 2.6 (Unitary map)**.** Let H and K be Hilbert spaces. Then any bijection $U \in \mathcal{L}(H, K)$, which preserves the inner product is a *unitary map*.

We observe that, $U \in \mathcal{L}(H, K)$ is unitary if and only if for all $\psi, \phi \in H$:

$$\langle U\psi, U\phi \rangle_K = \langle U^*U\psi, \phi \rangle_K = \langle \psi, \phi \rangle_H.$$

Definition 2.7 (Orthogonal Complement)**.** Let $M \subseteq H$ be a subspace of H. Then the set

$$M^\perp \coloneqq \{\psi \in H \mid \text{ for all } \phi \in M : \langle \phi, \psi \rangle = 0\}$$

is the orthogonal complement of M in H. Then $M^\perp$ is a subspace such that

$$H = M \oplus M^\perp.$$

Definition 2.8 (Orthogonal Projection)**.** Let H be a Hilbert space. A *projection* is an operator $P \in \mathcal{L}(H)$ such that $P = P^2 = P^*$.

If $P \in \mathcal{L}(H)$ is a projection, then $(PH)^\perp = (1 - P)H$, so the projection $(1 - P)$ is the *orthogonal complement* of P. As above, it then follows that

$$H = PH \oplus (1 - P)H.$$

Moreover, if $\{\psi_i\}_{i=1}^k$ is an orthonormal basis of $M = PH$ then

$$P\phi = \sum_{i=1}^{k} \langle \psi_i, \phi \rangle \psi_i, \;\; \phi \in H.$$

Definition 2.9 (Spectrum)**.** The set of eigenvalues $\{\lambda_1, \lambda_2, ..., \lambda_n\}$ of an operator $A \in \mathcal{L}(H)$ is the *spectrum* of A, denoted $\sigma(A)$.

Given a normal matrix A and a function $f : \sigma(A) \to \mathbb{C}$, it is possible to make sense of $f(A)$. Let $A = \sum_\lambda \lambda P_\lambda$ be the spectral decomposition of the normal matrix A. Then define

$$f(A) \coloneqq \sum_\lambda f(\lambda) P_\lambda.$$

We observe that when f is a polynomial,

$$f(z) = a_0 + a_1 z + \cdots + a_n z^n,$$

then

$$f(A) = a_0 + a_1 A + \cdots + a_n A^n.$$

We can use this idea to define the square root of a positive operator. Suppose we have a positive operator E with spectral decomposition $E = \sum_\lambda \lambda P_\lambda$, then we may define

$$\sqrt{E} = \sum_\lambda \sqrt{\lambda} P_\lambda,$$

as each eigenvalue $\lambda \geq 0$.

Example 2.10. Suppose we have an operator A where

$$A = diag(\lambda_1, ..., \lambda_n) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix},$$

with $\lambda_i \geq 0$, then

$$\sqrt{A} = diag(\sqrt{\lambda}_1, ..., \sqrt{\lambda}_n) = \begin{pmatrix} \sqrt{\lambda}_1 & & 0 \\ & \ddots & \\ 0 & & \sqrt{\lambda}_n \end{pmatrix}.$$

Remark 2.11. An operator A is positive if and only if there exists B such that $A = B^*B$. Then $A^* = \left(B^*B\right)^* = B^*B = A$, thus positive implies self-adjoint.

In this case, one may take $B = \sqrt{A}$, since

$$B^*B = \sqrt{A^*}\sqrt{A} = \sqrt{A}\sqrt{A} = A.$$

Proposition 2.12 (Polar Decomposition)**.** *Let $A \in \mathcal{L}(H)$, then there exists a unitary $U \in \mathcal{L}(H)$ such that*

$$A = U\sqrt{A^*A}.$$

3. Tensor Products

3.1. **Tensor Product of Hilbert Spaces.** For Hilbert spaces H_1 and H_2, consider the set, T, of all finite linear combinations of elements in $H_1 \times H_2$, defined by

$$T \coloneqq \Big\{ \sum_{j=1}^{J} a_j(\psi_j, \phi_j) \mid a_1, ..., a_J \in \mathbb{C}, \psi_j \in H_1, \phi_j \in H_2 \Big\},$$

and the equivalence relation $\sim$ on T such that

$$\begin{aligned} &1)(\psi, \phi_1 + \phi_2) \sim (\psi, \phi_1) + (\psi, \phi_2), \\ &2)(\psi_1 + \psi_1, \phi_2) \sim (\psi_1, \phi) + (\psi_2, \phi), \\ &3)\lambda(\psi, \phi) \sim (\lambda\psi, \phi) \sim (\psi, \lambda\phi), \quad \text{for all } \lambda \in \mathbb{C}. \end{aligned}$$

Then tensor products between Hilbert spaces are defined as follows.

Definition 3.1 (Tensor Product Space)**.** The tensor product of Hilbert spaces H_1 and H_2 is defined as

$$H_1 \otimes H_2 \coloneqq T/\sim$$

where

$$\Big\langle \sum_{j=1}^{J} c_j(\psi_j, \phi_j) \, , \, \sum_{k=1}^{K} d_k(\psi'_k, \phi'_k) \Big\rangle_{H_1 \otimes H_2} \coloneqq \sum_{j=1}^{J} \sum_{k=1}^{K} \bar{c_j} d_k \langle \psi_j, \psi'_k \rangle_{H_1} \langle \phi_j, \psi'_k \rangle_{H_2}$$

with respect to which the closure is taken. So, we get the *tensor product space*

$$\Big(H_1 \otimes H_2 \, , \, \langle \cdot, \cdot \rangle \Big).$$

3.2. **Tensor Product of Vectors.** In the subsection above, we defined a tensor product space as the space of equivalence classes corresponding to $\sim$. Perhaps unsurprisingly, we define the tensor product between $\psi \in H_1$ and $\phi \in H_2$ by their corresponding equivalence class.

Definition 3.2 (Tensor Product of Vectors)**.** The tensor product between vectors is defined by

$$\psi \otimes \phi \coloneqq [(\psi, \phi)]_{\sim} \in H_1 \otimes H_2.$$

Such a tensor is a *simple tensor*. The inner product on simple tensors in $H_1 \otimes H_2$ is simply defined by

$$\langle \psi \otimes \phi, \, \psi' \otimes \phi' \rangle_{H_1 \otimes H_2} \coloneqq \langle \psi, \psi' \rangle_{H_1} \cdot \langle \phi, \phi' \rangle_{H_2}$$

Any element of $H_1 \otimes H_2$ is therefore of the form $\sum_{i=1}^{n} c_i \psi_i \otimes \phi_i$.

To gain a feel for the mechanics of the tensor product we introduce what is known as the *Kronecker product*. It offers an explicit representation of the tensor product.

Definition 3.3. Let ψ be an element of the n-dimensional Hilbert space $\mathbb{C}^n$ and ϕ be an element of an m-dimensional Hilbert space $\mathbb{C}^m$. Then the *Kronecker product*, which

represents the tensor product, is defined by

$$\psi \otimes \phi = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_n \end{pmatrix} \otimes \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_m \end{pmatrix} = \begin{pmatrix} \psi_1 \cdot \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_m \end{pmatrix} \\ \vdots \\ \psi_n \cdot \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_m \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \psi_1 \cdot \phi_1 \\ \vdots \\ \psi_1 \cdot \phi_m \\ \vdots \\ \vdots \\ \psi_n \cdot \phi_1 \\ \vdots \\ \psi_n \cdot \phi_m \end{pmatrix}.$$

This explicit view given by the Kronecker product can help to determine useful properties of the tensor product.

Theorem 3.4. *Let H_1, H_2 be n- and m-dimensional Hilbert spaces, respectively. Let $\{e_i\}_{i=1}^n$ and $\{f_i\}_{i=1}^m$ be orthonormal basis for H_1 and H_2, respectively. Then*

(1) *$\{e_i \otimes f_j\}_{i,j=1}^{n,m}$ is an orthonormal basis for $H_1 \otimes H_2$;*

(2) *$dim(H_1 \otimes H_2) = dim(H_1) \cdot dim(H_2)$;*

(3) $H_1 \otimes H_2 \coloneqq \Big\{ \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} e_i \otimes f_j \mid a_{ij} \in \mathbb{C} \Big\}$.

Remark 3.5. Some practical rules for tensor products, which follow directly from $\sim$:

(1) $(\psi + a\phi) \otimes (\psi' + b\phi') = \psi \otimes \psi' + b\psi \otimes \phi' + a\phi \otimes \psi' + ab\phi \otimes \phi'$
where $\psi, \phi \in H_1$, $\psi', \phi' \in H_2$ and $a, b \in \mathbb{C}$;

(2) for all $\Psi \in H_1 \otimes H_2$, there is an $a_{ij} \in \mathbb{C}$ such that $\Psi \coloneqq \sum_{i,j} a_{ij} e_i \otimes f_j$
where $\{e_i\}_{i=1}^n$ and $\{f_i\}_{i=1}^m$ are orthonormal basies for H_1 and H_2, respectively.

3.3. **Tensor Product of Operators.** So far we have seen tensor products between Hilbert spaces, $H_1 \otimes H_2$, and tensor products between vectors, $\psi \otimes \phi$. We now look at tensor products between linear maps A and B, which we denote $A \otimes B$.

Definition 3.6 (Tensor Product of Linear Operators)**.** Let $A : H_1 \to H_1$ and $B : H_2 \to H_2$ be linear operators. Then the tensor product $A \otimes B$ is the unique linear operator

$$A \otimes B : \ H_1 \otimes H_2 \to H_1 \otimes H_2$$

satisfying

$$(A \otimes B)(\psi \otimes \phi) \coloneqq A\psi \otimes B\phi, \ \text{ for all } \psi \in H_1, \phi \in H_2.$$

Theorem 3.7. *If A, B are self-adjoint operators, then $A \otimes B$ is a self-adjoint operator.*

4. Dirac Notation

We begin by providing a result which motivates and justifies the use of Dirac notation. Consider $\psi \in H$. Define a linear map

$$\begin{aligned} T_\psi : H &\to \mathbb{C} \\ \phi &\mapsto \langle \psi, \phi \rangle. \end{aligned}$$

This is linear since for $a \in \mathbb{C}$, and $\xi, \eta \in H$ we have

$$\begin{aligned} T_\psi(a\xi + \eta) &= \langle \psi,\ a\xi + \eta \rangle \\ &= a\langle \psi, \xi \rangle + \langle \psi, \eta \rangle \\ &= aT_\psi(\xi) + T_\psi(\eta). \end{aligned}$$

Moreover,

$$\| T_\psi \|_\infty \coloneqq \sup_{\phi \in H} \frac{|T_\psi(\phi)|}{\| \phi \|} = \sup_{\phi \in H} \frac{|\langle \psi, \phi \rangle|}{\| \phi \|} \leq \sup_{\phi \in H} \frac{\| \psi \| \cdot \| \phi \|}{\| \phi \|} = \| \psi \|,$$

where the last inequality holds by Cauchy-Schwartz, and

$$\left| T_\psi \left(\frac{\psi}{\|\psi\|} \right) \right| = \frac{\psi}{\|\psi\|} |T_\psi(\psi)| = \frac{\psi}{\|\psi\|} |\langle \psi, \psi \rangle| = \|\psi\|$$

implies

$$\|T_\psi\|_\infty \geq \|\psi\|.$$

Thus, $\|T_\psi\|_\infty = \|\psi\|$.

Theorem 4.1. *Every $T \in \mathcal{L}(H, \mathbb{C})$ can be uniquely written as*

$$T = T_\psi.$$

Proof. If $T = 0_{\mathcal{L}(H,\mathbb{C})}$, then take $\psi = 0_H$, and we are done. If $T \neq 0_{\mathcal{L}(H,\mathbb{C})}$, then $ker(T)$ is a proper linear subspace of H, and

$$H = ker(T) \oplus ker(T)^\perp,$$

with $ker(T)^\perp \neq \{0\}$. Then we may pick some $\xi \in ker(T)^\perp$ such that $\xi \neq 0_H$, and without loss of generality we may assume $\|\xi\| = 1$. Take $\psi = \overline{T(\xi)}\xi \in ker(T)^\perp \subseteq H$, and let $\eta \in H$. Then,

$$\begin{aligned} T_\psi(\eta) - T(\eta) &= \langle \psi,\ \eta \rangle - T(\eta)\|\xi\|^2 \\ &= \langle \overline{T(\xi)}\xi,\ \eta \rangle - T(\eta)\langle \xi,\ \xi \rangle \\ &= \langle \xi,\ T(\xi)\eta \rangle - \langle \xi,\ T(\eta)\xi \rangle \\ &= \langle \xi,\ T(\xi)\eta - T(\eta)\xi \rangle. \end{aligned}$$

Then we observe that

$$T\Big(T(\xi)\eta - T(\eta)\xi\Big) = T(\xi)T(\eta) - T(\eta)T(\xi) = 0$$

implying that

$$T(\xi)\eta - T(\eta)\xi \in ker(T),$$

and since $\xi \in ker(T)^\perp$, then

$$T_\psi(\eta) - T(\eta) = \langle \xi,\ T(\xi)\eta - T(\eta)\xi \rangle = 0.$$

Hence, for $T \in \mathcal{L}(H, \mathbb{C})$, there exists $\psi \in H$ such that $T_\psi = T$. Now we show that ψ is unique.

Let ψ_1, ψ_2 be two such constructed vectors so that

$$T_{\psi_1} = T = T_{\psi_2}.$$

Then, for all $\eta \in H$

$$\begin{aligned} 0 = T_{\psi_1} - T_{\psi_2} &= \langle \psi_1,\, \eta \rangle - \langle \psi_2,\, \eta \rangle \\ &= \langle \psi_1 - \psi_2,\, \eta \rangle \end{aligned}$$

and thus,

$$\psi_1 = \psi_2.$$

Hence, for every $T \in \mathcal{L}(H, \mathbb{C})$ there exists a unique $\psi \in H$ such that $T_\psi = T$. □

Remark 4.2.

$$T_{\lambda\psi}(\phi) = \langle \lambda\psi, \phi \rangle = \bar{\lambda}\langle \psi, \phi \rangle = \bar{\lambda} T_\psi(\phi), \text{ for all } \lambda \in \mathbb{C}.$$

Together with the proof above, this shows that $H \ni \psi \mapsto T_\psi \in \mathcal{L}(H, \mathbb{C})$ is a conjugate linear unitary map.

4.1. **Dirac bra-ket Notation.** Dirac's "bra-ket" notation takes full advantage of *Theorem 4.1.* Since for any $T \in \mathcal{L}(H, \mathbb{C})$ there exists a unique $\psi \in H$ such that

$$T(\eta) \coloneqq \langle \psi,\, \eta \rangle$$

or

$$T(\cdot) \coloneqq \langle \psi,\, \cdot \rangle : H \to \mathbb{C},$$

Dirac uses the shorthand notation:

$$T = \langle \psi |$$

where the $\langle \cdot |$ is referred to as a *bra*. Moreover, Dirac notation expresses $\psi \in H$ as $|\psi\rangle$, where the $|\cdot\rangle$ is known as a *ket*.

Then,

$$T(\phi) = \langle \psi || \phi \rangle = \langle \psi | \phi \rangle \coloneqq \langle \psi, \phi \rangle_H.$$

So, we may think of $|\psi\rangle$ as the column vector $\psi \in H$, and $\langle \psi|$ as the conjugate row vector $|\psi\rangle^*$. Dirac notation provides a useful shorthand for the standard basis of $\mathbb{C}^2$:

$$|0\rangle \coloneqq \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ |1\rangle \coloneqq \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

where the number found in the "ket" signifies which position the non-zero entry is in. Then for any $|\psi\rangle \in \mathbb{C}^2$, we may write

$$|\psi\rangle = \frac{\langle 0|\psi\rangle}{\sqrt{\langle \psi|\psi\rangle}}|0\rangle + \frac{\langle 1|\psi\rangle}{\sqrt{\langle \psi|\psi\rangle}}|1\rangle.$$

This idea extends to $\mathbb{C}^n$ for any $n \in \mathbb{N}$; the i^{th} standard basis vector for $\mathbb{C}^n$ can be written as $|i\rangle$ where i indicates the position of the non-zero entry. Moreover, for the purposes of quantum information theory, it is useful to write the position i as its base-2 representation with respect to the dimensionality of the tensor product space.

Example 4.3. Suppose we have the tensor product space $(\mathbb{C}^2)^{\otimes 3}$ which has dimension $2^3 = 8$, then we represent the standard basis vector $|5\rangle$ as $|101\rangle$. A nice feature of this notation is that $|101\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle$. This will come in handy for applying operations to multi-partite quantum systems, and developing quantum error-correcting codes from classical codes.

For $|\psi\rangle, |\phi\rangle \in H$, $|\psi\rangle\langle\phi| \in \mathcal{L}(H)$ is defined by $\big(|\psi\rangle\langle\phi|\big)\big(|\xi\rangle\big) \coloneqq \langle\phi|\xi\rangle|\psi\rangle$ and is a *rank-1 projector* onto $\mathbb{C}|\psi\rangle$. In particular, if $|\psi\rangle = |\phi\rangle$ and $\||\psi\rangle\| = 1$, then $|\psi\rangle\langle\psi|$ is the rank-1 orthogonal projection onto $\mathbb{C}|\psi\rangle$.

Example 4.4. Consider the Hilbert space $H = \mathbb{C}^{2n}$. Let $|e_i\rangle$ denote the i^{th} standard basis vector for $\mathbb{C}^{2n}$. Then we can define $id_H \in \mathcal{L}(H)$ by

$$id_H \coloneqq \sum_{i=1}^{2n} |e_i\rangle\langle e_i|.$$

5. Quantum States and Operations

We begin by stating Postulate 1 of quantum mechanics to motivate the subsequent discussion.

> *With every quantum system, there is an associated complex Hilbert space, known as the* state space *of the system. The* states *of the system are all positive linear maps $\rho : H \to H$ for which*
>
> $$tr(\rho) = 1$$
>
> *and can be completely described by its* state vector*, which is a unit vector in the system's state space.*

Suppose we had a machine which could produce specified pure quantum vector states. Suppose further that this machine is error-prone and with certain probabilities produces a range of different pure states around the one specified. The set of pure vector states $|\psi_i\rangle$ one may observe with respective probability p_i, is denoted by $\{p_i, |\psi_i\rangle\}$, and is referred to as an *ensemble of pure states*.

A useful object in the study of the ensemble $\{p_i,\ |\psi_i\rangle\}_{i=0}^{n-1}$ is its *density operator*, defined by

$$\rho \coloneqq \sum_{i=0}^{n-1} p_i |\psi_i\rangle(|\psi_i\rangle)^* = \sum_{i=0}^{n-1} p_i |\psi_i\rangle\langle\psi_i|$$

Theorem 5.1 (Characterization of Density Operators)**.** *An operator $\rho \in \mathcal{L}(H)$ is the density operator associated to some ensemble $\{p_i, |\psi_i\rangle\}$ if and only if ρ satisfies both of the following conditions:*

1. *(Trace Condition): tr(ρ) = 1;*
2. *(Positivity Condition): ρ is a positive operator.*

Proof. Suppose $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ is the density operator associated to some ensemble $\{p_i, |\psi_i\rangle\}$. Then,

$$\begin{aligned} tr(\rho) &= tr\Big(\sum_{i=0}^{n-1} p_i |\psi_i\rangle\langle\psi_i|\Big) \\ &= \sum_{i=0}^{n-1} p_i \cdot tr(|\psi_i\rangle\langle\psi_i|) \\ &= \sum_{i=0}^{n-1} p_i \langle\psi_i|\psi_i\rangle \\ &= \sum_{i=0}^{n-1} p_i \\ &= 1. \end{aligned}$$

So, condition (1.) is satisfied. Suppose $|\phi\rangle$ is some vector in the state space. Then,

$$\begin{aligned} \langle\phi, \rho\phi\rangle &= \sum_i p_i \langle\phi \mid \psi_i\rangle\langle\psi_i \mid \phi\rangle \\ &= \sum_i p_i |\langle\phi \mid \psi_i\rangle|^2 \\ &\geq 0. \end{aligned}$$

Hence, condition 2. is satisfied.

Conversely, suppose ρ is an operator satisfying conditions (1.) and (2.). Since ρ is positive, it must have spectral decomposition

$$\rho = \sum_j \lambda_j |j\rangle\langle j|$$

where the vectors $|j\rangle$ are orthogonal, and λ_j are real, non-negative eigenvalues of ρ.

Then, from condition (1.), we get that $\sum_j \lambda_j = 1$. Therefore, a system in state $|j\rangle$ with probability λ_j will have density operator ρ. □

This theorem gives us an intrinsic characterization of density operators and motivates the following definition.

Definition 5.2 (Density Operator, Pure/Mixed State)**.** An operator $\rho \in \mathcal{L}(H)$ is a *density operator* if it is positive and $tr(\rho) = 1$. A quantum system with vetor state $|\psi\rangle$ which is exactly known is a *pure state*, and $\rho = |\psi\rangle\langle\psi|$. On the other hand, if we have the system ensemble $\{p_i, |\psi_i\rangle\}$, where probabilities $p_i < 1$, for all i, then

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

and the system is in a *mixed* state.

5.1. **Evolution.** Postulate 2 of quantum theory states:

> *The evolution of a* closed *quantum system is described by a* unitary transformation. *That is, the vector state $|\psi\rangle$ of the system at time t_1 is related to the vector state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which*

depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle.$$

We observe that the unitary evolution of quantum systems arrises naturally from the condition that both $|\psi\rangle$ and $|\psi'\rangle$ be vector states for H and H', respectively:

$$\begin{aligned}\langle\psi|\psi\rangle = 1 &= \langle\psi'|\psi'\rangle \\ &= \langle\psi'| \cdot |\psi'\rangle \\ &= |\psi'\rangle^* \cdot |\psi'\rangle \\ &= (U|\psi\rangle)^* U|\psi\rangle \\ &= \langle\psi|U^*U|\psi\rangle.\end{aligned}$$

Hence,

$$U^*U = 1$$

implying that U is unitary. Furthermore, if the system has corresponding ensemble $\{p_i, |\psi_i\rangle\}$, we can describe the state of the system following an evolution U by

$$\rho' = \sum_{i=0}^{n-1} p_i U|\psi_i\rangle(U|\psi_i\rangle)^* = \sum_{i=0}^{n-1} p_i U|\psi_i\rangle\langle\psi_i|U^* = U\rho U^*.$$

5.2. **Measurement.** *Postulate 3 of quantum mechanics* states that *quantum measurements* are described by a collection $\{M_m\}_{m=1}^n$ of operators called a *measurement system.* These *measurement operators* act on the state space of the quantum system being measured. The index m refers to the potential measurement outcomes in an experiment. If the vector state of some system is ψ immediately before the measurement M_m then the probability that m occurs is given by

$$p(m) = \langle\psi|M_m^* M_m|\psi\rangle = \langle M_m\psi, M_m\psi\rangle = \|M_m\psi\|^2$$

and the vector state of the system after the measurement is

$$\frac{M_m\psi}{\|M_m\psi\|}$$

then we have

$$\langle\psi|\psi\rangle = 1 = \sum_{m=1}^{n} p(m) = \sum_{m=1}^{n} \langle\psi, M_m^* M_m\psi\rangle = \langle\psi, \sum_{m=1}^{n} M_m^* M_m\psi\rangle$$

which motivates the *completeness equation*, measurement operators must satisfy

$$\sum_{m=1}^{n} M_m^* M_m = I.$$

Definition 5.3 (Positive Operator-Valued Measure; POVM)**.** A *POVM* is a finite set of positive operators $\{E_i\}_{i=1}^n$ such that

$$\sum_{i=1}^{n} E_i = I.$$

Proposition 5.4. *If $\{M_i\}_{i=1}^n$ is a measurement system, then $\{E_i\}_{i=1}^n$ is a POVM, where $E_i = M_i^* M_i$. Conversely, if $\{E_i\}_{i=1}^n$ is a POVM, then $\{\sqrt{E_i}\}_{i=1}^n$ is a measurement system.*

Definition 5.5 (Projector Valued Measure; PVM)**.** A *PVM* is a POVM $\{E_i\}_{i=1}^n$ such that each E_i is an orthogonal projection, i.e.

$$E_i = E_i^* = E_i^2.$$

Definition 5.6 (Observable)**.** An *observable* is a self-adjoint operator $A : H \to H$.

By the spectral theorem, any observable A can be written as $A = \sum_{i=1}^n \lambda_i |e_i\rangle\langle e_i|$, where λ_i is an eigenvalue of A and $\{|e_i\rangle\}_{i=1}^n$ is an orthonormal basis of eigenvectors of A. Then $\{|e_i\rangle\langle e_i|\}$ is the PVM associated to the observable A.

Example 5.7. Consider the measurement operators $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$ acting on $|\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle$, where $\psi_0, \psi_1 \in \mathbb{C}$. Then the probability of observing the vector state $|0\rangle$ is given by $p(0) = \|M_0|\psi\rangle\|^2$ with

$$M_0|\psi\rangle = |0\rangle\langle 0| \begin{pmatrix} \psi_0 \\ \psi_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \psi_0 \\ \psi_1 \end{pmatrix} = \begin{pmatrix} \psi_0 \\ 0 \end{pmatrix} = \psi_0|0\rangle.$$

This gives

$$p(0) = \|\psi_0|0\rangle\|^2 = |\psi_0|^2,$$

and the state of the system after the measurement is

$$\frac{M_0|\psi\rangle}{\|M_0|\psi\rangle\|} = \frac{M_0|\psi\rangle}{\|\psi_0|0\rangle\|} = \frac{\psi_0|0\rangle}{|\psi_0|} = \frac{\psi_0}{|\psi_0|}|0\rangle.$$

Similarly, $p(1) = |\psi_1|^2$ and the state after the measurement is

$$\frac{\psi_1}{|\psi_1|}|1\rangle.$$

Note that the *measurement statistics* for the two states $(\psi_1/|\psi_1|)|1\rangle$ and $|1\rangle$ are the same, that is,

$$\|M_j \frac{\psi_1}{|\psi_1|}|1\rangle\|^2 = \|M_j|1\rangle\|^2, \text{ for all } j.$$

In this case, the two states are equal up to *global phase factor* $\psi_1/|\psi_1|$.

5.3. **Distinguishability of states.**

Definition 5.8 (Distinguishable)**.** A set of states $\{|\psi_i\rangle\}_{i=1}^m$ is *distinguishable* if there exists a measurement system $\{M_i\}_{i=1}^n$, $n \geq m$, such that $\|M_i|\psi_j\rangle\|^2 = \delta_{i,j}$ for $i, j \in \{1, ..., m\}$.

Theorem 5.9. *A set of states $\{|\psi_i\rangle\}_{i=1}^m$ is distinguishable if and only if, for all $i, j \in \{1, ..., m\}$,*

$$|\psi_i\rangle \perp |\psi_j\rangle.$$

Proof. ($\Rightarrow$) Suppose we have a measurement system $\{M_i\}_{i=1}^n$ such that $\|M_i|\psi_j\rangle\| = \delta_{ij}$, for $i, j \in \{1, ..., n\}$. Consider $|\psi_1\rangle$ and $|\psi_2\rangle$. Then $|\psi_2\rangle$ can be expressed as $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\eta\rangle$, where $|\eta\rangle \perp |\psi_1\rangle$, $\||\eta\rangle\| = 1$. Since $1 = \|\psi\|^2 = |\alpha|^2 + |\beta|^2$, we have

$$\begin{aligned} 1 = \|M_2|\psi_2\rangle\|^2 &= \|M_2\big(\alpha|\psi_1\rangle + \beta|\eta\rangle\big)\|^2 \\ &= |\beta|^2\|M_2|\eta\rangle\|^2 \\ &\leq |\beta|^2\||\eta\rangle\|^2 \\ &\leq 1. \end{aligned}$$

Then $1 \leq |\beta|^2 \leq 1$, which implies $|\beta|^2 = 1$ and $\alpha = 0$. Therefore, $|\psi_2\rangle$ and $|\eta\rangle$ are collinear. Hence, $|\psi_2\rangle \perp |\psi_1\rangle$.

($\Leftarrow$) Let M_i be the orthogonal projection onto the one-dimensional subspace spanned by $|\psi_i\rangle$. Then, $M_i = M_i^* = M_i^* M_i$, for $i = 1, ..., n$, and $\sum_{i=1}^n M_i^* M_i$ is the orthogonal projection onto $span\{\psi_1, ..., \psi_n\}$. Let M_0 be the orthonormal projection onto $span\{\psi_1, ..., \psi_n\}^\perp$. Then $\sum_{j=0}^n M_j^* M_j = \sum_{j=0}^n M_j = I$. Furthermore, $M_i|\phi_j\rangle = \delta_{ij}|\psi_j\rangle$ for all $i, j \in \{1, ..., n\}$, so that $\|M_i|\phi_j\rangle\|^2 = \delta_{ij}$ for all $i, j \in \{1, ..., n\}$. Hence, $\{M_i\}_{i=1}^n$ is a measurement system. □

5.4. **The Qubit.** In the classical setting information is stored as bits, where a single bit can take on one of two values: 0 or 1. We refer to the value of the bit as the *state* of the bit. When one considers the state of an n-bit system, one is concerned with the cartesian product of the state of each bit, i.e. the state of the classical system can be viewed as an n-dimensional vector $\{a_i\}_{i=1}^n \in \mathbb{Z}_2^n$ where $a_i \in \mathbb{Z}_2$.

In the quantum setting however, information is stored as *quantum bits*, or *qubits*. A single qubit $|\psi\rangle$ is described by a unit vector in the Hilbert space $H = \mathbb{C}^2$. Then H is a 2-dimensional *state space*.

We have just described the simplest state space possible for quantum information, i.e. a single qubit. For multi-qubit systems we must make use of tensor products. A 2-qubit system is described by the tensor product between two individual single qubit systems. For the two qubits $|\psi_1\rangle \in \mathbb{C}^2$ and $|\psi_2\rangle \in \mathbb{C}^2$ we get the vector state of the multi-qubit system described by

$$|\psi_1\rangle \otimes |\psi_2\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$$

If $|\psi_1\rangle = a_1|0\rangle + b_1|1\rangle$ and $|\psi_2\rangle = a_2|0\rangle + b_2|1\rangle$, then by the rules for tensor products outlined earlier we get:

$$\begin{aligned} |\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle &= a_1a_2|0\rangle \otimes |0\rangle \ + \ a_1b_2|0\rangle \otimes |1\rangle \ + \ b_1a_2|1\rangle \otimes |0\rangle \ + \ b_1b_2|1\rangle \otimes |1\rangle \\ &= a_1a_2|00\rangle \ + \ a_1b_2|01\rangle \ + \ b_1a_2|10\rangle \ + \ b_1b_2|11\rangle. \end{aligned}$$

We observe that,

$$\begin{aligned} \langle \psi \mid \psi \rangle &= \sqrt{|a_1a_2|^2 + |a_1b_2|^2 + |b_1a_2|^2 + |b_1b_2|^2} \\ &= \sqrt{(|a_1|^2 + |b_1|^2)(|a_2|^2 + |b_2|^2)} \\ &= \langle \psi_1 \mid \psi_1 \rangle \cdot \langle \psi_2 \mid \psi_2 \rangle \\ &= 1. \end{aligned}$$

Hence, $|\psi\rangle$ is a vector state for the system $\mathbb{C}^2 \otimes \mathbb{C}^2$. This extends to systems of n-qubits.

Example 5.10. Let $H_1 = H_2 = \mathbb{C}^2$. Then

$$|01\rangle - |10\rangle \coloneqq \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] - \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right] = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \in \mathbb{C}^2 \otimes \mathbb{C}^2.$$

Remark 5.11. This element cannot be written as a simple tensor. We observe that for $\psi, \phi \in \mathbb{C}^2$, if

$$\psi \otimes \phi = \begin{pmatrix} \psi_1 \cdot \phi_1 \\ \psi_1 \cdot \phi_2 \\ \psi_2 \cdot \phi_1 \\ \psi_2 \cdot \phi_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix},$$

then

$$\psi_1 \cdot \phi_2 = 1 \text{ implies } \psi_1 \neq 0,$$

so

$$\psi_1 \cdot \phi_1 = 0 \text{ implies } \phi_1 = 0.$$

But

$$\psi_2 \cdot \phi_1 = -1 \text{ implies } \phi_1 \neq 0,$$

which is a contradiction. Thus, for all $\psi, \phi \in \mathbb{C}^2$

$$\psi \otimes \phi \neq \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}.$$

In other words,

$$H_1 \otimes H_2 \nsubseteq \{\psi \otimes \phi \mid \psi \in H_1,\ \phi \in H_2\}.$$

Definition 5.12 (Separable)**.** An element $\Psi \in H_1 \otimes H_2$ is *separable* if there exists $\phi \in H_1$, and $\psi \in H_2$ such that

$$\Psi = \phi \otimes \psi.$$

If Ψ is not of this form, then it is *non-separable.*

Definition 5.13 (Entanglement)**.** A pure state $\rho_\Psi \in \mathcal{L}(H_1 \otimes H_2)$ is called *non-entangle* if there exist pure states $\rho_\phi \in \mathcal{L}(H_1)$ and $\rho_\psi \in \mathcal{L}(H_2)$ such that

$$\rho_\Psi = \rho_\phi \otimes \rho_\psi.$$

Remark 5.14. Let $|\Psi\rangle \in H_1 \otimes H_2$ be separable, that is, there exists $|\psi\rangle \in H_1$ and $|\phi\rangle \in H_2$ such that $|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle$. Then the pure state $\rho_\Psi \in \mathcal{L}(H_1 \otimes H_2)$ corresponding to $|\Psi\rangle$ is

$$\begin{aligned} \rho_\Psi &= |\Psi\rangle\langle\Psi| \\ &= \big(|\psi\rangle \otimes |\phi\rangle\big)\big(\langle\psi| \otimes \langle\phi|\big) \\ &= |\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi| \\ &= \rho_\psi \otimes \rho_\phi. \end{aligned}$$

Thus, separable elements in $H_1 \otimes H_2$ have corresponding non-entangled pure states in $\mathcal{L}(H_1 \otimes H_2)$. Moreover, non-separable elements in $H_1 \otimes H_2$ have corresponding *entangled* pure states in $\mathcal{L}(H_1 \otimes H_2)$.

5.5. **Environments and Quantum Channels.**

Definition 5.15 (Partial Trace)**.** Consider $\mathcal{L}(H_1 \otimes H_2)$. We define the *partial trace* over $\mathcal{L}(H_2)$ by

$$tr_{\mathcal{L}(H_2)} \coloneqq I_{\mathcal{L}(H_1)} \otimes tr : \mathcal{L}(H_1 \otimes H_2) \to \mathcal{L}(H_1),$$

where for a simple element $\rho \otimes \phi \in \mathcal{L}(H_1 \otimes H_2)$

$$\rho \otimes \phi \mapsto tr(\phi)\rho.$$

Definition 5.16 (Reduced Density Operator)**.** Suppose we have a quantum system $H_1 \otimes H_2$ with corresponding density operator $\rho \in \mathcal{L}(H_1 \otimes H_2)$. We define the *reduced density operator*, ρ_{H_1}, as the partial trace of ρ over $\mathcal{L}(H_2)$, that is

$$\rho_{H_1} \coloneqq tr_{\mathcal{L}(H_2)}(\rho).$$

The dynamics of a closed quantum system can be described by a unitary transformation. Conceptually, one can think of the unitary transformation as a box into which the input state enters and from which the output exits.

A natural way to describe the dynamics of an *open* quantum system is to regard it as arising from an interaction between our system of interest, called the *principal system*, and an *environment* in which the principal system lives, which together form a *closed* system. In other words, suppose we have a principal system in state ρ, and in an environment in state ρ_{env}, then $\rho \otimes \rho_{env}$ describes the state of the closed system. In general, the final state of the principal system, $\mathcal{E}(\rho)$, may *not* be related by a unitary transformation to the initial state ρ. We assume that the system-environment input state is a non-entangled state, $\rho \otimes \rho_{env}$. Thus, we perform a partial trace over the environment to obtain the reduced state of the principal system alone

$$\mathcal{E}(\rho) = tr_{env}\big[U(\rho \otimes \rho_{env})U^*\big],$$

which motivates the following definition.

Definition 5.17 (Quantum Channel)**.** Let H_1, H_2 be state spaces. A *quantum channel* is a linear mapping $\mathcal{E} : \mathcal{L}(H_1) \to \mathcal{L}(H_2)$ satisfying

1. $\mathcal{E}$ is *trace preserving*;
$$tr\big(\mathcal{E}(\rho)\big) = tr(\rho), \quad \text{for all } \rho \in L(H_1).$$
2. $\mathcal{E}$ is *completely positive*;
$$id \otimes \mathcal{E} : \mathcal{L}(\mathbb{C}^k) \otimes \mathcal{L}(H_1) \to \mathcal{L}(\mathbb{C}^k) \otimes \mathcal{L}(H_2)$$
is a positive map, for all k.

Mathematically a quantum channel is a completely-positive trace-preserving map, otherwise referred to as a *CPTP* map [5].

Theorem 5.18. *The operator $\mathcal{E} : L(H_1) \to L(H_2)$ is a quantum operator if and only if*

$$\mathcal{E}(\rho) = \sum_{i=1}^{n} E_i \rho E_i^*$$

for some collection $\{E_i\}_{i=1}^n \subseteq L(H_1, H_2)$ satisfying $\sum_{i=1}^n E_i^* E_i = I$.

For the proof see [4].

Proposition 5.19. *Let $\mathcal{E}(\rho) = \sum_{i=1}^n E_i \rho E_i^*$, and let U be an $n \times n$ unitary matrix with complex entries u_{ij} where i refers to the row position and j refers to the column position. Set $F_i = \sum_{j=1}^n u_{ij} E_j$. Then,*

$$\mathcal{E}(\rho) = \sum_{i=1}^{n} F_i \rho F_i^*.$$

Proof.

$$\begin{aligned}\sum_{i=1}^{n} F_i \rho F_i^* &= \sum_{i=1}^{n} \Big(\sum_{j=1}^{n} u_{ij} E_j \Big) \rho \Big(\sum_{j=1}^{n} u_{ij} E_j \Big)^* \\ &= \sum_{i=1}^{n} \sum_{j,k=1}^{n} u_{ij} \overline{u}_{ik} E_j \rho E_k^* \\ &= \sum_{j,k=1}^{n} \Big(\sum_{i=1}^{n} u_{ij} \overline{u}_{ik} \Big) E_j \rho E_k^* \\ &= \sum_{j,k=1}^{n} E_j \rho E_k^* \\ &= \mathcal{E}(\rho)\end{aligned}$$

since $\sum_{i=1}^{n} u_{ij} \overline{u}_{ik}$ equals 0 if $j \neq k$ and equals 1 if $j = k$. □

6. Quantum Error-Correcting Conditions, and Pauli Operators

We begin by drawing analogies from classical coding theory to build an intuition for the theory of quantum-error correction. A classical binary linear code is a subspace C_{cl} of a larger binary vector space $\mathbb{Z}_2^n$. Suppose we send a codeword c through a noisy channel and get $y = c + e$ on the receiving end, where $e \in \mathbb{Z}_2^n$. Then the error may be detected by determining whether or not y is in C_{cl} by performing a *syndrome measurement* on y, where the possible *error-syndromes* correspond to distinct cosets of C_{cl}. Recovery of the original codeword is possible once we have identified the coset of C_{cl} in which y lies.

Analogously, a *quantum code*, C, is a subspace of a larger complex Hilbert space. Suppose we send a codeword in state ρ through a noisy channel and get $\sigma = \mathcal{E}(\rho)$ on the receiving end, where $\mathcal{E}$ is a quantum operator. Then the quantum-error may be detected by determining whether or not σ lies in C by a performing a syndrome measurement on σ, where the possible error-syndromes correspond to distinct orthogonal subspaces to C in the larger complex Hilbert space. Recovery of the original codeword is possible once we have identified the subspace in which σ lies.

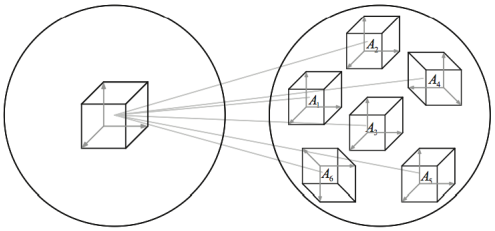

Figure 1. The box on the left represents the quantum (classical) code within a code space represented by the left circle, the boxes on the right represent the possible subspaces (cosets) in which a transmitted codeword may land. (Figure taken from [3])

Definition 6.1. Let C be a subspace of the complex Hilbert space H, and let $\mathcal{E} : \mathcal{L}(H) \to \mathcal{L}(H)$ be a quantum channel, where $\mathcal{E} = \{E_i\}_{i=1}^n$. If there exists an operation $\mathcal{R} : \mathcal{E}(\mathcal{L}(C)) \to$

$\mathcal{L}(C)$ such that, for any density operator $\rho \in \mathcal{L}(C)$, we have

$$\mathcal{R}\big(\mathcal{E}(\rho)\big) = \rho,$$

then $\mathcal{R}$ *corrects* $\mathcal{E}$ on *quantum code* C, and $\{E_i\}_{i=1}^n$ is a set of *correctable* errors on C.

Theorem 6.2 (Quantum error-correcting conditions)**.** *Let P be the projector onto some quantum code C, and suppose $\mathcal{E}$ is a quantum channel with elements $\{E_i\}_{i=1}^n$. Then there exists an error-correction operation $\mathcal{R}$ correcting $\mathcal{E}$ on C if and only if*

$$PE_i^*E_jP = \alpha_{ij}P$$

for some complex self-adjoint matrix α.

The elements of the noise operation $\mathcal{E} = \{E_i\}_{i=1}^n$ are known as *errors*, and if $\mathcal{R}$ corrects $\mathcal{E}$ on C then $\{E_i\}_{i=1}^n$ is a *correctable set of errors*.

Proof. Suppose $\{E_i\}_{i=1}^n$ is a set of operators which satisfy the error-correcting conditions. Then each pair of elements satisfies

$$PE_i^*E_jP = \alpha_{ij}P.$$

By assumption, the matrix α is self-adjoint, and thus can be diagonalized

$$d = u^*\alpha u$$

where u is unitary and d is diagonal. Now define the operators,

$$F_k := \sum_{i=1}^n u_{ik}E_i$$

then as was shown earlier $\{F_k\}$ is also a set of quantum operators for $\mathcal{E}$. By substitution we get

$$\begin{aligned}
PF_k^*F_tP &= P\Big(\sum_{i=1}^n u_{ik}^*E_i^*\Big)\Big(\sum_{j=1}^n u_{jt}E_j\Big)P \\
&= \sum_{i=1}^n\sum_{j=1}^n u_{ik}^*u_{jt}PE_i^*E_jP \\
&= \sum_{i=1}^n\sum_{j=1}^n u_{ik}^*u_{jt}\alpha_{ij}P \\
&= \sum_{i=1}^n\sum_{j=1}^n u_{ik}^*\alpha_{ij}u_{jt}P \\
&= d_{kt}P.
\end{aligned}$$

We observe that if $k \neq t$, then $d_{kt} = 0$.

· Detection:

Now we define the syndrome measurement using $PF_k^*F_tP = d_{kt}P$ and polar decomposition. From the polar decomposition of F_kP we have

$$F_kP = U_k\sqrt{PF_k^*F_kP} = U_k\sqrt{d_{kk}}P = \sqrt{d_{kk}}U_kP$$

where U_k is some unitary matrix. So F_k can be seen as a rotation of the coding subspace into the subspace defined by the projector

$$P_k \coloneqq U_k P U_k^* = \frac{1}{\sqrt{d_{kk}}} F_k P U_k^*$$

where if $d_{kk} = 0$ then $P_k = 0$. Then we note that, for $j \neq k$, we have

$$P_j P_k = P_j^* P_k = \frac{1}{\sqrt{d_{jj} d_{kk}}} U_j P F_j^* F_k P U_k^* = 0.$$

· Recovery:

Given some output state σ we can recover the original input state $\rho \in \mathcal{L}(C)$ by applying a unitary operator U_k^*. Thus the error-correcting operation $\mathcal{R}$, i.e. combined detection and recovery, corresponds to

$$\mathcal{R}(\sigma) = \sum_{k=1}^{n} U_k^* P_k \sigma P_k U_k + Q \sigma Q,$$

where $Q \coloneqq I - \sum_{k=1}^{n} P_k$. Since

$$\begin{aligned} \sum_{k=1}^{n} \left(U_k^* P_k\right)^* \left(P_k U_k\right) + Q^* Q &= \sum_{k=1}^{n} P_k U_k U_k^* P_k + Q^2 \\ &= \sum_{k=1}^{n} P_k + I - \sum_{k=1}^{n} P_k \\ &= I, \end{aligned}$$

we know that $\mathcal{R}$ is a CPTP map. Moreover, observe that

$$Q P_j = \Big(I - \sum_{k=1}^{n} P_k\Big) P_j = P_j - P_j^2 = 0,$$

since $P_k P_j = 0$, for all $k \neq j$.

For states ρ which have undergone some error resulting in $\mathcal{E}(\rho)$, correction is possible with

$$\begin{aligned}
\mathcal{R}(\mathcal{E}(\rho)) &= \sum_{k=1}^{n} U_k^* P_k \Big(\sum_{t=1}^{n} F_t \rho F_t^* \Big) P_k U_k + Q \Big(\sum_{t=1}^{n} F_t \rho F_t^* \Big) Q \\
&= \sum_{k,t=1}^{n} U_k^* P_k F_t \rho F_t^* P_k U_k + \sum_{t=1}^{n} Q F_t P \rho P F_t^* Q \\
&= \sum_{k,t=1}^{n} U_k^* \big(P_k^*\big) F_t P \rho P F_t^* \big(P_k\big) U_k + \sum_{t=1}^{n} d_{tt} Q P_t U_t \rho U_t^* P_t Q \\
&= \sum_{k,t=1}^{n} U_k^* \Big(U_k \frac{1}{\sqrt{d_{kk}}} P F_k^* \Big) F_t P \rho P F_t^* \Big(F_k P \frac{1}{\sqrt{d_{kk}}} U_k^* \Big) U_k \\
&= \sum_{k,t=1}^{n} \frac{1}{\sqrt{d_{kk}}} d_{kt} P \rho \, d_{tk} P \frac{1}{\sqrt{d_{kk}}} \\
&= \sum_{k=1}^{n} \frac{1}{\sqrt{d_{kk}}} d_{kk} P \rho P d_{kk} \frac{1}{\sqrt{d_{kk}}} \\
&= \sum_{k=1}^{n} d_{kk} P \rho P \\
&= \sum_{k=1}^{n} d_{kk} \rho \\
&= \rho,
\end{aligned}$$

where in the fourth equality we use that $QP_t = 0$. For the converse see *Theorem 10.2* of [3]. □

Theorem 6.3. *Let C be a quantum code with error-correcting operation $\mathcal{R}$ corresponding to the quantum channel $\mathcal{E}$ with elements $\{E_i\}_{i=1}^n$. Let $\mathcal{F}$ be the quantum channel with elements $\{F_t\}_{t=1}^m$ where $F_t = \sum_{i=1}^n \beta_{ti} E_i$ for some matrix β with complex entries. Then $\mathcal{R}$ also corrects for error process $\mathcal{F}$.*

Proof. The set $\{E_i\}_{i=1}^n$ must satisfy the quantum error-correcting condition $PE_i^* E_j P = \alpha_{ij} P$. From the proof of the previous theorem, without loss of generality we may take α to be a diagonal matrix, $\alpha_{ij} = d_{ij}$. Moreover, we can choose U_k so that $E_k P = \sqrt{d_{kk}} U_k P$. Then let $P_k \coloneqq \frac{1}{\sqrt{d_{kk}}} E_k P U_k^*$. Observe that, for states $\rho \in \mathcal{L}(C)$, we have

$$\begin{aligned}
U_k^* P_k E_i \sqrt{\rho} &= U_k^* P_k^* E_i P \sqrt{\rho} \\
&= \frac{1}{\sqrt{d_{kk}}} U_k^* U_k P E_k^* E_i P \sqrt{\rho} \\
&= \frac{d_{ki} P \sqrt{\rho}}{\sqrt{d_{kk}}}, \quad \text{equals 0 for } i \neq k \\
&= \delta_{ki} \frac{d_{kk} P \sqrt{\rho}}{\sqrt{d_{kk}}} \\
&= \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho}
\end{aligned}$$

Similarly, $\sqrt{\rho}E_i^* P_k U_k = \delta_{ki}\sqrt{d_{kk}}\sqrt{\rho}$.

By substituting $F_t = \sum_{i=1}^n \beta_{ti} E_i$, we get

$$\begin{aligned} U_k^* P_k F_t \sqrt{\rho} &= U_k^* P_k \Big(\sum_{i=1}^n \beta_{ti} E_i \Big) \sqrt{\rho} \\ &= \sum_{i=1}^n \beta_{ti} U_k^* P_k E_i \sqrt{\rho} \\ &= \sum_{i=1}^n \beta_{ti} \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho} \\ &= \beta_{tk} \sqrt{d_{kk}} \sqrt{\rho}. \end{aligned}$$

Similarly, $\sqrt{\rho} F_t^* P_k U_k = \bar{\beta}_{tk} \sqrt{d_{kk}} \sqrt{\rho}$. Then,

$$\begin{aligned} \mathcal{R}(\mathcal{F}(\rho)) &= \sum_{k=1}^n U_k^* P_k \Big(\sum_{t=1}^m F_t \rho F_t^* \Big) P_k U_k \\ &= \sum_{k=1}^n \sum_{t=1}^m U_k^* P_k F_t \sqrt{\rho} \sqrt{\rho} F_t^* P_k U_k \\ &= \sum_{k=1}^n \sum_{t=1}^m (\beta_{tk} \sqrt{d_{kk}} \sqrt{\rho})(\bar{\beta}_{tk} \sqrt{d_{kk}} \sqrt{\rho}) \\ &= \sum_{k=1}^n \sum_{t=1}^m |\beta_{tk}|^2 d_{kk} \rho \\ &= \alpha \rho \\ &= \rho \end{aligned}$$

where $\alpha = 1$ since $\mathcal{R}, \mathcal{F}$ are CPTP maps. □

6.1. **The Pauli Matrices.** An important set of unitary operators to the field of quantum information theory is the set of 2×2 Pauli matrices. The three Pauli matrices are denoted X, Z, Y, and are defined as follows:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

It is easy to see that $X^*X = Y^*Y = Z^*Z = I$. Hence the Pauli matrices are unitary. To get an idea of how the Pauli matrices operate, let $|\psi\rangle \in \mathbb{C}^2$. In terms of the standard basis, $|\psi\rangle = a|0\rangle + b|1\rangle$ for some $a, b \in \mathbb{C}$, so we get

$$X|\psi\rangle = X\big(a|0\rangle + b|1\rangle\big) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix} = b|0\rangle + a|1\rangle.$$

Thus, X interchanges the coefficients in the standard basis description of $|\psi\rangle$. In the computational interpretation, X acts as the *bit flip* operation. Similarly, for Y and Z we get

$$\begin{aligned} Y|\psi\rangle &= -ib|0\rangle + a|1\rangle, \\ Z|\psi\rangle &= a|0\rangle - b|1\rangle. \end{aligned}$$

Then Z is the *phase flip* operation, as it changes the phase on the $|1\rangle$ coefficient.

Next we find the eigenvalues and eigenvectors of elements X, Z, and Y with respect to the standard basis.

The eigenvalues of X satisfy

$$\det(X - \lambda I) = \det \begin{pmatrix} -\lambda & 1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 - 1 = (\lambda + 1)(\lambda - 1)$$

and hence

$$\lambda_{X+} = 1, \text{ and } \lambda_{X-} = -1.$$

A normalized eigenvector $|\psi\rangle = a|0\rangle + b|1\rangle$ corresponding to λ_{X+} satisfies

$$a|0\rangle + b|1\rangle \;=\; \lambda_{X+}\big(a|0\rangle + b|1\rangle\big) \;=\; X \begin{pmatrix} a \\ b \end{pmatrix} \;=\; b|0\rangle + a|1\rangle$$

implying that $a = b$. We obtain

$$\psi_{X+} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \;=\; \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big).$$

Similarly,

$$\psi_{X-} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \;=\; \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big).$$

In the literature, these are often denoted as $|+\rangle$ and $|-\rangle$, respectively. The eigenvalues and eigenvectors of the other Pauli matrices are found in the same way, which gives us

$$\lambda_{Y+} = 1, \quad \psi_{Y+} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \qquad \lambda_{Z+} = 1, \quad \psi_{Z+} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle,$$

$$\lambda_{Y-} = -1, \quad \psi_{Y-} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}, \qquad \lambda_{Z-} = -1, \quad \psi_{Z-} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle.$$

As a consequence, all Pauli matrices have eigenvalues of ± 1.

6.2. **The Real Pauli Group.** Now we define a group G constructed from Pauli matrices that will be central to our study of quantum error-correcting codes. Let $G = \langle X, Z \rangle$ be the group generated by X and Z via matrix multiplication. Then, it is easy to check that

$$X^2 = Z^2 = I \in G,$$

We also have

$$XZ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \;=\; \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \;=\; -\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -ZX \in G$$

and

$$(XZ)^2 = \; (XZ)(XZ) \;=\; -(ZX)(XZ) \;=\; -Z(XX)Z \;= -I \in G.$$

Hence, the group G is

$$G = \{\pm I, \pm X, \pm Z, \pm XZ\}.$$

Remark 6.4. Suppose w is in the centre of G, defined by

$$\mathcal{Z}(G) \coloneqq \{g \in G \mid gg' = g'g \text{ for all } g' \in G\}.$$

Then $wX = Xw$ and $wZ = Zw$, which implies $w = \pm I$. Thus, $\mathcal{Z}(G) = \{\pm I\}$.

We observe that G is a subgroup of the orthogonal group $O(2)$.

7. The Error Group E

The remainder of the discussion is centered on a paper by Calderbank et al. [1], which presents a geometric formalism to produce quantum error-correcting codes via a group theoretic framework.

Let E denote the set of elements $e \in \mathcal{L}((\mathbb{C}^2)^{\otimes n})$ of the form

$$e = w_1 \otimes \cdots \otimes w_n$$

where w_j is an element of the real Pauli group $G = \{\pm I,\ \pm X,\ \pm Z,\ \pm XZ\}$. Since,

$$aU_1 \otimes bU_2 = abU_1 \otimes U_2$$

we may rewrite elements $e \in E$ as $e = \pm w_1 \otimes \cdots \otimes w_n$ where the w_j now lie in the set $\{I,\ X,\ Z,\ XZ\}$.

We define multiplication of elements $e_1, e_2 \in E$ with $e_1 = \otimes_{i=1}^n u_i$ and $e_2 = \otimes_{i=1}^n v_i$, by

$$e_1 e_2 = \big(\overset{n}{\underset{i=1}{\otimes}} u_i\big)\big(\overset{n}{\underset{i=1}{\otimes}} v_i\big) = \overset{n}{\underset{i=1}{\otimes}} u_i v_i$$

Then, $u_i v_i \in G$, for all $i = 1, ..., n$, so $e_1 e_2 \in E$ for all $e_1, e_2 \in E$. Therefore E is closed under multiplication. The element $I_E = I^{\otimes n}$ is clearly the identity element of multiplication in E. Let $e = \otimes_{i=1}^n w_i$ in E. Then, since $w_i^{-1} \in G$ for all $i = 1, ...n$, we have that $e^{-1} = \otimes_{i=1}^n w_i^{-1}$ is in E, for all $e \in E$. Thus, E is a group under multiplication.

7.1. **Properties of the group E.** To construct an element of the group E, we must choose from the $4 = 2^2$ elements $\{I, X, Z, XY\}$ for each of the n tensor entries, which gives us $(2^2)^n = 2^{2n}$ elements of the group E. Then, since each element of E has a factor of ± 1, E is a group of $2(2^{2n}) = 2^{2n+1}$ orthogonal $2^n \times 2^n$ matrices.

The quotient group $E/\mathcal{Z}(E)$, plays an important role in the construction of quantum error correcting codes, so we determine $\mathcal{Z}(E)$.

Suppose $e = \otimes_{i=1}^n w_i \in \mathcal{Z}(E)$. Then, let $e_{X_j} = \otimes_{i=1}^n u_i, e_{Z_j} = \otimes_{i=1}^n v_i \in E$, with $u_j = X$, $v_j = Z$, and $u_i, v_i = I$, $\forall\, i \neq j$. Since $e \in \mathcal{Z}(E)$, we have that $e e_{X_j} = e_{X_j} e$ and $e e_{Z_j} = e_{Z_j} e$. In particular, we have that $w_j X = X w_j$ and $w_j Z = Z w_j$. Which implies $w_j \in \mathcal{Z}(G)$. Since j is a arbitrary in $\{1, ..., n\}$, this holds for any $j = 1, ..., n$. So $w_i = \pm I$, for all $i = 1, ..., n$. Thus, $\mathcal{Z}(E) = \{\pm I\}$.

With this, we define the quotient group

$$\bar{E} \coloneqq E/\mathcal{Z}(E) = \{e\mathcal{Z}(E) \mid e \in E\}.$$

Proposition 7.1. *$\bar{E}$ is abelian.*

Proof.

$$\begin{aligned}
\bar{e_1}\bar{e_2} &= (e_1\mathcal{Z}(E))(e_2\mathcal{Z}(E)) \\
&= e_1(\mathcal{Z}(E)e_2)\mathcal{Z}(E) \\
&= e_1(e_2\mathcal{Z}(E))\mathcal{Z}(E) \\
&= (e_1e_2)\mathcal{Z}(E) \\
&= (-e_2e_1)\mathcal{Z}(E) \\
&= (-e_2\mathcal{Z}(E))(e_1\mathcal{Z}(E)) \\
&= e_2(-I)\mathcal{Z}(E)\overline{e}_1 \\
&= e_2\mathcal{Z}(E)\overline{e}_1 \\
&= \bar{e_2}\bar{e_1}.
\end{aligned}$$

Hence, $\bar{E}$ is abelian.

□

We can express $\bar{e} \in \bar{E}$ as a $2n$-dimensional vector $v = (v_1, ..., v_{2n}) \in \mathbb{Z}_2^{2n}$ in the following way.

If $\bar{e}$ contains an I on the j^{th} qubit, then $v_j = 0 = v_{n+j}$. If $\bar{e}$ contains an X on the j^{th} qubit, then $v_j = 1$ and $v_{n+j} = 0$. If $\bar{e}$ contains an Z on the j^{th} qubit, then $v_j = 0$ and $v_{n+j} = 1$. If $\bar{e}$ contains both an X and a Z on the j^{th} qubit, then $v_j = 1 = v_{n+j}$. We denote the vector $v \in \mathbb{Z}_2^{2n}$ corresponding to $\bar{e} \in \bar{E}$ as $v = (a|b)$, where $(a|b)$ is the concatenation of vector $a \in \mathbb{Z}_2^n$ corresponding to the position of X operations in $e \in E$, and vector $b \in \mathbb{Z}_2^n$ corresponding to the position of Z operations in $e \in E$. Then, we notice that multiplication in E corresponds to vector addition modulo 2 in $\bar{E}$, that is, for $e_1, e_2 \in E$ with $\bar{e}_1 = (a_1|b_1)$ and $\bar{e}_2 = (a_2|b_2)$ in $\bar{E}$, the image of e_1e_2 in $\bar{E}$, is given by

$$\overline{e_1e_2} = (a_1 \oplus a_2|b_1 \oplus b_2)$$

Thus, we define

$$\bar{e}_1\bar{e}_2 \coloneqq \overline{e_1e_2}.$$

Definition 7.2 (Weight)**.** The *weight* of an element $\bar{e} = (a|b) \in \bar{E}$ is defined by

$$w(\bar{e}) = \sum_{i=1}^{n}(a_i + b_i).$$

The distance between two elements $\bar{e}_1, \bar{e}_2 \in \bar{E}$ is defined to be the weight of their difference. Suppose we have $\bar{e}_1, \bar{e}_2 \in \bar{E}$, then

$$\begin{aligned}
w(\bar{e}_1\bar{e}_2) &= w\big((a_1 \oplus a_2|b_1 \oplus b_2)\big) \\
&= \sum_i \big((a_{1_i} + a_{2_i} \pmod 2) + (b_{1_i} + b_{2_i} \pmod 2)\big) \\
&\leq \sum_i (a_{1_i} + b_{1_i} \pmod 2) + \sum_i (a_{2_i} + b_{2_i} \pmod 2) \\
&= w(\bar{e}_1) + w(\bar{e}_2).
\end{aligned}$$

Thus, $w(\bar{e}_1\bar{e}_2) \leq w(\bar{e}_1) + w(\bar{e}_2)$.

8. Quantum Error-Correcting Codes

To motivate the following discussion, we describe classical binary linear codes from an unusual perspective. A classical code C is a subspace of $\mathbb{Z}_2^n$. But, $\mathbb{Z}_2^n$ is also the group of possible errors on C, i.e. C is a subgroup of the error group. Then an error e is in C when translation by e takes codewords to codewords, which means e is an undetectable error. A set of errors is a detectable set if the sum of any two errors from the set lies outside of C. Even though the sum can be equal to the trivial error 0, which lies in C and thus undetectable, it has no effect.

In the quantum setting it is possible for errors to be non-trivial and yet have no effect on the encoded state. Then we construct quantum codes from two subgroups of the quantum error group E; the subgroup of undetectable errors, S', and a subgroup of S', denoted S, composed of errors which have no effect. Then S is equivalent to the 0 error in the classical setting.

For this construction we will require that every element of S' commutes with S, which implies S is abelian. So we need a criterion for when two elements of E commute.

Let A be the $2n \times 2n$ matrix defined by

$$A = \begin{pmatrix} \mathbf{0} & I_{n\times n} \\ \mathbf{0} & \mathbf{0} \end{pmatrix},$$

and define the binary quadratic form $Q : \bar{E} \to \mathbb{Z}_2$ by $Q(\bar{e}) \mapsto \bar{e}A\bar{e}^T$. Then for an element $\bar{e} = (a|b) \in \bar{E}$ we have

$$\begin{aligned} \bar{e}A\bar{e}^T &= (a|b)A(a|b)^T \\ &= (a|b)(b|0)^T \\ &= a \cdot b + 0 \\ &= \sum_{i=1}^{n} a_i b_i \pmod 2. \end{aligned}$$

Hence for $e = w_1 \otimes \cdots \otimes w_n$ in E with image $\bar{e} \in \bar{E}$, $Q(\bar{e})$ is the parity of the number of components w_j which equal XZ.

Definition 8.1 (Totally singular)**.** A subspace $\bar{S} \subseteq \bar{E}$ is said to be *totally singular* if $\forall\, \bar{s} \in \bar{S}$ we have $Q(\bar{s}) = 0$.

We now define a *symplectic inner product* $\langle \cdot\ ,\ \cdot \rangle_{\bar{E}} : \bar{E} \times \bar{E} \to \mathbb{Z}_2$, which serves as our commutativity criterion. Let $\Lambda \coloneqq A + A^T$,

$$\Lambda = \begin{pmatrix} \mathbf{0} & I_{n\times n} \\ I_{n\times n} & \mathbf{0} \end{pmatrix},$$

and let $\bar{e_1} = (a_1|b_1)$, $\bar{e_2} = (a_2|b_2)$ in $\bar{E}$. Then define the the map $\langle \cdot,\ \cdot \rangle_{\bar{E}} : \bar{E} \times \bar{E} \to \mathbb{Z}_2$ by

$$\langle \bar{e_1},\ \bar{e_2} \rangle_{\bar{E}} = \bar{e_1} \Lambda \bar{e_2}^T = a_1 b_2 + b_1 a_2 \pmod 2.$$

Then $e_1, e_2 \in E$ commute if and only if $\langle \bar{e_1},\ \bar{e_2} \rangle_{\bar{E}} = 0$. Thus, we get

$$e_1 e_2 = (-1)^{\langle \bar{e_1},\ \bar{e_2} \rangle_{\bar{E}}} e_2 e_1,$$

for all $e_1, e_2 \in E$.

Definition 8.2 (Totally isotropic)**.** A subspace $\bar{S} \subseteq \bar{E}$ is *totally isotropic* if for all $\bar{s_1}, \bar{s_2} \in \bar{S}$ we have $\langle \bar{s_1},\ \bar{s_2} \rangle_{\bar{E}} = 0$.

Proposition 8.3. *If $\bar{S} \subseteq \bar{E}$ is a totally singular subspace, then $\bar{S}$ is totally isotropic.*

Proof. Let $\bar{s}, \bar{s}' \in \bar{S}$. Then $Q(\bar{s}) = Q(\bar{s}') = 0$. Suppose that $\langle \bar{s}, \bar{s}' \rangle_{\bar{E}} \neq 0$. Then, $\bar{s}'' = \bar{s} \oplus \bar{s}' \in \bar{S}$ so $\bar{s}'' = (a \oplus a' \mid b \oplus b')$, and we get

$$\begin{aligned} Q(\bar{s}'') &= (a \oplus a' \mid b \oplus b') A (a \oplus a' \mid b \oplus b')^T \\ &= (a \oplus a' \mid b \oplus b')(b \oplus b' \mid 0)^T \\ &= \sum_{i=1}^{n} (a_i + a'_i)(b_i + b'_i) \\ &= \sum_{i=1}^{n} a_i b_i + \sum_{i=1}^{n} (a_i b'_i + a'_i b_i) + \sum_{i=1}^{n} a'_i b'_i \\ &= Q(\bar{s}) + (a \mid b)(b' \mid a')^T + Q(\bar{s}') \\ &= \langle \bar{s},\ \bar{s}' \rangle_{\bar{E}} \neq 0, \end{aligned}$$

implying that $\bar{s}'' \notin \bar{S}$.

Therefore, for all $\bar{s}, \bar{s}' \in \bar{S}$ we have $\langle \bar{s},\ \bar{s}' \rangle_{\bar{E}} = 0$. Hence, $\bar{S}$ is totally isotropic. □

Next we show that, for all $e \in E$, e is diagonalizable. Let u_X, u_Z, and u_Y be the unitary matrices which diagonalize X, Z, and XZ, respectively, that is,

$$\begin{aligned} d_X &= u_X^* X u_X, \\ d_Y &= u_Y^* XZ u_Y, \\ d_Z &= u_Z^* Z u_Z. \end{aligned}$$

Then for $e = \otimes_{i=1}^{n} w_i$ in E, define $U_e \coloneqq \otimes_{i=1}^{n} u_{w_i}$, and so

$$\begin{aligned} U_e^* e U_e &= \big(\overset{n}{\underset{i=1}{\otimes}} u_{w_i}^* \big) \big(\overset{n}{\underset{i=1}{\otimes}} w_i \big) \big(\overset{n}{\underset{i=1}{\otimes}} u_{w_i} \big) \\ &= \overset{n}{\underset{i=1}{\otimes}} u_{w_i}^* w_i u_{w_i} \\ &= \overset{n}{\underset{i=1}{\otimes}} d_{w_i} \\ &= d_e. \end{aligned}$$

Thus we can diagonalize elements of E.

Definition 8.4 (Simultaneously diagonalizable)**.** Let $\{e_i\}_{i=1}^{k}$ be a set of self-adjoint operators on some Hilbert space H. Then the set $\{e_i\}_{i=1}^{k}$ is *simultaneously diagonalizable* if there exists a unitary operator U such that

$$U^* e_i U = d_i \,,$$

for all $i = 1, ..., k$, where d_i is some real diagonal matrix. In other words, the e_i's share a joint orthonormal eigenbasis.

Theorem 8.5. *Let $\{e_i\}_{i=1}^{k}$ be a set of self-adjoint operators on some Hilbert space H. Then the set $\{e_i\}_{i=1}^{k}$ is simultaneously diagonalizable if and only if $e_i e_j = e_j e_i$, for all $i, j = 1, ..., k$.*

For the proof see [6].

Then, since S is a commutative set of self-adjoint operators, it is simultaneously diagonalizable and thus each element $s \in S$ shares a joint orthonormal eigenbasis of $(\mathbb{C}^2)^{\otimes n}$.

By the following theorem, we take one of these eigenspaces to be our quantum error-correcting code.

Theorem 8.6. *Suppose that $\bar{S}$ is a k-dimensional totally singular subspace of $\bar{E}$. Let $\bar{S}^{\perp}$ be the subspace orthogonal to $\bar{S}$ with respect to the symplectic inner product $\langle \cdot\ ,\ \cdot \rangle_{\bar{E}}$ (that is, $\bar{S} \subseteq \bar{S}^{\perp}$). Further suppose that for any two elements e_1, e_2 in a quantum channel $\mathcal{E} \subseteq E$, either $\bar{e}_1\bar{e}_2 \in \bar{S}$ or $\bar{e}_1\bar{e}_2 \notin \bar{S}^{\perp}$. Then for any eigenspace C corresponding to $\bar{S}$ there exists an error-correcting operation $\mathcal{R}$ which corrects for the quantum channel $\mathcal{E}$ on C.*

Proof. Consider the element $\bar{s} \in \bar{S}$ with eigenvalue λ_s, where s is the associated representation. Then for any $|c\rangle \in C$ we have $s|c\rangle = \lambda_s|c\rangle$, and for any $e \in E$ we have

$$se|c\rangle = (-1)^{\langle \bar{s}\ ,\ \bar{e}\rangle_{\bar{E}}} es|c\rangle = (-1)^{\langle \bar{s}\ ,\ \bar{e}\rangle_{\bar{E}}} \lambda_s e|c\rangle.$$

Then, independent of $|c\rangle$, for any $\bar{e} \notin \bar{S}^{\perp}$ we get $\langle \bar{s}\ ,\ \bar{e}\rangle_{\bar{E}} = 1$. So, the action of e permutes the eigenspaces generated by the elements of s.

We proceed by splitting the proof into two cases, $\bar{e}_1\bar{e}_2 \in \bar{S}$ or $\bar{e}_1\bar{e}_2 \notin \bar{S}^{\perp}$. We begin by defining a projector P onto eigenspace C. Let the orthonormal basis for C be given by the set $\{|c_i\rangle\}_{i=1}^{k}$ and define P by

$$P \coloneqq \sum_{i=1}^{k} |c_i\rangle\langle c_i|.$$

Case 1: Suppose $\bar{e}_1\bar{e}_2 \in \bar{S}$. Then

$$\begin{aligned} Pe_1e_2P &= Pe_1e_2\Big(\sum_{i=1}^{k} |c_i\rangle\langle c_i|\Big) \\ &= P\Big(\sum_{i=1}^{k} e_1e_2|c_i\rangle\langle c_i|\Big) \\ &= P\Big(\sum_{i=1}^{k} \lambda_{e_1e_2}|c_i\rangle\langle c_i|\Big) \\ &= \lambda_{e_1e_2}P^2 \\ &= \lambda_{e_1e_2}P, \end{aligned}$$

where $\lambda_{e_1e_2}$ is a diagonal entry in the real diagonal matrix (thus, self-adjoint) given by the diagonalization of $e_1e_2 \in S$. Hence, any two elements $e_1, e_2 \in \mathcal{E}$, with $\bar{e}_1\bar{e}_2 \in \bar{S}$, are correctable.

Case 2: Suppose $\bar{e}_1\bar{e}_2 \notin \bar{S}^{\perp}$. Then for some $s \in S$ we have $se_1e_2 = -e_1e_2s$, so

$$se_1e_2|c_i\rangle = -e_1e_2s|c_i\rangle = -\lambda_s e_1e_2|c_i\rangle$$

implying that

$$e_1e_2|c_i\rangle \notin C.$$

In particular, $e_1e_2|c_i\rangle$ is in an eigenspace, C', which is orthogonal to C. Then we have

$$\begin{aligned} Pe_1e_2P &= Pe_1e_2\Big(\sum_{i=1}^{k} |c_i\rangle\langle c_i|\Big) \\ &= \sum_{i,j=1}^{k} |c_j\rangle\langle c_j|e_1e_2|c_i\rangle\langle c_i| \\ &= 0, \end{aligned}$$

since $\langle c_j|e_1e_2|c_i\rangle = 0$, for all i, j. ∎

We observe that if we have $\bar{e} \in \bar{S}^{\perp}$, $\bar{e} \neq 0$, then $se = es$, for all $s \in S$. In particular, $se|c_i\rangle = es|c_i\rangle = \lambda_i e|c_i\rangle$ so, $e|c_i\rangle \in C$. This shows that $\bar{S}^{\perp}$ permutes elements of C. Then $\bar{S}^{\perp}$ is analogous to classical errors which map codewords to codewords, that is, $\bar{S}^{\perp}$ is the set of non-trivial undetectable errors.

Corollary 8.7. *Suppose $\bar{S}$ is a k-dimensional linear subspace of $\bar{E}$ where $\bar{S} \subseteq \bar{S}^{\perp}$ with respect to the symplectic inner product. Suppose further that there are no vectors of weight less than d in $\bar{S}^{\perp} \setminus \bar{S}$. Then there exists a quantum-error-correcting code which can correct $(d-1)/2$ errors.*

Proof. Let $\mathcal{E} \subseteq E$ be the set of errors $e \in E$ with $w(\bar{e}) \leq (d-1)/2$. Then for any $\bar{e}_1$, $\bar{e}_2 \in \bar{E}$ we get

$$w(\bar{e}_1\bar{e}_2) \leq w(\bar{e}_1) + w(\bar{e}_2) \leq d - 1 < d$$

and thus,

$$\bar{e}_1\bar{e}_2 \notin \bar{S}^{\perp} \setminus \bar{S}.$$

This shows that either $\bar{e}_1\bar{e}_2 \in \bar{S}$, or $\bar{e}_1\bar{e}_2 \notin \bar{S}^{\perp}$. Thus, by the previous theorem, there is a quantum-error-correcting code which will correct any error $e \in \mathcal{E}$. Hence, there is a quantum-error-correcting code which will correct $(d-1)/2$ errors. □

The remainder of this discussion will be centred around two examples of quantum-error-correcting codes. In the first example we construct a quantum-error-correcting code from and existing classical binary error-correcting code, in the second example we discuss *the five qubit code*.

Example 8.8. Suppose we have a classical linear binary-error-correcting code $C \subset \mathbb{Z}_2^n$ which maps k bit messages into n bit codewords, and has minimum distance d. Further, suppose $C^{\perp} \subset C$, where $C^{\perp}$ is orthogonal to C with respect to the standard dot-product, $\cdot$, modulo 2. Then C corrects $t = \lfloor (d-1)/2 \rfloor$ errors in the classical setting. We can construct a quantum-error-correcting code from the linear code C as follows.

Define $\bar{S}$ to consist of all vectors $(\alpha_1|\alpha_2) \in \bar{E}$ with $\alpha_1, \alpha_2 \in C^{\perp}$. Then for $\beta_1, \beta_2 \in C$, we have that $(\beta_1|\beta_2)$ is in $\bar{E}$ and that for any $(\alpha_1|\alpha_2) \in \bar{S}$

$$\big\langle (\alpha_1|\alpha_2), (\beta_1|\beta_2) \big\rangle_{\bar{E}} = \alpha_1 \cdot \beta_2 + \alpha_2 \cdot \beta_1 = 0.$$

Thus the set consisting of vectors $(\beta_1|\beta_2) \in \bar{E}$ with $\beta_1, \beta_2 \in C$ is contained in $\bar{S}^{\perp}$.

$$\big\{ (\beta_1|\beta_2) \in \bar{E} \mid \beta_1, \beta_2 \in C \big\} \subseteq \bar{S}^{\perp}.$$

Now let $(\beta_1|\beta_2) \in \bar{S}^{\perp}$. Then, for all $(\alpha_1|\alpha_2) \in \bar{S}$, we have

$$\big\langle (\alpha_1|\alpha_2), (\beta_1|\beta_2) \big\rangle_{\bar{E}} = 0.$$

In particular, we may assume $\alpha_2 = 0 \in C^{\perp}$. Which implies that for all $\alpha_1 \in C^{\perp}$

$$\big\langle (\alpha_1|0), (\beta_1|\beta_2) \big\rangle_{\bar{E}} = \alpha_1\beta_2 = 0,$$

and thus,

$$\beta_2 \in (C^{\perp})^{\perp} = C.$$

Similarly, $\beta_1 \in C$. Thus,

$$\bar{S}^{\perp} \subseteq \big\{ (\beta_1|\beta_2) \in \bar{E} \mid \beta_1, \beta_2 \in C \big\}.$$

Therefore, we have $S^{\perp} = \big\{ (\beta_1|\beta_2) \in \bar{E} \mid \beta_1, \beta_2 \in C \big\}$. Then, since there is no vector in $\bar{S}^{\perp}$ with weight less than d, there exists a quantum-code capable of correcting up to t errors.

Example 8.9. Let C be a quantum code which maps 1 qubit into 5 quits and is composed of the two codewords

$$\begin{aligned}|c_0\rangle = |00000\rangle &\\ &+ |11000\rangle + |01100\rangle + |00110\rangle + |00011\rangle + |10001\rangle\\ &- |10100\rangle - |01010\rangle - |00101\rangle - |10010\rangle - |01001\rangle\\ &- |11110\rangle - |01111\rangle - |10111\rangle - |11011\rangle - |11101\rangle,\\ |c_1\rangle = |11111\rangle &\\ &+ |00111\rangle + |10011\rangle + |11001\rangle + |11100\rangle + |01110\rangle\\ &- |01011\rangle - |10101\rangle - |11010\rangle - |01101\rangle - |10110\rangle\\ &- |00001\rangle - |10000\rangle - |01000\rangle - |00100\rangle - |00010\rangle.\end{aligned}$$

Then the associated error group E is contained in $\mathcal{L}((\mathbb{C}^2)^{\otimes 5})$, and $\bar{E} = \mathbb{Z}_2^{10}$. Consider $\bar{e} = (11000|00101) \in \bar{E}$, corresponding to $e = \otimes_{k=1}^5 w_k \in E$. Then $Q(\bar{e}) = (11000)\cdot(00101) = 0$, and it easy to see that $e|c_0\rangle = |c_0\rangle$ and $e|c_1\rangle = |c_1\rangle$, that is, $|c_0\rangle, |c_1\rangle$ are in the $+1$-eigenspace of e. Notice that $|c_0\rangle, |c_1\rangle$ are fixed under cyclic permutations.

Then let $\pi : S_5 \to \mathcal{U}((\mathbb{C}^2)^{\otimes 5}) \subseteq \mathcal{L}((\mathbb{C}^2)^{\otimes 5})$ be defined by

$$\begin{aligned}\pi(\sigma)|\psi_k\rangle^{\otimes_{k=1}^5} &= \pi(\sigma)\big(|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \otimes |\psi_4\rangle \otimes |\psi_5\rangle\big)\\ &= |\psi_{\sigma^{-1}(1)}\rangle \otimes |\psi_{\sigma^{-1}(2)}\rangle \otimes |\psi_{\sigma^{-1}(3)}\rangle \otimes |\psi_{\sigma^{-1}(4)}\rangle \otimes |\psi_{\sigma^{-1}(5)}\rangle,\end{aligned}$$

where S_5 is the symmetric group on 5 symbols and $\mathcal{U}((\mathbb{C}^2)^{\otimes 5})$ is the group of unitary operators on $(\mathbb{C}^2)^{\otimes 5}$. Then, restricting π to the subgroup of cyclic permutations $C_5 \subset S_5$, we get

$$\pi(\sigma)|c_i\rangle = |c_i\rangle,$$

for all $\sigma \in C_5$, $i = 0, 1$. In particular,

$$\begin{aligned}|c_i\rangle &= \pi(\sigma)e\pi^{-1}(\sigma)|c_i\rangle\\ &= \pi(\sigma)e\pi^{-1}(\sigma)\sum_{j=1}^{16}\alpha_j|\psi_k\rangle_{j_i}^{\otimes_{k=1}^5}\\ &= \pi(\sigma)e\sum_{j=1}^{16}\alpha_j|\psi_{\sigma(k)}\rangle_{j_i}^{\otimes_{k=1}^5}\\ &= \pi(\sigma)\sum_{j=1}^{16}\alpha_j\big(w_k|\psi_{\sigma(k)}\rangle_{j_i}\big)^{\otimes_{k=1}^5}\\ &= \sum_{j=1}^{16}\alpha_j\big(w_{\sigma^{-1}(k)}|\psi_k\rangle_{j_i}\big)^{\otimes_{k=1}^5}\\ &= \big(\bigotimes_{k=1}^5 w_{\sigma^{-1}(k)}\big)|c_i\rangle,\end{aligned}$$

for all $\sigma \in C_5$, $i = 0, 1$. Thus, $|c_0\rangle, |c_1\rangle$ are fixed under all cyclic permutations of e. Using these permutations as generators, we can construct a subspace $\bar{S} \subset \bar{E}$ which by Proposition 8.3 is totally isotropic. Then $\bar{S}$ corresponds to an abelian group $S \subseteq E$ which fixes $|c_0\rangle$, $|c_1\rangle$.

Then $\bar{S}$ is the 4-dimensional totally singular subspace generated by

$$(11000|00101)$$
$$(01100|10010)$$
$$(00110|01001)$$
$$(00011|10100)$$

The fifth permutation is left out of the generators since only four permutations of e are linearly independent. Then $\bar{S}^{\perp}$ is generated by $\bar{S}$ and the additional vectors $(11111|00000)$, $(00000|11111)$. It is straightforward to check that the minimum weight in $\bar{S}$ is $d = 3$. Thus, by Corollary 8.7 there exists a quantum-error-correcting operation which can correct up to 1 error.

This geometric formalism presented by Calderbank et al. [1] has also been used to describe important error-correcting codes, such as Shor's *nine qubit code*, and codes arising from the stabilizer formalism (see *Section 10.5* of [3]). For further reading see [1], [2], [3], and [4].

References

[1] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane; *Quantum Error Correction and Orthogonal Geometry.* Physical Review Letters. Vol. 78, No. 3, (1996), 405-407.

[2] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane; *Quantum Error Correction Via Codes Over GF(4).* IEEE Transactions on Information Theory, Vol. 44, No. 4, (July 1998), 1369-1387.

[3] Nielsen, M. and Chuang, I.; *Quantum Computation and Quantum Information.* Tenth Edition, Cambridge University Press, (2010).

[4] Paulsen; W 2016, *Section 4: Theory of CP maps*, Corollary 4.13, lecture notes, Entanglement and non-locality, University of Waterloo.

[5] Choi, Man Duen; *Completely positive linear maps on complex matrices.* Linear Algebra and Appl. 10 (1975), 285-290. 15A60 (46L05)

[6] Hoffman, K. and Kunze, R.A., *Linear Algebra*, Section 9.5, Prentice-Hall, (1971).

E-mail address: Alex.Conlon@gmail.com