Quantum Error Correcting Codes: An introduction

Piyush P Kurur
Department of Computer Science and Engineering
Indian Institute of Technology Kanpur,
Kanpur, Uttar Pradesh, India
email:ppk@cse.iitk.ac.in *

Abstract

The aim of this article is to introduce the theory of quantum error correction codes. Starting with classical codes we build the necessary mathematical machinery to construct and analyse quantum codes. We will look at codes over the Hilbert space $L^2(A)$ for some additive abelian group A and use the Weyl operators U_a and V_b to describe errors. We quickly specialise to special codes called stabiliser codes and look at stabiliser codes over finite fields. We also give quantum algorithm for error correction in the case of stabiliser codes.

Key words: Quantum codes, Weyl Operators, stabiliser codes.

1 Introduction

The basic problem of communication is the following: There are two entities, the sender and the receiver. From time to time the sender wishes to send information to the receiver. For this they are provided with a noisy channel. To set up reliable communication over this inherently noisy channel, we incorporate enough redundancy so that even if few errors occur during transmission, the receiver is able to detect and sometimes correct these errors. The goal of classical error correction is to design efficient encoding and decoding methods. For an introduction the reader may consult [4].

The aim of this article is to introduce the subject of quantum error correcting codes. Here the sender and receiver are quantum entities and the channel is a quantum channel. It may appear that classical techniques will not help in this situation because of some of the strange properties of quantum system like the non-cloning theorem. However this is not the case. Starting with classical codes we build up the mathematical machinery for constructing and analysing quantum codes, in the process show how remarkably similar their theory is. We quickly specialise to the beautiful theory of stabiliser codes. We also give a description of error correcting algorithm for stabiliser codes.

*The author was a Ph.D student at the Institute of Mathematical Sciences when this tutorial lecture was given as part of QICC 2005, IIT Kharagpur

2 Classical Error correction

We begin with a brief overview of classical error correcting codes. An *alphabet* is a finite set Σ of *letters*. A *word* of length n over an alphabet Σ is an element of Σ^n. Any channel comes with an underlying alphabet. Letters of the alphabet are the smallest unit of information that can be sent across the channel. Due to *noise*, during the transmission some of the letters get corrupted.

Assume that we have a sender who, from time to time, sends one of the messages $M_1, \ldots, M_k$ to a receiver through a channel C. There is an encoding procedure which is agreed upon by both the sender and receiver — a set of words $\mathbf{w}_1, \ldots, \mathbf{w}_k$ over the underlying alphabet of the channel, all of which we assume are of length n, are chosen such that the sender sends $\mathbf{w}_i$ whenever he wishes to send M_i. However, since the channel is not ideal, errors creep in. Our task is to find a subset $\mathcal{C} \subseteq \Sigma^n$ of size k such that for certain number of errors the receiver can detect (or sometimes correct) it. Such a set $\mathcal{C}$ is called a code and n is the length of the code.

We now make some simplifying assumptions. We will assume, without loss of generality, that Σ is an additive abelian group $(A, +, 0)$. Words of length n are now elements of the additive abelian group A^n. Errors now become additive errors — suppose a word $\mathbf{u}$ is sent and a word $\mathbf{v}$ is received then we can think of the channel adding an error of $\mathbf{e} = \mathbf{v} - \mathbf{w}$. We now define a metric structure on A^n.

Definition 2.1 (Hamming Distance)**.** Given words $\mathbf{u} = u_1 \ldots u_n$ and $\mathbf{v} = v_1 \ldots v_n$ in A^n the *Hamming distance*, $d(\mathbf{u}, \mathbf{v})$, is the number of positions i such that $u_i \neq v_i$. For an element $\mathbf{u} = u_1 \ldots u_n$, the weight $w(\mathbf{u})$ is $\#\{u_i : u_i \neq 0\}$.

Note that $d(\mathbf{u}, \mathbf{v}) = w(\mathbf{u} - \mathbf{v})$.

An error that effects t positions is nothing but an additive error of weight t. We are interested in codes $\mathcal{C} \subset A^n$ that can tolerate t-errors. For a code $\mathcal{C}$ we define the distance $d(\mathcal{C})$ to be $\min\{d(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in \mathcal{C} \text{ and } \mathbf{u} \neq \mathbf{v}\}$ One has the following theorem.

Theorem 2.2. *A code of minimal distance d can* detect $d-1$ *errors and* correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ *errors.*

Proof sketch. An additive error of weight less than d will not take a valid code word to another codeword. So one can detect an error that corrupts at most $d-1$ positions.

Decoding is done using nearest neighbour algorithm: Given a word output the nearest code word. This will work provided at most $\left\lfloor \frac{d-1}{2} \right\rfloor$ positions are corrupted. This is because if we consider balls of radius less than $\left\lfloor \frac{d-1}{2} \right\rfloor$ then none of the balls intersect. □

3 Quantum error correcting code

We saw that for classical channels there is an underlying alphabet, elements of which are the smallest units of information that can be sent. In the case of quantum channel the analogous entity is a finite dimensional Hilbert space $\mathcal{H}$. Again with out loss of

generality we assume that the Hilbert space $\mathcal{H}$ is $L^2(A)$, the space of functions from an additive abelian group $(A, +, 0)$ to $\mathbb{C}$. This space is nothing but a finite dimensional Hilbert space with orthonormal basis $|a\rangle$, $a \in A$. Vectors in $L^2(A)$ are analogous to letters in the classical setting. Naturally "quantum word" of length n should be elements of the tensor product $L^2(A)^{\otimes^n}$. For a word $\mathbf{w} = w_1 \dots w_n$ in A^n we will use $|\mathbf{w}\rangle$ to denote the vector $|w_1\rangle \otimes \dots \otimes |w_n\rangle$. Thus $\{|\mathbf{w}\rangle : \mathbf{w} \in A\}$ gives a orthonormal basis for $L^2\left(A\right)^{\otimes^n}$. A quantum code is a subspace $\mathcal{C}$ of $L^2\left(A\right)^{\otimes^n}$.

The sender and receiver are quantum entities and the channel is a quantum channel. The messages that the sender wishes to send come from a finite dimensional Hilbert space $\mathcal{H}_M$ with orthonormal basis $|0\rangle, \dots, |k\rangle$. As before the sender and receiver agrees upon a code $\mathcal{C}$ with orthonormal basis say $|\psi_0\rangle, \dots, |\psi_k\rangle$. To send $|i\rangle$ the sender transmits $|\psi_i\rangle$. What if the sender wishes to send an arbitrary unit vector $|\phi\rangle$ in $\mathcal{H}_M$? He just extend the encoding process linearly. In other words if $|\phi\rangle = \sum \alpha_i |i\rangle$ then the sender transmits $\sum \alpha_i |\psi_i\rangle$.

4 Quantum errors and Weyl Operators

In the classical setting the only errors were the so called position errors. Errors were elements of A^n that acted additively on words. In the quantum setting we have to worry about two types of error, position errors and phase errors. These errors are best explained using Weyl Operators.

First position errors. Consider the unitary operator U_x, $x \in A$, defined by $U_x |a\rangle = |a + x\rangle$ for all $a \in A$. These operators corresponds to position errors. To understand phase errors we have to look at characters of A.

Given an abelian group $(A, +, 0)$ we consider its group of characters $(\hat{A}, ., 1)$. Let χ_1 and χ_2 be two homomorphisms from A to the unit circle $S^1 = \{z : z \in \mathbb{C} \text{ and } |z| = 1\}$. Define the product $\chi_1.\chi_2$ to be the homomorphism that maps $a \in A$ to $\chi_1(a)\chi_2(a)$. The set of all such homomorphisms together with the product forms an abelian group $(\hat{A}, ., 1)$ which is called the group of characters of A.

The character group $\hat{A}$ is isomorphic to A. We now define an explicit isomorphism between A and $\hat{A}$. Let A be an additive abelian group. By the fundamental theorem of finite abelian group there exists $h_1, \dots, h_k \in A$ of orders $r_1, \dots, r_k$ respectively such that every element of a of A can be expressed as a sum $x_1h_1 + \dots + x_kh_k$, $0 \leq x_i < r_i$. Fix a basis $h_1, \dots, h_k$ for A. For any positive integer n let $\zeta_n = e^{\frac{2\pi\iota}{n}}$ be the primitive n^{th} root of unity. Consider an element $a = \sum x_ih_i$ of A. We define the element $\chi_a \in \hat{A}$ as follows:

$$\chi_a\left(\sum_{i=1}^{k} y_ih_i\right) = \prod_{i=1}^{k} \zeta_{r_i}^{x_i.y_i}.$$

The map $a \mapsto \chi_a$ is an isomorphism from the additive group A to the multiplicative group $\hat{A}$. There is nothing canonical about the isomorphism $a \mapsto \chi_a$. It depends on the basis we have chosen for A. From now on when we talk about χ_a we take for granted

that an isomorphism from A to $\hat{A}$ has been fixed and χ_a is the image of a under this isomorphism.

An important property of characters is the so called Schur's orthogonality property.

Lemma 4.1 (Schur's Orthogonality)**.**

$$\sum_{x\in A}\chi_x(a) = \begin{cases} 0 \text{ if } a \neq 0 \\ \#A \text{ otherwise} \end{cases} \tag{1}$$

$$\sum_{x\in A}\chi_a(x) = \begin{cases} 0 \text{ if } a \neq 0 \\ \#A \text{ otherwise} \end{cases} \tag{2}$$

Here are some properties of characters that will be useful

Proposition 4.2. *1.* $\chi_a \cdot \chi_b = \chi_{a+b}$,

2. $\chi_a(b) = \chi_b(a)$,

3. $\chi_a^{-1} = \overline{\chi}_a = \chi_{-a}$.

We now define the unitary operator V_a as follows : $V_a|b\rangle = \chi_a(b)|b\rangle$. The operators U_a and V_b are called Weyl operators and satisfies the Weyl commutation relation: $\chi_a(b)U_aV_b = V_bU_a$. We extend the Weyl operators to $L^2(A)^{\otimes^n}$ as follows. For any word $\mathbf{a} = a_1 \ldots a_n$, $U_{\mathbf{a}}$ is the tensor product $U_{a_1}\otimes\ldots\otimes U_{a_n}$. Similarly $V_{\mathbf{a}}$ is the tensor product $V_{a_1}\otimes\ldots\otimes V_{a_n}$.

Fourier transforms and Phase errors

To make phase errors $V_{\mathbf{b}}$ look less mysterious, we show that there is a natural interpretation of phase errors as position errors in the Fourier basis. Consider a character $\chi \in \hat{A}$. Define the vector $|\chi\rangle$ in $L^2(A)$ as follows: $|\chi\rangle = \frac{1}{\sqrt{\#A}}\sum_{a\in A}\chi(a)|a\rangle$. Using Schur's orthogonality we can show that $\{|\chi_a\rangle : a \in A\}$ also forms a orthonormal basis for $L^2(A)$. It is also easy to verify the following proposition $V_a|\chi_b\rangle = |\chi_{a+b}\rangle$. This shows that V_a is nothing but position errors in the Fourier basis.

The unitary map F that performs the basis change $|a\rangle \mapsto |\chi_a\rangle$ is called the *Fourier transform* which we denote by F. It is easy to see that $F^\dagger V_a F = U_a$. If the abelian group A is the field $\mathbb{F}_2$ then the Fourier transform is the so called Hadamard matrix. We denote the unitary matrix $\overbrace{F\otimes\ldots\otimes F}^{n}$, the Fourier transform on $L^2(A)^{\otimes^n}$, by F_n. It is easy to see that $F_n^\dagger V_{\mathbf{a}} F_n = U_{\mathbf{a}}$.

5 The Error Group

Consider the Hilbert space $\mathcal{H} = L^2(A)$. Let $\mathcal{B}(\mathcal{H})$ denote the space of linear operators on $\mathcal{H}$. The set $\mathcal{B}(\mathcal{H})$ is itself a Hilbert space with inner product $\langle A, B\rangle$ defined as $\mathrm{Tr}(A^\dagger B)$.

Together with operator composition, which will be the multiplication, $\mathcal{B}(\mathcal{H})$ forms a ring (or in mathematical jargon a C^*-algebra). Unitary operators form a multiplicative subgroup of $\mathcal{B}(\mathcal{H})$. The subgroup of unitary operators generated by the Weyl operators $\{U_a V_b : a, b \in A\}$ is called the *error group* of the Hilbert space $\mathcal{H}$. The importance of the error group comes form the following proposition.

Proposition 5.1. *The error group $\mathcal{E}(\mathcal{H})$ forms an orthonormal basis for $\mathcal{B}(H)$*

The error group of $L^2(A)^{\otimes^n}$ is the group generated by $\{U_{\mathbf{a}} V_{\mathbf{b}} : \mathbf{a}, \mathbf{b} \in A^n\}$.

Let $\mathcal{E}$ be the error group of $L^2(A)^{\otimes^n}$. Our model of quantum communication is as follows. The sender sends a message $|\phi\rangle$. The noise is modelled as an unknown $U \in \mathcal{E}$ that gets applied to $|\phi\rangle$. Recall that a quantum code $\mathcal{C}$ is a subspace of $L^2(A)^{\otimes^n}$. Given a subset $\mathcal{A} \subseteq \mathcal{E}$ an $\mathcal{A}$-error correcting code is a quantum code that corrects errors arising from the set $\mathcal{A}$, i.e. there should be a unitary operator U acting on $L^2(A)^{\otimes^n} \otimes \mathbb{C}^{2^{\otimes^m}}$, for sufficiently large m, such that for any vector $|\psi\rangle$ in $\mathcal{C}$ and $U_{\mathbf{a}} V_{\mathbf{b}} \in \mathcal{A}$ we have

$$U(U_{\mathbf{a}} V_{\mathbf{b}} |\psi\rangle) \otimes |0^m\rangle = |\psi\rangle \otimes |\phi_{\mathbf{a},\mathbf{b}}\rangle .$$

The following criteria know as the Knill-Laflamme criteria can be used to check when a code $\mathcal{C}$ is a $\mathcal{A}$-error correcting code [3].

Theorem 5.2 (Knill-Laflamme theorem)**.** *Let $\mathcal{C}$ be a code with an orthonormal basis $|\psi_0\rangle, \ldots, |\psi_k\rangle$. Let $\mathcal{A}$ be a subset of the error group then $\mathcal{C}$ is an $\mathcal{A}$-error correcting code if and only if for all $0 \leq i, j \leq k$ and $U, V \in \mathcal{A}$ we have*

$$\langle\psi_i| U^\dagger V |\psi_j\rangle = \begin{cases} 0 \text{ if } i \neq j \\ \Gamma(U^\dagger V) \text{ otherwise} \end{cases}$$

where $\Gamma(UV)$ is a function of UV independent of i and j.

Proof sketch. Let $|\psi_i\rangle$, $1 \leq i \leq n$ be a basis for $\mathcal{C}$. Let $\mathcal{A} = \{U_1, \ldots U_M\}$. Let $\mathcal{H}_i$ be the subspace spanned by $U_r |\psi_i\rangle$, $1 \leq r \leq M$. Let $|\psi_{ij}\rangle$, $1 \leq j \leq n_i$, be an orthonormal basis for $\mathcal{H}_i$.

To prove that the condition is sufficient note that for $i \neq j$, $\mathcal{H}_i$ is orthogonal to $\mathcal{H}_j$. There exists a unitary operator acting on $L^2(A)^{\otimes^n} \otimes \mathbb{C}^{2^{\otimes^m}}$, for some suitable m such that $U |\psi_{ij}\rangle \otimes |0^m\rangle = |\psi_i\rangle \otimes |j\rangle$. This is the error correction operator.

To prove that the condition is necessary we assume that there is a error correction operator U acting on $L^2(A)^{\otimes^n} \otimes \mathbb{C}^{2^{\otimes^m}}$ such that for each $|\psi\rangle \in \mathcal{C}$ and $U_r \in \mathcal{A}$ we have

$$U(U_r |\psi\rangle) \otimes |0^m\rangle = |\psi\rangle \otimes |\phi_r\rangle .$$

We want to compute $\langle\psi_i| U_r^\dagger U_s |\psi_j\rangle$. Note that

$$\langle\psi_i| U_r^\dagger U_s |\psi_j\rangle = (\langle 0^m| \otimes \langle\psi_i| U_r^\dagger)(U_s |\psi_j\rangle \otimes |0^m\rangle).$$

Since unitary operators preserve inner products we have

$$\langle\psi_i| U_r^\dagger U_s |\psi_j\rangle = (\langle\phi_r| \otimes \langle\psi_i|)(|\psi_j\rangle \otimes |\phi_s\rangle) = \langle\psi_i|\psi_j\rangle \langle\phi_r|\phi_s\rangle .$$

This above expression is 0 if $i \neq j$ and is independent of i (is equal to $\langle\phi_r|\phi_s\rangle$) if $i = j$. □

Intuitively two different basis $|\psi_i\rangle$ and $|\psi_j\rangle$ under errors U and V should continue to remain orthogonal for error correction to be possible.

Remark. Let $\mathcal{C}$ be a code that can correct errors arising from the subset $\mathcal{A} = \{U_1, \ldots, U_M\}$. From the proof the Knill-Laflamme theorem we can assume a stronger condition on the error correcting algorithm (unitary operator). We can assume that there is a unitary operator U acting on $L^2(A)^{\otimes^n} \otimes \mathbb{C}^{2^{\otimes^m}}$ such that $U(U_r |\psi\rangle) \otimes |0^m\rangle = |\psi\rangle \otimes |r\rangle$ for all $|\psi\rangle$ in $\mathcal{C}$. From now on we will assume this stronger definition of error correcting operator.

To complete the analogy between classical error correction we also define error detection.

Definition 5.3. Let $\mathcal{C}$ be a quantum code with basis $|\psi_0\rangle, \ldots, |\psi_k\rangle$. We say that $\mathcal{C}$ can *detect* error $U \in \mathcal{E}$ if for all $0 \leq i, j \leq k$ we have

$$\langle\psi_i| U |\psi_j\rangle = \begin{cases} 0 \text{ if } i \neq j \\ \Gamma(U) \text{ otherwise} \end{cases}$$

The intuition behind the definition is similar to that of the classical case. We want $U|\psi\rangle$ be orthogonal to all ψ_i for the error to be detected. It is easy to see from Theorem 5.2 that $\mathcal{C}$ is a $\mathcal{A}$-error correcting code if and only if it is a $\mathcal{A}^\dagger\mathcal{A}$-error detecting code.

We now want to rephrase the Knill-Laflamme criteria in terms of the projection operator. Since any code is a subspace there is an associated projection operator P. The Knill-Laflamme criteria becomes

Theorem 5.4 (Knill-Laflamme)**.** *Let $\mathcal{C}$ be a code with P as its associated projection operator. The $\mathcal{C}$ is a $\mathcal{A}$-error correcting code if for all U and V in $\mathcal{A}$ we have $PU^\dagger VP = \Gamma(U^\dagger V)P$.*

Let $\mathcal{C}$ be a quantum code. The set of error operators detected by $\mathcal{C}$, denoted by $\mathcal{D}(\mathcal{C})$, is the set

$$\mathcal{D}(\mathcal{C}) = \{U \in \mathcal{E} | PUP = \Gamma(U)P\}.$$

Note that $\mathcal{C}$ is a $\mathcal{A}$-correcting quantum code if and only if $\mathcal{A}^\dagger\mathcal{A} \subseteq \mathcal{D}(\mathcal{C})$.

Let $(\mathbf{a}, \mathbf{b}) \in A^n \times A^n$. We define the combined weight (which we will abbreviate as weight) as

$$w(\mathbf{a}, \mathbf{b}) = \#\{i | (a_i, b_i) \neq (0, 0)\}$$

For $t \leq n$ define $\mathcal{A}_t$ to be the subset $\{U_\mathbf{a} V_\mathbf{b} | w(\mathbf{a}, \mathbf{b}) \leq t\}$. A t-error correcting code is an $\mathcal{A}_t$-error correcting code. Given a quantum code C with projection operator P. By *distance* of $\mathcal{C}$, written $d(\mathcal{C})$ we mean the largest integer d such that $\mathcal{D}(\mathcal{C}) \supseteq \mathcal{A}_{d-1}$. Analogous to Theorem 2.2 in the classical setting we have the following theorem.

Theorem 5.5. *A quantum code $\mathcal{C}$ of distance d can detect $d-1$ errors and correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.*

Sometimes it is more natural to use the projection operators while talking about a quantum code. Consider a quantum code $\mathcal{C}$. Let P be the corresponding projection operator. Often when P is more natural to the discussion we will use P instead of $\mathcal{C}$. For example we may use $\mathcal{D}(P)$ to denote the set of errors detected by $\mathcal{C}$ (i.e. the set $\mathcal{D}(\mathcal{C})$). Similarly we may use $d(P)$ to denote the distance of $\mathcal{C}$.

6 The Calderbank-Shor-Stean code

We now give an example of a quantum error correcting code. This family is the so called Calderbank-Shor-Stean code or the CSS code for short. We pick two classical linear codes C_1 and C_2 such that $C_2 \subseteq C_1$.[1]

We first describe what linear codes. Fix a finite field $\mathbb{F}$ say $\mathbb{F}_2$. A linear code C of length n is a subspace of $\mathbb{F}^n$. A linear code C is a $[n, k, d]$ code if C is a subspace of $\mathbb{F}^n$ of dimension k and distance d. The minimal distance of a code is given by $d(C) = \min\{w(\mathbf{w}) : \mathbf{w} \in C\}$.

For a code C let $C^\perp$ denote the orthogonal complement of $\mathbb{F}^n$. Let P be the projection operator into the vector space $C^\perp$. Then P usually called the *parity check matrix* for C. Note that $P\mathbf{u} = 0$ for all code words $\mathbf{u} \in C$.

The nearest neighbour decoding procedure of linear codes is quite elegant. On receiving a word $\mathbf{m}$ we want to decode it to the nearest code word. Let $\mathbf{u}$ be the nearest code word and let $\mathbf{e} = \mathbf{m} - \mathbf{u}$. Since P annihilates $\mathbf{u}$ we have $\mathbf{e} = P\mathbf{m}$. We output the code word $\mathbf{u}$ by going over all words in C an outputting the nearest codeword to $\mathbf{e}$. For a message $\mathbf{m}$ the word $\mathbf{e} = P\mathbf{m}$ is called the *syndrome*. Often there are much more elegant algorithm to find the nearest codeword to the syndrome than the boring brute force algorithm. A challenging task is to come up with efficient codes where the brute force algorithm can be avoided.

We are now ready to describe the CSS construction for classical codes C_1 and C_2 over $\mathbb{F}_q$ such that $C_2 \subseteq C_1$. If C_1 is an $[n, k_1]_q$ code and C_2 is an $[n, k_2]_q$ code then the constructed quantum code will be a $q^{k_1-k_2}$ dimensional code. Also if C_1 and $C_2^\perp$ can correct t errors then the constructed code can also correct t quantum errors.

Consider the coset group C_1/C_2. For a coset $x + C_2$ of C_2 in C_1 define $|x + C_2\rangle$ as follows

$$|\mathbf{x} + C_2\rangle = \frac{1}{\sqrt{\#C_2}} \sum_{\mathbf{y} \in C_2} |\mathbf{x} + \mathbf{y}\rangle .$$

Consider an error $E = U_{\mathbf{a}} V_{\mathbf{b}}$ such that $w(\mathbf{a})$ and $w(\mathbf{b})$ are less than t. The error E on $|\mathbf{x} + C_2\rangle$ will give the following vector

[1] The CSS construction can be carried out for groups codes C_1 and C_2 over the alphabet. We leave this as an exercise for the reader.

$$E\left|\mathbf{x}+C_2\right\rangle = \frac{1}{\sqrt{\#C_2}}\sum_{\mathbf{y}\in C_2}\chi_{\mathbf{b}}(\mathbf{x}+\mathbf{y})\left|\mathbf{x}+\mathbf{y}+\mathbf{a}\right\rangle$$

The error correction is done in two stages. First the position errors are corrected and then the phase errors. Let H_1 and H_2 be the parity check matrix of C_1 and $C_2^{\perp}$ respectively. Let $\mathbf{z}\in\mathbb{F}^n$ be any vector. We define the following unitary matrix

$$U_p\left|\mathbf{z}\right\rangle\otimes\left|\mathbf{w}\right\rangle = \left|\mathbf{z}\right\rangle\left|\mathbf{w}+H_1\mathbf{z}\right\rangle$$

The unitary matrix U_p writes down the syndrome in the ancilla register which can now be used to correct error. The classical algorithm for the code C_1 can be used to correct the position error by measuring the ancilla. This gives the vector

$$\frac{1}{\sqrt{\#C_2}}\sum_{\mathbf{y}\in C_2}\chi_{\mathbf{b}}(\mathbf{x}+\mathbf{y})\left|\mathbf{x}+\mathbf{y}\right\rangle$$

Now to correct the phase errors we can use the error correcting properties of $C_2^{\perp}$. We will use the fact that phase errors are position errors in Fourier domain. Applying the Fourier transform we get (I neglect the normalising factor)

$$\sum_{\mathbf{y}\in C_2}\chi_{\mathbf{b}}(\mathbf{x}+\mathbf{y})\sum_{\mathbf{z}}\chi_{\mathbf{z}}(\mathbf{x}+\mathbf{y})\left|\mathbf{z}\right\rangle.$$

This can be rewritten as

$$\sum_{\mathbf{w}}\left(\sum_{\mathbf{y}\in C_2}\chi_{\mathbf{y}}(\mathbf{w})\right)\chi_{\mathbf{x}}(\mathbf{w})\left|\mathbf{w}-\mathbf{b}\right\rangle. \tag{3}$$

Now $\left(\sum_{\mathbf{y}\in C_2}\chi_{\mathbf{y}}(\mathbf{w})\right)$ is 0 unless $\mathbf{w}\in C_2^{\perp}$ in which case it is $\#C_2$. The state is Equation 3 becomes

$$\sum_{\mathbf{w}\in C_2^{\perp}}\chi_{\mathbf{x}}(\mathbf{w})\left|\mathbf{w}-\mathbf{b}\right\rangle.$$

This is as if a position error of $-\mathbf{b}$ has occurred. Using the error correcting properties of C_2 we can correct the error $\mathbf{b}$ just like the previous case. Applying the inverse Fourier transform we get be error corrected state.

7 Error correction in the general setting

A more general model of error correction is given through the density matrix formalism for quantum computation. For a quantum channel there is an underlying Hilbert space $\mathcal{H}$. We assume that the sender send a state ρ. On sending a state ρ the receiver gets a

state $\sum L_i^\dagger \rho L_i$ where L_i's come from the some subspace $\mathcal{A}$ of $\mathcal{B}(\mathcal{H})$ such that $\sum L_i^\dagger L_i$ is identity.

Consider n-fold tensor product $\mathcal{H}^{\otimes^n}$. A n sized code is a subspace of $\mathcal{H}^{\otimes^n}$. We say that $\mathcal{C}$ is a $\mathcal{A}$-error correcting code if there exists a set of operators $M_1, \ldots, M_n$ such that for any collection $L_1, \ldots, L_r$ of operators in $\mathcal{A}$ with the property that $\sum L_i^\dagger L_i = I$, we have

$$\sum_{i,j} M_i^\dagger L_j^\dagger \rho L_j M_i = \rho$$

for any state ρ with support in $\mathcal{C}$.

We now formalise t-error correcting codes in this model. We define the subspace $\mathcal{A}_t$ of $\mathcal{B}\left(\mathcal{H}^{\otimes^n}\right)$ to be the span of operators L which are of the form $L_1 \otimes \ldots \otimes L_n$, $L_i \in \mathcal{B}(\mathcal{H})$ where all but t of the L_i's are identity operator.

How does this model of error compare with whatever we have been talking about in the previous sections ? Is it sufficient to concentrate only on errors of the form $U_{\mathbf{a}}V_{\mathbf{b}}$? We show that indeed this is the case.Without loss of generality we will assume that the Hilbert space $\mathcal{H}$ is $L^2(A)$ for some additive abelian group A. We make use of the following theorem for Weyl operators.

Theorem 7.1. *The collection of operators $\{U_a V_b : a, b \in A\}$ forms an orthonormal basis for the space $\mathcal{B}\left(L^2(A)\right)$. Moreover an orthonormal basis for $\mathcal{B}\left(L^2(A)^{\otimes^n}\right)$ is given by $\{U_{\mathbf{a}}V_{\mathbf{b}} : \mathbf{a}, \mathbf{b} \in A^n\}$.*

It follows from Theorem 7.1 that the space $\mathcal{A}_t$ of t-errors is spanned by $U_{\mathbf{a}}V_{\mathbf{b}}$ for $\mathbf{a}, \mathbf{b} \in A^n$ of weight $w(\mathbf{a}, \mathbf{b}) \leq t$. Consider a t-error correcting code $\mathcal{A}$ as defined in Subsection 5. There is an error correcting algorithm that we modelled as a unitary operator U. Consider a collection of errors L_i coming form $\mathcal{A}_t$. Each L_i can be written as a combination of $U_{\mathbf{a}}V_{\mathbf{b}}$. Since U corrects each of the error $U_{\mathbf{a}}V_{\mathbf{b}}$, it can correct any linear combination of these errors. Hence it is sufficient to concentrate on the Weyl operators while designing codes. General errors, which are just linear combinations of these operators, will automatically be corrected by linearity.

There is an alternate way of looking at the above mentioned error model. The sender sends a state ρ. Since the channel is not completely isolated from the environment, which we model as a Hilbert space $\mathcal{H}_{\text{env}}$, an unknown unitary operator U acts on the combined system $\mathcal{H} \otimes \mathcal{H}_{\text{env}}$. However the receiver has access only to the $\mathcal{H}$ portion of the combined system and as a result the state he receives is that which is obtained by tracing out the $\mathcal{H}_{\text{env}}$ portion of the state. It can be shown that these formalisms are equivalent. Also if $\mathcal{H}$ is of dimension d, it is sufficient to consider environments of dimension at most d^2. This model, in some sense, is more satisfying from the physics point of view and turns out to be equivalent to the operator formalism.

In view of the discussion we had is this section, we will consider only errors of the type $U_{\mathbf{a}}V_{\mathbf{b}}$ while designing codes. This simplifies the process of constructing and analysing quantum codes.

8 Stabiliser codes

There are certain quantum codes called stabiliser codes that have a neat description. As before the underlying Hilbert space is $L^2(A)$ for some additive abelian group A. Codes of length n are subspaces of $L^2(A)^{\otimes^n}$. We will use $\mathcal{E}$ to denote the error group associated with the $L^2(A)^{\otimes^n}$.

Consider a subset $\mathcal{A} \subseteq \mathcal{E}$. Let $\mathcal{C}$ be the subset of vectors of $L^2(A)^{\otimes^n}$ that are stabilised by $\mathcal{A}$, i.e. set of all $|\psi\rangle$ in $L^2(A)^{\otimes^n}$ such that $U|\psi\rangle = |\psi\rangle$ for all $U \in \mathcal{A}$. It can be easily verified that $\mathcal{C}$ forms a subspace of $L^2(A)^{\otimes^n}$. Moreover $\mathcal{C}$ is stabilised by all the elements in the subgroup of $\mathcal{E}$ generated by $\mathcal{A}$. Codes that arise as subspaces stabilised by a subgroup $\mathcal{S}$ of $\mathcal{E}$ are called *stabiliser codes* (or sometimes *additive codes*). Let $\mathcal{S}$ be a subgroup of $\mathcal{E}$. We will use $\mathcal{C}_\mathcal{S}$ to denote the stabilised subspace of $\mathcal{S}$. Elements of $\mathcal{S}$ are of the form $\zeta U_\mathbf{a} V_\mathbf{b}$ for some root of unity ζ. Not all subgroups of $\mathcal{E}$ lead to nontrivial codes. We now look at conditions that $\mathcal{S}$ should satisfy so that $\mathcal{C}_\mathcal{S}$ is nontrivial.

Theorem 8.1. *Let $\mathcal{S}$ be a subgroup of the error group $\mathcal{S}$ and let $\mathcal{C}_\mathcal{S}$ be the stabiliser code corresponding to it. For $\mathcal{C}_\mathcal{S}$ to be nontrivial $\mathcal{S}$ should satisfy the following conditions:*

1. *For any nontrivial root of unity ζ, $\zeta I \notin \mathcal{S}$.*
2. *For any two roots of unity ζ and μ if both $\zeta U_\mathbf{a} V_\mathbf{b}$ and $\mu U_\mathbf{a} V_\mathbf{b}$ belong to $\mathcal{S}$ then $\zeta = \mu$.*
3. *The subgroup $\mathcal{S}$ should be abelian.*

Proof sketch.

1. Let $\zeta I \in \mathcal{S}$. For any vector $|\psi\rangle$, $\zeta I|\psi\rangle = \zeta|\psi\rangle$ and hence for $\mathcal{C}_\mathcal{S}$ to be nontrivial $\zeta = 1$.
2. If $\zeta U_\mathbf{a} V_\mathbf{b}$ and $\mu U_\mathbf{a} V_\mathbf{b}$ belong to $\mathcal{S}$ then then $\zeta\overline{\mu} I \in \mathcal{S}$ and hence $\zeta = \mu$.
3. For any two U and V in $\mathcal{E}$ the commutator $[U, V] = \zeta I$ for some root of unity ζ. Again from part 1 of the theorem we have the commutator subgroup $[\mathcal{S}, \mathcal{S}] = \{I\}$.

□

The above theorem gives the necessary conditions for $\mathcal{S}$ to give a nontrivial stabiliser subgroup. By a *Gottesman* subgroup of the error group we mean a subgroup $\mathcal{S}$ such that $\zeta I \notin \mathcal{S}$ for all nontrivial root of unity ζ. From the proof of Theorem 8.1 it is clear that a Gottesman subgroup $\mathcal{S}$ satisfies all the properties of Theorem 8.1. We now show that any Gottesman subgroup leads to a nontrivial stabiliser code and derive a formula for the dimension of the code $\mathcal{C}_\mathcal{S}$.

Let $\mathcal{S}$ be a Gottesman subgroup of the error group and let $\hat{\mathcal{S}}$ denote its character group. Consider any nontrivial character $\chi \in \hat{\mathcal{S}}$. Define the operator P_χ as follows

$$P_\chi = \frac{1}{\#\mathcal{S}} \sum_{s \in \mathcal{S}} \chi(s) s.$$

Lemma 8.2.

$$P_{\chi_1} P_{\chi_2} = \begin{cases} P_{\chi_1} \text{ if } \chi_1 = \chi_2, \\ 0 \text{ otherwise.} \end{cases}$$

Proof sketch. Use Schur's orthogonality (Lemma 4.1). □

The above lemma, in particular, shows that P_χ is a projection operator. The following lemma gives the dimension of the subspace $\mathrm{Img}(P_\chi)$.

Lemma 8.3. *The dimension of $Img(P_\chi)$ is $\frac{\#A^n}{\#\mathcal{S}}$.*

Proof. The dimension of $\mathrm{Img}(P_\chi)$ is given by $Tr(P_\chi)$. Note that if $\mathbf{a}$ and $\mathbf{b}$ are elements of A^n such that $(\mathbf{a}, \mathbf{b}) \neq (0, 0)$ we have $Tr(U_{\mathbf{a}} V_{\mathbf{b}}) = 0$. As a result $Tr(\chi(s)s) = 0$ for all $s \neq I$ in $\mathcal{S}$. This shows that TrP_χ is $\frac{1}{\#\mathcal{S}} TrI = \frac{\#A^n}{\#\mathcal{S}}$. □

.

The Lemmas 8.2 and 8.3 implies that the projections P_χ "partition" the Hilbert space $L^2(A)^{\otimes^n}$ into orthogonal subspace, i.e. $\sum_{\chi \in \hat{\mathcal{S}}} P_\chi = I$. We can derive the dimension formula now.

Theorem 8.4. *For a Gottesman subgroup $\mathcal{S}$ of $\mathcal{E}$ the stabiliser subspace $\mathcal{C}(\mathcal{S})$ is the image of the projection $P(\mathcal{S})$ given by*

$$P(\mathcal{S}) = P_1 = \frac{1}{\#\mathcal{S}} \sum_{s \in \mathcal{S}} s.$$

Hence $\mathcal{C}_\mathcal{S}$ is of dimension $\frac{\#A^n}{\#\mathcal{S}}$.

Proof sketch. Consider any $s \in S$. We have $sP_\chi = \chi(s)P_\chi$. Hence the subspace $\mathrm{Img}(P_1)$ is a subspace of $\mathcal{C}_\mathcal{S}$. To prove $\mathrm{Img}(P_1)$ is indeed $\mathcal{C}_\mathcal{S}$ note that for any operator $s \in S$, $\mathrm{Img}(P_\chi)$ is the eigen space corresponding to the eigen value $\chi(s)$. As a result there is no vector $|\psi\rangle$ orthogonal to $\mathrm{Img}(P_1)$ such that $s|\psi\rangle = |\psi\rangle$ for all $s \in S$. □

Consider the homomorphism ϕ from $\mathcal{E}$ to $A^n \times A^n$ that maps $\zeta U_{\mathbf{a}} V_{\mathbf{b}}$ to $(\mathbf{a}, \mathbf{b})$. It follows from Theorem 8.1 that ϕ restricted to $\mathcal{S}$ is an injection. Let S denote subgroup $\phi(\mathcal{S})$. For $\mathcal{S}$ to be abelian, it requires that for all $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ and $\mathbf{d}$ such that $(\mathbf{a}, \mathbf{b})$ and $(\mathbf{c}, \mathbf{d})$ lies in S, $\chi_{\mathbf{a}}(\mathbf{d}) = \chi_{\mathbf{b}}(\mathbf{c})$ holds. Together with Theorem 8.1 we have the following characterisation of stabiliser codes.

Theorem 8.5. *Any Gottesman subgroup $\mathcal{S}$ of $\mathcal{E}$ is given by*

$$\mathcal{S} = \{\rho(\mathbf{a}, \mathbf{b}) U_{\mathbf{a}} V_{\mathbf{b}} | (\mathbf{a}, \mathbf{b}) \in S\}$$

where S is a subgroup of $A^n \times A^n$ and ρ is a function from S to the unit circle in $\mathbb{C}$ with the property that for all $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ and $\mathbf{d}$ such that $(\mathbf{a}, \mathbf{b})$ and $(\mathbf{c}, \mathbf{d})$ is in S the following condition should hold:

1. $\chi_{\mathbf{a}}(\mathbf{d}) = \chi_{\mathbf{b}}(\mathbf{d})$ *and*
2. $\rho(\mathbf{a}, \mathbf{b})\rho(\mathbf{c}, \mathbf{d})\chi_{\mathbf{b}}(\mathbf{c}) = \rho(\mathbf{a} + \mathbf{c}, \mathbf{b} + \mathbf{d})$.

For a subgroup $\mathcal{S}$ of $\mathcal{E}$ by $\mathrm{C}(\mathcal{S})$ we denote the centraliser of $\mathcal{S}$, i.e. the subgroup of elements of $\mathcal{E}$ that commute with every elements of $\mathcal{S}$. For a Gottesman group $\mathcal{S}$ we have $\mathrm{C}(\mathcal{S}) \supseteq \mathcal{S}$. The Knill-Laflamme criteria for stabiliser codes becomes a statement about the centraliser of $\mathcal{S}$.

Theorem 8.6. *Let $\mathcal{S}$ be a Gottesman subgroup of the error group $\mathcal{E}$. The set of errors that $\mathcal{C}_{\mathcal{S}}$ cannot detect is $\mathrm{C}(\mathcal{S}) \setminus \mathcal{S}$.*

Proof sketch. Let $P = \frac{1}{\#S} \sum_{s \in \mathcal{S}} s$ be the projection operator corresponding to $\mathcal{C}_{\mathcal{S}}$. Let g be any element of $\mathcal{E}$. The code $\mathcal{C}_{\mathcal{S}}$ can detect g if and only if $PgP = cP$ for some scalar c. It can be easily seen that if $g \in S$ then $PgP = P$ and if $g \in \mathcal{E} \setminus \mathrm{C}(S)$ then $PgP = 0 = 0P$. It can also be seen that PgP for g in $\mathrm{C}(\mathcal{S}) \setminus \mathcal{S}$ cannot be written as cP for any scalar c. This is because $PgP = gP^2 = gP$ and since $g \in \mathrm{C}(\mathcal{S}) \setminus \mathcal{S}$, the operators gP and P have disjoint support. This proves our theorem. □

The above theorem leads to the following useful lemma.

Lemma 8.7. *Let $\mathcal{S}$ be a Gottesman subgroup of the error group and let $\mathcal{C}_{\mathcal{S}}$ be the corresponding stabiliser code. The distance of the code $\mathcal{C}_{\mathcal{S}}$ is given by the minimum of $w(\mathbf{a}, \mathbf{b})$ over all $\mathbf{a}$ and $\mathbf{b}$ such that $\zeta U_{\mathbf{a}} V_{\mathbf{b}} \in \mathrm{C}(\mathcal{S}) \setminus \mathcal{S}$.*

9 Stabiliser codes over finite fields

In this section we deal with stabiliser codes over finite fields, i.e. quantum codes where the underlying Hilbert space is $L^2(\mathbb{F}_q)$. One hopes that the rich algebraic properties of finite fields can be used to give succinct description of codes and would lead to efficient encoding and decoding algorithms.

We introduce some notations. For $q = p^l$, p a prime, by $\mathbb{F}_q$ we mean the unique finite field of cardinality q. We will be interested in quantum codes over $L^2(\mathbb{F}_q)^{\otimes^n}$. By $((n, r, d))_q$ we mean a quantum code over $L^2(\mathbb{F}_q)^{\otimes^n}$ with distance d and dimension r. For codes with dimension a power of q, we use the notation $[[n, k, d]]_q$ to denote a $((n, q^k, d))_q$ code over $L^2(\mathbb{F}_q)^{\otimes^n}$. The notation $[[n, k, d]]_q$ is analogous to the notation $[n, k, d]_q$ used to denote a n length linear code of dimension k and distance d over $\mathbb{F}_q$.

Consider a nontrivial character ω of $\mathbb{F}_q$. For an element $a \in \mathbb{F}_q$ define the character ω_a which maps $x \in \mathbb{F}_q$ to $\omega(ax)$. The mapping $a \mapsto \omega_a$ is an isomorphism from $\mathbb{F}_q$ to its character group. Consider the group $\mathbb{F}_q^n$. For $\mathbf{a}$ in $\mathbb{F}_q^n$, let $\omega_{\mathbf{a}}$ denote the map $\mathbf{x} \mapsto \omega(\mathbf{a}^T\mathbf{x})$. Again the mapping $\mathbf{a} \mapsto \omega_{\mathbf{a}}$ is an isomorphism from $\mathbb{F}_q^n$ to its character group. To study stabiliser codes over finite fields, we fix a finite field $\mathbb{F}_q$ and a nontrivial character ω of it. Let $\mathcal{E}$ be the error group associated with $L^2\left(\mathbb{F}_q\right)^{\otimes^n}$.

We can think of elements of $\mathbb{F}_q^n \times \mathbb{F}_q^n$ as vectors in $\mathbb{F}_q^{2n}$. Any element $\mathbf{u} \in \mathbb{F}_q^{2n}$ is of the form $(\mathbf{a}, \mathbf{b})$ for $\mathbf{a}$ and $\mathbf{b}$ in $\mathbb{F}_q^n$. By $U_{\mathbf{u}}$ we mean the operator $U_{\mathbf{a}}V_{\mathbf{b}}$. We define the *symplectic* inner product $\langle\langle\ ,\ \rangle\rangle$ from $\mathbb{F}_q^n \times \mathbb{F}_q^n$ to $\mathbb{F}_q$ as follows: Given $\mathbf{u} = (\mathbf{a}, \mathbf{b})$ and $\mathbf{v} = (\mathbf{c}, \mathbf{d})$ in $\mathbb{F}_q^n \times \mathbb{F}_q^n$, $\langle\langle \mathbf{u}, \mathbf{v} \rangle\rangle = \mathbf{a}^T\mathbf{d} - \mathbf{b}^T\mathbf{c}$

Theorem 8.5 takes the following form

Theorem 9.1. *Any Gottesman subgroup $\mathcal{S}$ of the error group $\mathcal{E}$ is of the form*

$$\mathcal{S} = \{\omega(\rho(\mathbf{u}))U_{\mathbf{u}} : \mathbf{u} \in S\}.$$

where S is a additive subgroup of $\mathbb{F}_q^n \times \mathbb{F}_q^n$ satisfying the symplectic condition $\langle\langle u, v \rangle\rangle = 0$ for all u and v in S and ρ is a function from S to $\mathbb{F}_q$ such that for $\mathbf{u} = (\mathbf{a}, \mathbf{b})$ and $\mathbf{v} = (\mathbf{c}, \mathbf{d})$ in S we have $\rho(\mathbf{u}) + \rho(\mathbf{v}) + \mathbf{b}^T\mathbf{c} = \rho(\mathbf{u} + \mathbf{v})$.

Consider a subgroup S of $\mathbb{F}_q^n \times \mathbb{F}_q^n$. Define the subgroup $\overline{S}$ to be the set of vectors $\mathbf{x}$ such that $\langle\langle \mathbf{x}, \mathbf{u} \rangle\rangle$ is zero for all $\mathbf{u}$ in S. The subgroup $\overline{S}$ is the "orthogonal complement" of S under the symplectic inner product. Let S be a subgroup which together with a function ρ gives a Gottesman subgroup $\mathcal{S}$ as in Theorem 9.1. We have the following lemma on the distance of $\mathcal{C}_{\mathcal{S}}$.

Lemma 9.2. *The subgroup $\overline{S}$ contains S and the distance of $\mathcal{C}_{\mathcal{S}}$ is the minimum of $w(\mathbf{x})$, $\mathbf{x}$ in $\overline{S} \setminus S$.*

Proof sketch. The result follows from the fact that the centraliser of $\mathcal{S}$ consists of elements of the form $\zeta U_{\mathbf{x}}$ for $\mathbf{x} \in \overline{S}$. □

The task of constructing stabiliser codes involves constructing subgroups S and ρ with the above mentioned properties. For a detailed account on how such an S and ρ can be constructed we refer the reader to [2] and [1]. Here we give two examples.

CSS code as stabiliser code

We show that the codes constructed by the CSS construction in Section 6 can be seen as a stabiliser code. Let C_1 and C_2 be linear codes over $\mathbb{F}_q$ of length n such that $C_1 \supseteq C_2$. Recall that we have to construct a subgroup S of $\mathbb{F}_q^n \times \mathbb{F}_q^n$ and a function ρ satisfying the conditions of Theorem 9.1. It can be readily checked that if ρ is the constant function that takes value 1 and S is the set of all $(\mathbf{a}, \mathbf{b})$ such that $\mathbf{a} \in C_2$ and $\mathbf{b} \in C_1^{\perp}$, the conditions are met. Define $\mathcal{S}$ defined as

$$\mathcal{S} = \{U_{\mathbf{a}}V_{\mathbf{b}} | \mathbf{a} \in C_2 \text{ and } \mathbf{b} \in C_1^{\perp}\}.$$

The stabiliser code $\mathcal{C}_{\mathcal{S}}$ is the required CSS code. Here we took S to be $C_2 \times C_1^{\perp}$ and ρ to be the constant function that takes zero at all points.

Let C_1 and $C_2^{\perp}$ be $[n, k_1, d]_q$ and $[n, n-k_2, d]$ code respectively (i.e. C_2 is a $[n, k_2]_q$ code). Note that $\#S$ is $q^{k_2}.q^{n-k_1}$. As a result the dimension of $\mathcal{C}_{\mathcal{S}}$ is $q^{k_1-k_2}$ code. Also note that $\overline{S}$ is nothing but $C_1 \times C_2^{\perp}$. Hence $\overline{S} \setminus S$ consist of elements of weight at least d. In fact a stronger property holds, namely all the non-zero elements of $\overline{S}$ have weight at least d. Such codes are called pure codes. A Gottesman subgroup $\mathcal{S}$ is called a *d-pure* subgroup if the centre $\mathrm{C}(\mathcal{S})$ does not contain any element of weight less than d. It is clear that a d-pure Gottesman subgroup yields a distance d stabiliser code $\mathcal{C}_{\mathcal{S}}$.

Laflamme code

We give the description of a $[[5, 1, 3]]_q$ stabiliser code over $\mathbb{F}_q$ which is known as the Laflamme code. The smallest classical code that can correct one error requires at least 3 bit. In the case of quantum code the smallest code that can correct 1 qbit error requires at least 5 qbits (see [2]). For the case when $q = 2$ the Laflamme code is optimal.

Our base field is $\mathbb{F}_q$. Let C be the subspace of $\mathbb{F}_q^5$ consisting of vectors $(a_1, \ldots, a_5)$ such that $\sum a_i = 0$. Let L be the matrix

$$L = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

The matrix L is a so called *circulant matrix*. If σ denotes the cyclic shift then the rows of L are obtained by applying σ to the row vector $(0, 0, 1, 1, 0)$. Let D be any matrix such that $L = D + D^T$, for example D is the upper triangular matrix whose upper triangle coincides with that of L. It can be easily verified that the subgroup $\mathcal{S}$ defined by

$$\mathcal{S} = \{\omega(\mathbf{a}^T D\mathbf{a}) U_{\mathbf{a}} V_{L\mathbf{a}} : \mathbf{a} \in C\}$$

is a Gottesman subgroup of the error group. We have chosen the set S to be $\{(\mathbf{a}, L\mathbf{b}) : \mathbf{a} \in C\}$ and the function ρ to be $\mathbf{a}^T D\mathbf{a}$. The dimension of the code is given by $\frac{q^5}{q^4} = q$.

To check that distance of $\mathcal{C}_{\mathcal{S}}$ is 3 we have to verify that $\overline{S} \setminus S$ had distance 3. The elements of $\overline{S}$ consists of $(\mathbf{x}, \mathbf{y})$ such that $\mathbf{a}^T(\mathbf{y} - L\mathbf{x}) = 0$, i.e. $\mathbf{y} - L\mathbf{x}$ belongs to $C^{\perp}$. One can show that for $(\mathbf{x}, \mathbf{y})$ of combined weight 2 this cannot happen.

For the code to be a distance 3 code it was sufficient for $\overline{S} \setminus S$ not to contain elements of weight 2 or less. Also note that the Laflamme code is a 3-pure code.

10 Error correction algorithms for stabiliser codes

In this section we describe error correcting algorithm for quantum stabiliser codes. We will describe the error correcting algorithm for the case when the underlying abelian

group is $\mathbb{F}_q$. For codes over $L^2(A)$ for abelian groups A, a similar algorithm can be devised. For the purpose of this section we assume that a Gottesman subgroup $\mathcal{S}$ is given. Let $\mathcal{S} = \{\omega(\rho(\mathbf{u}))U_{\mathbf{u}} : \mathbf{u} \in S\}$. where S and ρ satisfies the conditions of Theorem 9.1. Recall that $\overline{S}$ is "orthogonal complement" of S under the symplectic inner product $\langle\langle\ ,\ \rangle\rangle$. Although the construction of $\mathcal{S}$ involves choosing S and ρ with the desired properties, from the error correction point of view it is the subgroups S and $\overline{S}$ that really matters. To simplify things, we assume that S is indeed a subspace of $\mathbb{F}_q^n \times \mathbb{F}_q^n$.

Let d be the distance $d(\mathcal{C}_{\mathcal{S}})$ of the code $\mathcal{C}_{\mathcal{S}}$. This means that for all $\mathbf{v} \in \overline{S} \setminus S$, $w(\mathbf{v}) > d$. Let $\mathbf{u}_1, \ldots, \mathbf{u}_k$ be a basis for S. The unitary operators $\omega(\rho(\mathbf{u}_i))U_{\mathbf{u}_i}$ generate the Gottesman subgroup $\mathcal{S}$. We have the following lemma

Lemma 10.1. *For any vectors $\mathbf{v}_1$ and $\mathbf{v}_2$, $U_{\mathbf{v}_1}$ $U_{\mathbf{v}_2}$ are in the same coset of $\mathrm{C}(\mathcal{S})$ if and only if for all $1 \leq i \leq k$, $\langle\langle \mathbf{v}_1, \mathbf{u}_i\rangle\rangle$ is equal to $\langle\langle \mathbf{v}_2, \mathbf{u}_i\rangle\rangle$*

Proof. Since $\mathbf{u}_i$'s form a basis for S, if $\langle\langle \mathbf{v}_1, \mathbf{u}_i\rangle\rangle$ equals $\langle\langle \mathbf{v}_2, \mathbf{u}_i\rangle\rangle$ for all i then $\langle\langle \mathbf{v}_1, \mathbf{u}\rangle\rangle$ equals $\langle\langle \mathbf{v}_2, \mathbf{u}\rangle\rangle$ for all $\mathbf{u}$ in S. This implies that $\langle\langle \mathbf{v}_1 - \mathbf{v}_2, \mathbf{u}\rangle\rangle = 0$ for all $\mathbf{u}$ in S. As a result $\mathbf{v}_1 - \mathbf{v}_2$ is in $\overline{S}$ which proves our lemma. □

Assume that the sender sends $|\psi\rangle$ and an unknown error $U_{\mathbf{x}} = U_{\mathbf{x}_1}V_{\mathbf{x}_2}$ occurred. We will give a quantum algorithm for error correction that can correct errors $U_{\mathbf{x}}$ for $\mathbf{x}$ of weight less than or equal to $t = \lfloor \frac{d-1}{2} \rfloor$.

The received state is given by $|\phi\rangle = U_{\mathbf{x}}|\psi\rangle$. For $(\mathbf{a}, \mathbf{b})$ in S, it is easy to see that $|\phi\rangle$ is an eigen vector of $U_{\mathbf{a}}V_{\mathbf{b}}$ with eigen value $\langle\langle(\mathbf{a}, \mathbf{b}), (\mathbf{x}, \mathbf{y})\rangle\rangle$. We now give the error correction algorithm.

1. For each basis element $\mathbf{u}_i = (\mathbf{a}_i, \mathbf{b}_i)$ of S compute the eigen value of the operator $U_{\mathbf{a}_i}V_{\mathbf{b}_i}$ corresponding to the vector $|\phi\rangle$ using Kitev's phase estimation method. This gives us a sequence of k linear equations one for each basis element.
2. We solve this equation and find a solution of weight less than or equal to t.
3. Let the solution vector be $\mathbf{v}$. The error corrected state is given by $U_{\mathbf{v}}^{\dagger}|\phi\rangle$.

To prove the correctness of the algorithm note that $U_{\mathbf{x}}$ and $U_{\mathbf{v}}$ are in the same coset of $\mathrm{C}(\mathcal{S})$ (by Lemma 10.1). Also since $\mathbf{x}$ and $\mathbf{v}$ are of weight less or equal to t we have $w(\mathbf{x} - \mathbf{v}) \leq d$ and as a result $\mathbf{x} - \mathbf{v} \in S$ (because $\overline{S} \setminus S$ contains vectors of weight greater than d). This proves that $U_{\mathbf{v}}^{\dagger}|\phi\rangle = (U_{\mathbf{v}}^{\dagger}U_{\mathbf{x}})|\psi\rangle$ is nothing but $\zeta|\psi\rangle$. The correctness of the algorithm follows as the overall phase ζ can be neglected.

References

[1] V. Arvind and K. R. Parthasarathy. A family of stabilizer codes based on Weyl commutation relation over a finite field. *Volume in honor of C.S. Seshadri's 70th birthday*, pages 133–153, 2003. Preprint quant-ph/0206174.

[2] Calderbank, Rains, Shor, and Sloane. Quantum Error Correction Via Codes Over GF(4). *IEEETIT: IEEE Transactions on Information Theory*, 44, 1998.

[3] Emanuel Knill and Raymond Laflamme. A theory of quantum error correcting codes. *Physical Review letters*, 84:2525–2528, 2000. Preprint quant-ph/9604034.

[4] J. H. van Lint. *Introduction to Coding Theory*, volume 86 of *Graduate Texts in Mathematics*. Springer-Verlag, New York Inc, 3^{rd} edition, 1998.