A Survey on Quantum Error Correcting Codes

(양자 오류 정정 부호에 대한 연구)

2018년 2월

서울대학교 대학원
수 리 과학 부
황 규 호
A Survey on Quantum Error Correcting Codes

by

Gyuho Hwang

A DISSERTATION

Submitted to the faculty of the Graduate School
in partial fulfillment of the requirements
for the degree Master of Science
in the Department of Mathematics
Seoul National University
February 2018
Abstract

Quantum error-correcting codes is used to protect quantum information against noise. In this thesis we explain the structure and error correction process of the Calderbank-Shor-Steane codes (CSS) codes and the stabilizer codes. Also we describe CSS codes in the context of stabilizer formalism. Furthermore we will discuss the logical basis states and the encoding circuit of stabilizer codes.

Keywords: Quantum error correcting code, CSS code, Stabilizer code

Student number: 2014-22356
# Contents

Abstract ................................................................. i

1 Introduction .......................................................... 1

2 Preliminaries .......................................................... 3
   2.1 Quantum mechanics ............................................. 3
       2.1.1 The postulates of quantum Mechanics ................ 3
       2.1.2 Density operators ....................................... 5
       2.1.3 Quantum channel ....................................... 6

3 Quantum error correcting codes ................................... 9
   3.1 Basic concepts .................................................. 9
   3.2 Quantum error correction condition ......................... 10

4 Calderbank-Shor-Stean codes ...................................... 13
   4.1 Classical linear codes ....................................... 13
   4.2 CSS codes ...................................................... 17
   4.3 Error correction process of CSS codes ...................... 17

5 Stabilizer codes ...................................................... 21
   5.1 Stabilizer codes ................................................ 21
CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2 Error correction process of stabilizer codes</td>
<td>26</td>
</tr>
<tr>
<td>5.3 Describing CSS codes as stabilizer codes</td>
<td>30</td>
</tr>
<tr>
<td>5.4 Standard form and logical basis states</td>
<td>32</td>
</tr>
<tr>
<td>5.5 Encoding Stabilizer Codes</td>
<td>35</td>
</tr>
<tr>
<td>The bibliography</td>
<td>41</td>
</tr>
</tbody>
</table>

국문초록

국문초록
Chapter 1

Introduction

In the field of quantum algorithms it is known that quantum computers would have extraordinary power on some tasks which are not feasible on a classical computer. For example, some quantum algorithms based upon Shor’s quantum Fourier transform [6] is exponentially faster than classical algorithms for solving the factoring problem. But quantum computers have the challenge of protecting quantum information from errors. Since a quantum computer will interact with its surroundings, quantum decoherence causes errors and so the quantum information decays with time. This is inevitable because large quantum systems cannot be perfectly isolated. Also, quantum gates cannot be implemented exactly since the set of unitary operators is continuous.

Quantum error correction is used to protect quantum information stored or transmitted over a noisy communication channel. Also quantum error correction is applied to fault-tolerant quantum computation, techniques which are used to compute on encoded quantum states successfully even with faulty gates. Shor [7] and Steane [8] discovered the first quantum error
CHAPTER 1. INTRODUCTION

correcting code.

Chapter 2 provides a overview of basic materials in quantum mechanics. Chapter 3 introduces the concept of quantum error correcting codes, and describes the quantum error correction condition. Chapter 4 is about the Calderbank-Shor-Steane codes (or CSS codes, after the initials of the inventors). Calderbank and Shor [1], and Steane [9] developed CSS codes by using classical error correcting codes. We will review the theory of classical linear codes, and explain the structure and error correction process of CSS codes. Finally, Chapter 5 discusses the stabilizer codes. Gottesman [2] introduced the stabilizer formalism. It is a large class of quantum codes including CSS codes. After explaining the structure and the error correction properties of the stabilizer code, we will describe CSS codes in terms of stabilizer codes. Also, we will discuss the logical basis states and encoding circuit for stabilizer codes.

This thesis is primarily based on [4] and [2].
Chapter 2

Preliminaries

2.1 Quantum mechanics

2.1.1 The postulates of quantum Mechanics

Any isolated physical system is associated to a complex Hilbert space, called the state space of the system. The state vector is a unit vector in the state space which refers to the state of the system. We are most concerned with the qubit (or quantum bit) system. The state space of a qubit is a two dimensional Hilbert space, $\mathbb{C}^2$, and any state vector in the state space can be written in the form

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

for some fixed orthonormal basis $\{|0\rangle, |1\rangle\}$ of $\mathbb{C}^2$ where $\alpha$, $\beta$ are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. In this context, a qubit is the quantum analogue of the classical binary bit. The $n$ qubits space is the $n$ fold tensor product of a qubit space $\mathbb{C}^2$. Note that $\{|x_1 \cdots x_n\rangle : x_i = 0 \text{ or } 1\}$ forms an orthonormal basis for $n$ qubits space $(\mathbb{C}^2)^\otimes n = \mathbb{C}^{2^n}$. We say that these states $|0 \cdots 0\rangle, \cdots, |1 \cdots 1\rangle$ are computational basis states of $n$ qubits space.
CHAPTER 2. PRELIMINARIES

The time evolution of the state of a closed quantum system is described by a unitary transformation. Let \( |\psi(t)\rangle \) denote the state of the system at time \( t \). Then the equation

\[
|\psi(t_2)\rangle = U(t_1, t_2)|\psi(t_1)\rangle
\]

holds for some unitary operator \( U(t_1, t_2) \) which depends only on the system and the times \( t_1 \) and \( t_2 \). This is derived from the Schrödinger equation. See the subsection 2.2.2 of [4] for details.

A quantum measurements is described by a family \( \{M_m\} \) of operators acting on the state space and satisfying the completeness equation:

\[
\sum_m M_m^* M_m = I.
\]

The operators \( M_m \) are called the measurement operators and the index \( m \) refers to the measurement outcomes. If we have a state vector \( |\psi\rangle \) then the result \( m \) occur with the probability

\[
p(m) = \langle \psi | M_m^* M_m | \psi \rangle.
\]

The completeness equation shows the fact that the sum of probabilities is one:

\[
\sum_m p(m) = \sum_m \langle \psi | M_m^* M_m | \psi \rangle = \langle \psi | \sum_m M_m^* M_m | \psi \rangle = \langle \psi | \psi \rangle = 1.
\]

Given that outcome is \( m \) occurred, the state after the measurement is

\[
\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^* M_m | \psi \rangle}} = \frac{M_m |\psi\rangle}{\sqrt{p(m)}}.
\]

There is a special class of general measurements. A projective measurement is described by a Hermition operator, called an observable. Suppose that

\[
M = \sum_m \lambda_m P_m
\]
CHAPTER 2. PRELIMINARIES

is a spectral decomposition of an observable $M$ where $\lambda_m$ is an eigenvalues of $M$ and $P_m$ is the projector onto $\lambda_m$-eigenspace. Then the eigenvalues $\lambda_m$ of the observable correspond to the measurement outcomes. The probability of outcome $m$ is given by

$$p(m) = \langle \psi | P_m | \psi \rangle$$

, and the state after the measurement is

$$\frac{P_m}{\sqrt{p(m)}}$$

The phrase 'measure in an orthonormal basis $\{|\psi_m\rangle\}$' means to perform the measurement with the measurement operators $|\psi_m\rangle \langle \psi_m|$, or equivalently, to perform the projective measurement with $P_m = |\psi_m\rangle \langle \psi_m|$. 

2.1.2 Density operators

The density operator is an alternate useful tool to describe quantum systems whose state is not completely known. First, let’s look at the general definition of the density operator.

**Definition 2.1.1.** An operator $\rho \in B(\mathcal{H})$ is called a density operator if $\rho$ is a positive operator and $\text{tr}(\rho) = 1$.

In the density operator language, a state $|\psi\rangle$ corresponds to the operator $|\psi\rangle \langle \psi|$. Suppose that the state vector of a quantum system is $|\psi_i\rangle$ with respective probabilities $p_i$. Note that the linear combination $\sum_i p_i |\psi_i\rangle$ is NOT a state vector in general. But the ensemble $\{p_i, |\psi_i\rangle\}$ can be associated to the density operator $\sum_i p_i |\psi_i\rangle \langle \psi_i|$. Conversely, any density operator is associated to some ensemble by its spectral decomposition.
CHAPTER 2. PRELIMINARIES

The postulates of quantum mechanics are reformulated mathematically equivalently in terms of the density operator as follows. The state of an isolated physical system is described by the density operator acting on the state space of the system. The evolution of a closed quantum system is described by a unitary transformation. If the density operators $\rho(t_1), \rho(t_2)$ denote the states of the system at time $t_1, t_2$ respectively, then

$$\rho(t_2) = U \rho(t_1) U^*$$

where $U$ is the unitary operator depending on the system and times $t_1, t_2$. If we perform the measurement with the measurement operators $\{M_m\}$ to the state $\rho$ then the result $m$ occur with the probability

$$p(m) = \text{tr}(M_m^* M_m \rho),$$

and the state after the measurement is

$$\frac{M_m \rho M_m^*}{\text{tr}(M_m^* M_m \rho)} = \frac{M_m \rho M_m^*}{p(m)}.$$

2.1.3 Quantum channel

Suppose that we want to apply an operator to a particular quantum system or send quantum information of the system. Then the quantum system is not closed since external we interact with the system. The system of interest is called the principal system. Also a environment refers to a system that forms a closed system together with the principal system.

Assume for now that the entire system is in a product state $\rho \otimes \rho_{\text{env}}$. Then the state of the entire system after the evolution is

$$U(\rho \otimes \rho_{\text{env}}) U^*$$
CHAPTER 2. PRELIMINARIES

where $U$ is the unitary operator associated with the evolution. If the principal system does not interact with the environment after the transformation $U$, then we can obtain the state of the principal system

$$
\Phi(\rho) = \text{tr}_{\text{env}} [U(\rho \otimes \rho_{\text{env}})U^*]
$$

by performing a partial trace over the environment. Quantum channels are defined to generalize this situation.

**Definition 2.1.2.** A linear map

$$
\Phi : B(\mathcal{H}_1) \rightarrow B(\mathcal{H}_2)
$$

is called a quantum channel if it is completely positive and trace preserving.

Quantum channels which we will be most concerned with are channels whose input and output spaces both are $n$ qubit spaces. The following theorem is useful to characterize quantum channels.

**Theorem 2.1.1** (Corollary 2.27 in [10], section 8.2 of [4]). For a linear map $\Phi$ on a finite dimensional Hilbert space $\mathcal{H}$, the followings are equivalent.

1. $\Phi$ is a quantum channel.

2. There exists a collection of linear operator $\{E_i\} \subset B(\mathcal{H})$ such that

$$
\sum_i E_i^* E_i = I
$$

and

$$
\Phi(\rho) = \sum_i E_i \rho E_i^* \quad (2.1)
$$

for all $\rho \in B(\mathcal{H})$. 
3. There exists the system (called environment) with the state space $\mathcal{H}_{env}$ and the pure state $|e_0\rangle$ in $\mathcal{H}_{env}$ such that

$$\Phi(\rho) = \text{tr}_{env} [U (\rho \otimes |e_0\rangle\langle e_0|) U^*]$$

for some unitary operator $U$ on $\mathcal{H} \otimes \mathcal{H}_{env}$

In the theorem 2.1.1 the operators $\{E_i\}$ and the equation 2.1 are called operation elements and operator sum representation of the quantum channel $\Phi$, respectively.

**Physical interpretation of quantum channels**

Suppose that operators $\{E_i\}$ are operation elements of a quantum channel $\Phi$. Then the quantum channel $\Phi$ is represented by

$$\rho \mapsto \Phi(\rho) = \sum_i E_i \rho E_i^*$$

$$= \sum_i \text{tr}(E_i \rho E_i^*) \frac{E_i \rho E_i^*}{\text{tr}(E_i \rho E_i^*)}, \text{ for } \rho \in D(\mathcal{H}).$$

If $\rho$ is a density operator then $E_i \rho E_i^*/\text{tr}(E_i \rho E_i^*)$ is also a density operator for each index $i$. Also note that $\sum_i \text{tr}(E_i \rho E_i^*) = \sum_i \text{tr}(E_i^* E_i \rho) = 1$ since $\sum_i E_i^* E_i = I$. When quantum channel $\Phi$ is applied to the state $\rho$, it is interpreted that state

$$\rho_k = \frac{E_k \rho E_k^*}{\text{tr}(E_k \rho E_k^*)}$$

is obtained with probability

$$p(k) = \text{tr}(E_k \rho E_k^*).$$

In fact, this is equivalent to the result of the measurement of the environment in some basis where the environment is given as in the theorem 2.1.1. See [4].
Chapter 3

Quantum error correcting codes

In this chapter we will discuss the basic theory of the quantum error correcting codes.

3.1 Basic concepts

Quantum error correcting codes are used to do quantum information processing reliably against the effects of noise. These steps are as follows. Firstly, we encode quantum states to make them resilient. After applying a quantum channel, we decode the states to recover the original state.

![Quantum error correction diagram]

Figure 3.1: Quantum error correction
CHAPTER 3. QUANTUM ERROR CORRECTING CODES

Someone defines quantum error correcting codes as an encoding map, but we will use the definition such that a code just refers to the space containing codewords.

**Definition 3.1.1.** A quantum error correcting code is a subspace of some larger Hilbert space.

A quantum error correcting code $C$ is called a $[n, k]$ code if $C$ is a $2^k$ dimensional subspace of $n$ qubits space $(\mathbb{C}^2)^\otimes n$. A $[n, k]$ quantum code is used to encode $k$ qubits in $n$ qubits.

![Figure 3.2: $[n, k]$ quantum codes](image)

3.2 Quantum error correction condition

In this section we will introduce error correction conditions for quantum channels. Before that, let’s look at the formal definition of *errors* for a quantum channel and what it means to *correct* errors.

Let $\Phi$ be a quantum channel with operation elements $\{E_i\}$. Then we call operators $\{E_i\}$ *errors* for the quantum channel $\Phi$. For example, consider
CHAPTER 3. QUANTUM ERROR CORRECTING CODES

the bit flip channel on the qubit space

\[ \rho \mapsto (1 - p)\rho + pX\rho X^* \]

where \( p \in [0, 1] \) is fixed and \( X \) is the Pauli sigma \( x \) operator \( \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \).

Observe that the errors for the bit flip channel are \( \sqrt{1 - p}I \) and \( \sqrt{p}X \). Since this channel takes the state \( |\psi\rangle \) to the state \( X|\psi\rangle \) with the probability \( p \) and leaves the state unchanged with the probability \( (1 - p) \), the definition tells us the type of error, including the probability of occurrence.

**Definition 3.2.1.** Let \( \Phi \) be a quantum channel on \( B(\mathcal{H}) \) with operation elements \( \{E_i\} \). For a quantum error correcting code \( C \subset \mathcal{H} \), a quantum channel \( R \) on \( B(\mathcal{H}) \) is called an error-correction operation correcting \( \Phi \) on \( C \) if

\[ (R \circ \Phi)(\rho) = \rho \quad \text{when supp}\rho \subset C. \]

If such \( R \) exist, then we say \( \{E_i\} \) is a correctable set of errors.

**Theorem 3.2.1** (Quantum error correction condition, Theorem 10.1 in [4]). Let \( C \) be a quantum code and \( P \) be the projector onto \( C \). For a quantum channel \( \Phi \) with the operation elements \( \{E_i\} \), there is an error correction operator \( R \) if and only if there is a Hermition matrix \( \alpha \) such that

\[ PE_i^*E_jP = \alpha_{ij}P. \quad (3.1) \]

A operator sum representation of a quantum channel is not unique. If \( \{E_i\}_{i=1}^n \) and \( \{F_i\}_{i=1}^n \) are operation elements of quantum channels \( \Phi \) and \( \Psi \), respectively, then \( \Phi = \Psi \) if and only if there exist a unitary matrix \( (u_{ij}) \) such that

\[ E_i = \sum_j u_{ij}F_j. \quad (3.2) \]
Therefore if \( \{E_i\}_{i=1}^n \) or \( \{F_i\}_{i=1}^n \) is a correctable set of errors for some quantum code \( C \), then so is the other one automatically.

More generally, the following theorem holds.

**Theorem 3.2.2** (Discretization of errors, Theorem 10.2 in [4]). Let \( \Phi \) and \( \Psi \) be quantum channels with operation elements \( \{E_i\} \) and \( \{F_j\} \) respectively satisfying

\[
F_j = \sum_i m_{ji} E_i
\]

for some complex numbers \( m_{ij} \). Then if \( R \) is an error correction operation correcting \( \Phi \) on for some quantum code \( C \), then \( R \) is also corrects \( \Psi \) on \( C \).

The theorem 3.2.2 says that it is sufficient to consider a finite set of errors, the four Pauli matrices:

\[
I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
\]

on a single qubit and \( n \) fold tensor products of the Pauli matrices on \( n \) qubits space.
Chapter 4

Calderbank-Shor-Steane codes

The Calderbank-Shor-Steane codes (or CSS codes) are quantum error correcting codes using the error correction properties of classical linear codes. In this chapter, firstly will we review the theory of classical linear codes, and study the structure and error correction process of CSS codes.

4.1 Classical linear codes

In classical coding theory data can be represented as binary vectors in $\mathbb{F}_2^n$ where $\mathbb{F}_2 = \{0, 1\}$ denote the field with two elements. A $[n, k]$ code is a subset of $\mathbb{F}_2^n$ containing $2^k$ elements and so a $k$-bits message is encoded in a string of length $n$.

**Definition 4.1.1 (Linear code).** Suppose that $G \in M_{(n,k)}(\mathbb{F}_2)$ has full rank. Then the subspace

$$C := \{Gx|x \in \mathbb{F}_2^k\}$$
CHAPTER 4. CALDERBANK-SHOR-STEAN CODES

of $\mathbb{F}_2^n$ is called the $[n, k]$ linear code with the generator matrix $G$.

Since a $[n, k]$ linear code $C$ is $k$ dimensional, there exists a $(n - k) \times n$ matrix $H$ which has linearly independent rows with entries in $\mathbb{F}_2$ such that

$$C = \ker H.$$  

We say that $H$ is the parity check matrix of the linear code $C$. A linear code is completely determined by the parity check matrix as well as its generator matrix.

A $[n, k]$ linear code $C$ is able to correct an error $e \in \mathbb{F}_2^n$ if and only if we can detect the error when the error $e$ occur on any codeword in $C$. Suppose that we have an corrupted codeword $y'$, that is, $y' = y + e$ for some $y \in C$. If we know what is $e$ then we can recover original codeword $y$ by adding the error $e$ on $y'$. Conversely if we get the original codeword $y$ by some way, then the error can be calculated easily : $e = y' + y$. The error correction capability of a linear code is closely related to the 'distance' of the code. From now on we will introduce the definition of Hamming distance and a useful lemma to calculate Hamming distance for a linear code.

**Definition 4.1.2.** 1. The Hamming distance of $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n) \in \mathbb{F}_2^n$ is defined by

$$d(x, y) := |\{i : x_i \neq y_i\}|$$

2. The Hamming weight of $x = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$ is defined by

$$\text{wt}(x) := d(x, 0)$$

3. The (Hamming) distance of a linear code $C$ is defined by

$$d(C) := \min_{x, y \in C, x \neq y} d(x, y) = \min_{x \in C, x \neq 0} \text{wt}(x)$$
4. An \([n, k]\) code \(C\) whose distance is \(d\) is called an \([n, k, d]\) code.

**Lemma 4.1.1.** Suppose that \(H\) is the parity check matrix for an \([n, k]\) linear code \(C\). Then the followings are equivalent.

(i) The distance of \(C\) is \(d\).

(ii) Any \((d - 1)\) columns of \(H\) are linearly independent and there is a set of \(d\) linearly dependent columns of \(H\).

**Proof.** Recall that the distance of the code is given by

\[
    d(C) = \min_{x \in C, x \neq 0} \text{wt}(x).
\]

Hence if the distance of \(C\) is \(d\), then

\[
    Hx = 0 \text{ for some codeword } x \in C \text{ with } \text{wt}(x) = d, \text{ and } \tag{4.1}
\]

\[
    He \neq 0 \text{ for any } e \in \mathbb{F}_2^n \text{ satisfying } 0 < \text{wt}(e) \leq d - 1. \tag{4.2}
\]

But the combination of the equations 4.1 and 4.2 is equivalent to the condition \((ii)\) clearly. \(\square\)

The next theorem is about the error correction condition for linear codes.

**Theorem 4.1.1.** Suppose that \(C\) is a \([n, k, d]\) linear code and \(t \in \mathbb{N}\). Then \(C\) is able to correct errors on up to \(t\) bits if and only if \(d \geq 2t + 1\).

**Proof.** \((\Rightarrow)\) Suppose that \(d \leq 2t\). Then there are \(y_1, y_2 \in C\) such that \(d(y_1, y_2) \leq 2t\), i.e., \(\text{wt}(y_1 + y_2) \leq 2t\). So we can choose \(e_1, e_2 \in \mathbb{F}_2^n\) such that \(y_1 + y_2 = e_1 + e_2\) and \(\text{wt}(e_j) \leq t\) for \(j = 1, 2\). Thus if the corrupted codeword was \(y' := y_1 + e_1 = y_2 + e_2\) we cannot detect that what error occur.

\((\Leftarrow)\) Suppose that \(d \geq 2t + 1\). First we claim that if \(e_1\) and \(e_2\) are distinct
elements of $\mathbb{F}_2^n$ whose weight are both less than $t$, then $He_1 \neq He_2$. If $e_1 \neq e_2$ and $\text{wt}(e_j) \leq t$ for $j = 1, 2$, then $0 < \text{wt}(e_1 - e_2) \leq 2t < d$. So $H(e_1 - e_2)$ is a sum of less than $d$ columns of $H$. By the lemma 4.1.1 $H(e_1 - e_2) \neq 0$ and so $He_1 \neq He_2$. Now assume that the original codeword $y$ is corrupted by an error $e \in \mathbb{F}_2^n$ such that $\text{wt}(e) \leq t$. Then we can detect the error $e$ by computing as

$$Hy' = H(y + e) = H y + He = 0 + He = He.$$  
So we can get the original codeword $y$ by adding the error $e$ to $y'$:

$$y = y' + e$$

In the proof of the theorem 4.1.1 the equation $Hy' = He$ tells us that what error occur. In this sense, we call $He$ the error syndrome of the error $e$.

Now we introduce the dual code of a linear code. It will be used for the construction of the Calderbank-Shor-Steane codes in the next section.

**Definition 4.1.3.** Let $C$ be a $[n,k]$ linear code with the generator matrix $G$ and the parity check matrix $H$. Then the linear code with the generator matrix $H^T$ and the parity check matrix $G^T$ is called the dual of $C$, and denoted by $C^\perp$.

In the above definition, the generator matrix $H^T$ of $C^\perp$ is an $n \times (n-k)$ matrix with full rank. Therefore the dual code $C^\perp$ of an $[n,k]$ linear code $C$ is an $[n,n-k]$ linear code.
CHAPTER 4. CALDERBANK-SHOR-STEAN CODES

4.2 CSS codes

Definition 4.2.1. Suppose that $C_i$ are $[n, k_i]$ linear codes, $i = 1, 2$, such that

$$
\begin{cases}
C_2 \subset C_1 \\
C_1 \text{ and } C_2^\perp \text{ both correct } t \text{ bits errors}
\end{cases}
$$

(4.3)

Then the CSS code of $C_1$ over $C_2$ is defined by

$$
\text{CSS}(C_1, C_2) = \text{span}\{|x + C_2 : x \in C_1\} \subset (\mathbb{C}^2)^{\otimes n}
$$

(4.4)

where

$$
|x + C_2\rangle = \frac{1}{|C_2|}\sum_{y \in C_2}|x + y\rangle
$$

(4.5)

and the sum $x + y$ in the equation 4.5 is bitwise addition modulo 2.

Note that if $x + C_2$ and $x' + C_2$ are different cosets, then $x + y \neq x' + y'$ for any $y, y' \in C_2$ and so $|x + C_2\rangle$ and $|x' + C_2\rangle$ are orthonormal states in $(\mathbb{C}^2)^{\otimes n}$. Therefore the dimension of $\text{CSS}(C_1, C_2)$ is the number of cosets in $C_1/C_2$. But the number of cosets in $C_1/C_2$ is $|C_1/C_2| = |C_1|/|C_2| = 2^{k_1 - k_2}$. Hence $\text{CSS}(C_1, C_2)$ in the definition 4.2.1 is $[n, k_1 - k_2]$ code.

4.3 Error correction process of CSS codes

In this section we will show that the CSS code as in the definition 4.2.1 is able to correct arbitrary errors on less than $t$ qubits.

Lemma 4.3.1. For an $[n, k]$ linear code $C$,

$$
\sum_{y \in C} (-1)^{xy} = \begin{cases}
|C|, & \text{if } x \in C^\perp \\
0, & \text{if } x \notin C^\perp
\end{cases}
$$

(4.6)
CHAPTER 4. CALDERBANK-SHOR-STEAN CODES

Proof. First we will show that for $x \in \mathbb{F}_2^n$, $x \in C^\perp$ if and only if $x \cdot y = 0$ for every $y \in C$. Suppose that $x \in C^\perp$. Choose arbitrary element $y$ of $C$. Then $y = Gx'$ for some $x \in \mathbb{F}_2^k$ where $G$ is the generator matrix of $C$. Since $G^T$ is the parity check matrix of $C^\perp$, we have

$$x \cdot y = x^T y = x^T Gx' = (G^T x)^T x' = 0^T x' = 0$$

Conversely, if $x \cdot y = 0$ for any $y \in C$,

$$G^T x = \begin{pmatrix} v_1^T \\ \vdots \\ v_k^T \\ v_k \cdot x \end{pmatrix} x = \begin{pmatrix} v_1 \cdot x \\ \vdots \\ v_k \cdot x \end{pmatrix} = 0$$

where $v_i = Ge_i \in C$ for $i = 1, \cdots, k$.

Now observe that if $x \in C^\perp$ then

$$\sum_{y \in C} (-1)^{x \cdot y} = \sum_{y \in C} (-1)^0 = |C|,$$

and if $x \notin C^\perp$ then there is an element $z$ of $C$ such that $x \cdot z = 1$ and

$$\sum_{y \in C} (-1)^{x \cdot y} = \sum_{y \in C} (-1)^{x \cdot (y+z)} = -\sum_{y \in C} (-1)^{x \cdot y}.$$

Thus we have $\sum_{y \in C} (-1)^{x \cdot y} = 0$. \qed

Error correction process

Let $CSS(C_1, C_2)$ be a CSS code as in the definition 4.2.1. We will show that $CSS(C_1, C_2)$ is able to correct $t$ qubits errors. To do this it suffice to assume that the bit flip error $X$ or the phase flip error $Z$, or both of them occur on up to $t$ qubits by the discretization of errors. Hence we shall suppose that the original state was $|x + C_2\rangle$ and the corrupted state is

$$\frac{1}{|C_2|} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_2} |x + y + e_1\rangle$$

(4.7)
CHAPTER 4. CALDERBANK-SHOR-STEAN CODES

for some \(e_1, e_2 \in \mathbb{F}_2^n\) such that \(\text{wt}(e_i) \leq t, \ i = 1, 2\). Here \(e_1\) and \(e_2\) describe the places at which the errors \(X\) or \(Z\) occur, respectively.

Firstly, we prepare \((n - k_1)\) ancilla bits and apply \(\prod_{ij} (\text{CNOT}_{(j,n+i)} h_{ij})\) to the corrupted state where \(h_{ij}\) is the \((i,j)\) entry of \(H_1\), the parity check matrix of \(C_1\). Here \(\text{CNOT}_{(i,j)}\) is the controlled-NOT gate which perform a bit flip on \(j\) th qubit if the \(i\) th qubit is set to \(|1\rangle\) in terms of the computational basis. Then we get the state

\[
\frac{1}{|C_2|} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_2} |x + y + e_1\rangle |H_1(x + y + e_1)\rangle. \tag{4.8}
\]

Since \(x + y\) is a codeword in \(C_1\), it become

\[
\frac{1}{|C_2|} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_2} |x + y + e_1\rangle |H_1 e_1\rangle. \tag{4.9}
\]

Measure the last \((n - k_1)\) qubits in computational basis to obtain \(H_1 e_1\). Then we can detect \(e_1\) since the linear code \(C_1\) correct up to \(t\) bits error. After the measurement, discard ancilla bits to get the state

\[
\frac{1}{|C_2|} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_2} |x + y + e_1\rangle. \tag{4.10}
\]

Correct bit flip error by applying Pauli \(X\) operators to qubits at which corresponding component of \(e_1\) is 1, giving the state

\[
\frac{1}{|C_2|} \sum_{y \in C_2} (-1)^{(x+y) \cdot e_2} |x + y\rangle. \tag{4.11}
\]

Apply the Hadamard transform \(H^\otimes n = \begin{bmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \\ 1 & -1 \\ \sqrt{2} & \sqrt{2} \end{bmatrix}^\otimes n\) to detect phase flip errors, taking the state to

\[
\frac{1}{\sqrt{|C_2|2^n}} \sum_{z \in \mathbb{F}_2^n} \sum_{y \in C_2} (-1)^{(x+y) \cdot z'} |z' + e_2\rangle. \tag{4.12}
\]
Putting $z' := z + e_2$, we have

$$\frac{1}{\sqrt{|C_2|2^n}} \sum_{z' \in F_2^n} \sum_{y \in C_2} (-1)^{(x+y)-(e_2+z)}|z\rangle \quad (4.13)$$

$$= \frac{1}{\sqrt{|C_2|2^n}} \left( \sum_{z' \in C_2} \sum_{y \in C_2} (-1)^{(x+y)-(e_2+z)}|z\rangle + \sum_{z' \not\in C_2} \sum_{y \in C_2} (-1)^{(x+y)-(e_2+z)}|z\rangle \right) \quad (4.14)$$

$$= \frac{1}{\sqrt{|C_2|2^n}} \left( \sum_{z' \in C_2} \sum_{y \in C_2} (-1)^{x \cdot z' -(1)^{y \cdot z'}|z\rangle + \sum_{z' \not\in C_2} \sum_{y \in C_2} (-1)^{x \cdot z' -(1)^{y \cdot z'}|z\rangle \quad (4.15)$$

By the lemma 4.3.1, this state written as

$$\frac{1}{\sqrt{2^n/|C_2|}} \sum_{z' \in C_2} (-1)^{x \cdot z'}|z' + e_2\rangle. \quad (4.16)$$

Repeat the same process from the equation 4.8 to the equation 4.11 using the parity check matrix $H_2$ for $C_2$ to correct $e_2$. Then we obtain the state

$$\frac{1}{\sqrt{2^n/|C_2|}} \sum_{z' \in C_2} (-1)^{x \cdot z'}|z\rangle. \quad (4.17)$$

Because the inverse of the Hadamard gate $H$ is itself, applying $H^{\otimes n}$ again we have the original state

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle = |x + C_2\rangle \quad (4.18)$$

such as the state in (4.11) with $e_2 = 0$. 
Chapter 5

Stabilizer codes

5.1 Stabilizer codes

A stabilizer code is determined by the group of operators which stabilize the codewords. We say that a state $|\psi\rangle$ is stabilized by an operator $A$ if

$$A|\psi\rangle = |\psi\rangle.$$ 

In the stabilizer formalism the group of interest is the Pauli group

$$G_n = \{ \alpha \sigma_1 \otimes \cdots \otimes \sigma_n : \alpha = \pm 1, \text{ or } \pm i, \quad \sigma_j = I, X, Y, \text{ or } Z \}$$

acting on $n$ qubits. For a subgroup $S$ of the Pauli group $G_n$, let $V_S$ denote the vector space stabilized by $S$, that is,

$$V_S = \{ |\psi\rangle \in (\mathbb{C}^2)^\otimes n : g|\psi\rangle = |\psi\rangle \text{ for all } g \in S \}.$$ 

Then we say that $S$ is the stabilizer of the space $V_S$. Now let’s see the necessary conditions for $V_S$ to be non trivial.
CHAPTER 5. STABILIZER CODES

Proposition 5.1.1. Let $S$ be a subgroup of the Pauli group $G_n$ for some $n \in \mathbb{N}$. If $V_S$ is non-trivial vector space, then every elements of $S$ commute and $S$ does not contain $-I \in G_n$.

Proof. Suppose that $V_S$ contains an non-zero vector $|\psi\rangle$. Recall that any pair of elements in $G_n$ is either commute or anti-commute. If there are elements $M, N$ of $S$ such that $MN = -MN$, then

$$|\psi\rangle = MN|\psi\rangle = -NM|\psi\rangle = -|\psi\rangle.$$ 

Also, if $-I \in S$ then

$$|\psi\rangle = -I|\psi\rangle = -|\psi\rangle.$$ 

But the equation $|\psi\rangle = -|\psi\rangle$ contradicts that $|\psi\rangle \neq 0$. $\square$

In fact, two conditions stated in the proposition 5.1.1 are also sufficient conditions of $S$ for $V_S$ to be non trivial. We will show that later.

We use the useful notations for characterization of the stabilizer.

Definition 5.1.1. 1. For a element $g = \alpha \sigma_1 \otimes \cdots \otimes \sigma_n$ of $G_n$, let $r(g)$ denote the $2n$ dimensional row vector given by

<table>
<thead>
<tr>
<th>$\sigma_j$</th>
<th>jth entry of $r(g)$</th>
<th>(n + j)th entry of $r(g)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$X$</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$Z$</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$Y$</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

2. The check matrix associated with $g_1, \cdots, g_l \in G_n$ is an $l \times 2n$ matrix defined by

$$G = \begin{bmatrix} r(g_1) \\ \vdots \\ r(g_l) \end{bmatrix} \tag{5.1}$$ 

22
CHAPTER 5. STABILIZER CODES

Lemma 5.1.1. Let $g_1, g_2 \in G_n$.
Then $g_1$ and $g_2$ are commute if and only if $r(g_1) A r(g_2)^T = 0$.

Proof. Write $r(g_1) = [a_1 \cdots a_n | a_{n+1} \cdots a_{2n}]$ and $r(g_2) = [b_1 \cdots b_n | b_{n+1} \cdots b_{2n}]$.
Then $j$-th components of $g_1$ and $g_2$ commute if and only if $(a_j b_{n+j} + a_{n+j} b_j) = 0$. Thus we have
\[ g_1 g_2 = (-1)^{\sum_{j=1}^{n} (a_j b_{n+j} + a_{n+j} b_j)} g_2 g_1 \] (5.2)
Since $r(g_1) A r(g_2) = \sum_{j=1}^{n} (a_j b_{n+j} + a_{n+j} b_j)$, the equation 5.2 complete the proof. \qed

Definition 5.1.2. We say that $g_1, \cdots, g_l \in G_n$ are independent if
\[ <g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_l \geq_X <g_1, \cdots, g_l> \text{ for any } i \] (5.3)

Lemma 5.1.2 (Proposition 10.3 in [4]). Let $S$ be a subgroup of the Pauli group $G_n$ generated by $g_1, \cdots, g_l \in G_n$ such that $-I \in S$. Then the followings are equivalent.

(i) $g_1, \cdots, g_l \in G_n$ are independent.

(ii) $r(g_1), \cdots, r(g_l)$ are linearly independent.

Proof. Note that $g_i^2 = I$ for $i = 1, \cdots, l$ since $S$ does not contain $-I$. Also $r(g) + r(g') = r(gg')$. Suppose that $r(g_1), \cdots, r(g_l)$ are linearly independent. Then there are not all zero $a_1, \cdots, a_l \in \mathbb{F}_2$, say $a_j = 1$, such that $\sum_{i=1}^{l} a_i r(g_i) = 0$. So $\prod_i g_i^{a_i} \in S$ is the identity up to multiplicative factor. But by the hypothesis that $-I \in S$ implies the multiplicative factor is 1. Thus $\prod_i g_i^{a_i} \in S = I$ and we have
\[ g_j = g_j^{-1} = \prod_{i \neq j} g_i^{a_i} \] (5.4) \qed
Lemma 5.1.3 (Proposition 10.4 in [4]). Suppose that $S$ is a subgroup of $G_n$ generated by $g_1, \cdots, g_l \in G_n$ such that $I \notin S$ and $\text{Fix} i \in \{1, \cdots, l\}$. Then there is an element $g$ of $G_n$ such that

$$gg_jg^* = \begin{cases} -g_j & \text{if } j = i \\ g_j & \text{otherwise} \end{cases}$$

Proof. Let $G$ be the check matrix associated to $g_1, \cdots, g_l$. Since $g_1, \cdots, g_l$ are independent, rows of $G$ are linearly independent by proposition 5.1.2. Therefore $G$ has the full rank and so there is $x \in (\mathbb{F}_2)^{2n}$ such that

$$GAx = e_i$$

where $e_i$ is . Choose $g \in G_n$ so that $r(g) = x^T$. \hfill \Box

Theorem 5.1.1 (Proposition 10.5 in [4]). Let $S = \langle g_1, \cdots, g_{n-k} \rangle$ be a subgroup of $G_n$ such that

(i) $g_1, \cdots, g_{n-k}$ are independent and commute

(ii) $-I \notin S$

Then $V_S$ is a $2^k$-dimensional vector space.

Proof. For each $(n-k)$-tuple $x = (x_1, \cdots, x_{n-k}) \in (\mathbb{F}_2)^{n-k}$ define

$$P^x_S := \frac{\prod_{j=1}^{n-k} (I + (-1)^{x_j}g_j)}{2^{n-k}}.$$ 

Especially put

$$P := P^{(0, \cdots, 0)}_S = \frac{\prod_{j=1}^{n-k} (I + g_j)}{2^{n-k}}$$

CHAPTER 5. STABILIZER CODES

Firstly we will show that $P$ is the projector onto $V_S$. Recall that every elements of $G_n$ is unitary. Also note that every $g_j$ has multiplicative factor either $+1$ or $-1$ since $S$ does not contain $-I$. So $g_j$’s are Hermition. Direct calculation shows that $(\frac{I+g_j}{2})^2 = \frac{I+g_j}{2}$. Now using commutativity of $\{g_j\}$ we get $P^* = P$ and $P^2 = P$. Let $P = \sum_i |v_i\rangle\langle v_i|$ be the spectral decomposition.

We claim that $\{|v_i\rangle\}$ is a orthonormal basis for $V_S$. It suffice to show that $\text{span}\{|v_i\rangle\} = V_S$. For any $j$ and $l$,

$$|v_j\rangle = \sum_i |v_i\rangle\langle v_i|v_j\rangle = P|v_j\rangle$$

$$= \frac{1}{2}(I + g_1 \cdots I + g_{n-k})|v_j\rangle$$

$$\in (+1) - \text{eigen space of } g_l$$

So $|v_j\rangle$ is stabilized by $g_1, \cdots, g_{n-k}$, that is, $|v_j\rangle \in V_S$. To show that $V_S$ is spanned by $\{|v_i\rangle\}$, let $|\psi\rangle$ be an arbitrary element of $V_S$. Observe that

$$|\psi\rangle = P|\psi\rangle = \sum_i |v_i\rangle\langle v_i|\psi\rangle \in \text{span}\{|v_i\rangle\}$$

By lemma 5.1.3 for each $x = (x_1, \cdots, x_{n-k}) \in \mathbb{F}_2^{n-k}$ there is a elements $g_x$ of $G_n$ such that

$$g_x \prod_{j=1}^{n-k} (I + g_j) g_x^* = \prod_{j=1}^{n-k} (I + (-1)^{x_j}g_j)$$

In other words, $g_x P g_x^* = P_{S_x}^x$. Since $g_x$ is unitary, we have

$$\dim P_{S_x}^x = \dim P = \dim V_S, \text{ for any } x \in \mathbb{F}_2^{n-k} \quad (5.5)$$

Now we claim that $P_{S_x}^x$’s are orthogonal for distinct $x$’s. If $x = (x_1, \cdots, x_{n-k})$ and $x' = (x'_1, \cdots, x'_{n-k})$ are distinct, $x_j \neq x'_j$ for some $j$. Without loss of generality, assume $x_j = 0$ and $x'_j = 1$. Then $P_{S_x}^x$ (resp. $P_{S_x'}^x$) contains the projector $\frac{I+g_j}{2}$ (resp. $\frac{I-g_j}{2}$) onto $(+1)$-eigenspace of $g_j$ (resp. $(-1)$-eigenspace.
CHAPTER 5. STABILIZER CODES

of $g_j$). Since eigenvectors with different eigenvalues of Hermitian operator are orthogonal, we conclude that $P^x_S$ and $P^{x'}_S$ are orthogonal. In the other hand, observe that

$$I = \sum_{x \in \mathbb{F}_2^{n-k}} P^x_S$$

Combining the equation 5.6 and the fact that distinct $P^x_S$'s are orthogonal, we have

$$2^n = \dim I = \sum_{x \in \mathbb{F}_2^{n-k}} \dim P^x_S = 2^{n-k} \dim V_S.$$  

Thus we conclude that $\dim V_S = 2^k$. \hfill \Box

Definition 5.1.3 (Stabilizer code). Let $S = \langle g_1, \cdots, g_{n-k} \rangle$ be a subgroup of $G_n$ such that.. stabilizer code with the stabilizer $S < G_n$ is defined by

$$C(S) := V_S \subset (\mathbb{C}^2)^\otimes n$$

In the above definition, $C(S)$ is a $[n,k]$ code by the theorem 5.1.1.

5.2 Error correction process of stabilizer codes

Theorem 5.2.1 (Error correction conditions for stabilizer codes, Theorem 10.8 in [4]). Let $C(S)$ be a $[n,k]$ stabilizer code with the stabilizer $S = \langle g_1, \cdots, g_{n-k} \rangle$. Suppose that $\{E_i\}$ be a subset of $G_n$ such that

$$E_i^*E_j \notin N(S) - S \text{ for all } i, j$$

Then $\{E_i\}$ is a correctable set of errors for $C(S)$. 

Proof. Let $P$ be the projector onto $C(S)$. We need to find an Hermitian matrix $\alpha$ satisfying the equation (3.1). By the hypothesis $E_i^*E_j$ is either
CHAPTER 5. STABILIZER CODES

contained in $S$ or $G_n - N(S)$ for given $i, j$. If $E_i^* E_j \in S$, then $E_i^* E_i = (E_i^* E_j)^{-1} \in S$ and $PE_i^* E_j P = PE_j^* E_i P = P$. If $E_i^* E_j \in G_n - N(S)$, then without loss of generality, we may assume $E_i^* E_j$ anti-commute with $g_1 \in S$ and commute with other generators. From the proof of theorem 5.1.1, we know

$$P = \prod_{l=1}^{n-k} (I + g_l)$$

By anti-commutativity of $E_i^* E_j$ and $g_1$, we have

$$E_i^* E_j P = (I - g_1)E_i^* E_k \prod_{l=2}^{n-k} (I + g_l) 2^{n-k}$$  \hspace{1cm} (5.8)

Since $(I + g_1)(i - g_1) = 0$, $P(I - g_1) = 0$ and so

$$PE_i^* E_j P = 0$$  \hspace{1cm} (5.9)

Now put

$$\alpha_{ij} = \begin{cases} 1 \text{ if } E_i^* E_j \in S \\ 0 \text{ if } E_i^* E_j \in G_n - S \end{cases}$$  \hspace{1cm} (5.10) \hspace{1cm} \Box

Error correction

Let $C(S)$ be a stabilizer code as in the definition 5.1.3. Suppose that \{\(E_j\)\} $\subset G_n$ satisfy

$$E_i^* E_j \notin N(S) - S \text{ for all } i, j$$  \hspace{1cm} (5.11)

If an error $E_j$ occurred, we define the error syndrome $(\beta_1, \cdots, \beta_{n-k})$ for $E_j$ by

$$E_j g_l E_j^* = \beta_l g_l \text{ for } l = 1, \cdots, n - k$$  \hspace{1cm} (5.12)

Suppose that an error $E_j$ occur to a state $|\psi\rangle \in C(S)$. Then we have two cases.
1. If $E_j$ is the unique error operator having this syndrome then we just apply $E_j^*$ to corrupted state $E|\psi\rangle$ to recover the original state.

2. If distinct errors $E_j$ and $E_{j'}$ have the same error syndrome $(\beta_1, \cdots, \beta_{n-k})$,

$$E_j g_l E_j^* = \beta_l g_l = E_{j'} g_l E_{j'}^* \text{ for } l = 1, \cdots, n-k \quad (5.13)$$

Hence

$$(E_{j'}^* E_j) g_l (E_j^* E_j)^* = g_l \text{ for } l = 1, \cdots, n-k \quad (5.14)$$

and so

$$E_j^* E_j \in Z(S) = N(S). \quad (5.15)$$

Combining 5.11 and 5.15 we have

$$E_j^* E_j \in S$$

Therefore we get the original codeword $|\psi\rangle$ by applying $E_j^*$, where $E_j$ is any error whose error syndrome equals the syndrome of $E_j$.

**How to get the error syndrome**

Suppose that $|\psi\rangle \in C(S)$ and an error $E \in G_n$ occur. Note that the any generator of $S$ is Hermition and has the eigen values $(+1)$ and $(-1)$. Apply the projective measurement

$$g_l = (+1) \frac{I + g_l}{2} + (-1) \frac{I - g_l}{2}. \quad (5.16)$$

If $\beta_l = 1$, then

$$\frac{I + g_l}{2} E|\psi\rangle = E \frac{I + g_l}{2} |\psi\rangle = E|\psi\rangle \quad (5.16)$$

$$\frac{I - g_l}{2} E|\psi\rangle = E \frac{I - g_l}{2} |\psi\rangle = 0 \quad (5.17)$$
and so $p(+1) = \langle \psi | E^* \frac{I + g_l}{2} E | \psi \rangle = \langle \psi | E^* E | \psi \rangle = 1$ and the post state after the measurement is

$$\frac{I + g_l}{\sqrt{p(+1)}} E | \psi \rangle = E | \psi \rangle.$$  

If $\beta_l = -1$, then

$$\frac{I + g_l}{2} E | \psi \rangle = E \frac{I - g_l}{2} | \psi \rangle = 0 \quad (5.18)$$

$$\frac{I - g_l}{2} E | \psi \rangle = E \frac{I + g_l}{2} | \psi \rangle = E | \psi \rangle \quad (5.19)$$

So we have $p(-1) = 1$ and post state is $E | \psi \rangle$. Thus we can conclude that

$$\beta_l = \begin{cases} +1, & \text{if the measurement outcome is } +1 \\ -1, & \text{if the measurement outcome is } -1 \end{cases}\quad (5.20)$$

**Quantum circuit measuring $g_l$**

The state before the measurement in the quantum circuit Figure 5.1 is

$$\frac{|0\rangle I + g_l}{2} E | \psi \rangle + |1\rangle \frac{I - g_l}{2} E | \psi \rangle = \begin{cases} |0\rangle E | \psi \rangle, & \text{if } \beta = 1 \\ |1\rangle E | \psi \rangle, & \text{if } \beta = -1 \end{cases}\quad (5.21)$$

Hence we conclude that if the outcome of the measurement on the first qubit is $|0\rangle$[resp. $|1\rangle$], then $\beta_l$ is 1[resp. $-1$].

**Definition 5.2.1.** (i) the weight of $E \in G_n$ is the number of component of $E$ which are not equal to the identity
(ii) The distance of an stabilizer code $C(S)$ is defined by

$$\min_{E \in N(S) - S} \{ \text{weight of } E \}$$

(iii) If $C(S)$ is a $[n, k]$ stabilizer code with distance $d$, then we say that $C(S)$ is an $[n, k, d]$ stabilizer code.

If $C(S)$ is a $[n, k, d]$ stabilizer code such that $d \geq 2t + 1$, then $C(S)$ is able to correct arbitrary errors on any $t$ qubits. Suppose that $\{E_j\}$ is a subset of $G_n$ such that weight of $E_j$ is equal or less than $t$ for every $j$. Then weight of $E_j^*E_k$ is less than $2t$. Since $d \geq 2t + 1$, $E_j^*E_k \notin N(S) - S$.

### 5.3 Describing CSS codes as stabilizer codes

Suppose that $C_i$ be $[n, k_i]$ linear codes for $i = 1, 2$ such that $C_2 \subset C_1$ and $C_1, C_2^\perp$ both correct $t$ errors. Consider $CSS(C_1, C_2)$. Put

$$G := \begin{bmatrix} H[C_2^\perp] & 0 \\ 0 & H[C_1] \end{bmatrix}$$

(5.22)

Note that $G$ is a $(n - (k_1 - k_2)) \times 2n$ matrix. Choose $g_1, \cdots, g_{n-(k_1-k_2)} \in G_n$ so that

$$G = \begin{bmatrix} r(g_1) \\ \vdots \\ r(g_{n-(k_1-k_2)}) \end{bmatrix}$$

(5.23)

and $g_i$’s multiplicative factor are all 1. Let $S$ be a subgroup of $G_n$ generated by $g_1, \cdots, g_{n-(k_1-k_2)}$. Since the scalar multiplication factors of generators are all 1, $S$ does not contain $-I$. Since the rows of $H[C_2^\perp]$ and the rows of $H[C_1]$ are linearly independent, respectively, we have the fact that $G$ has...
linearly independent rows. So \(g_1, \ldots, g_{n-(k_1-k_2)}\) are independent by the lemma 5.1.2. Note that

\[
(GA^T)_{i,j} = e^T_i GA e_j = (G^T e_i)^T A G^T e_j = r(g_i) A r(g_j).
\]

(5.24)

On the other hand,

\[
GA^T = \begin{bmatrix}
H[C_2^\perp] & 0 \\
0 & H[C_1]
\end{bmatrix}
\begin{bmatrix}
0 & I \\
I & 0
\end{bmatrix}
\begin{bmatrix}
H[C_2^\perp] & 0 \\
0 & H[C_1]
\end{bmatrix}^T
\]

(5.25)

\[
= \begin{bmatrix}
0 & H[C_2^\perp]^T \\
H[C_1] & 0
\end{bmatrix}
\begin{bmatrix}
H[C_2^\perp]^T & 0 \\
0 & H[C_1]^T
\end{bmatrix}
\]

In the above equation, \(H[C_1] G[C_2] = O\) follows from the fact that \(C_2 \subset C_1\). By the equation 5.24 and 5.25, we have

\[
r(g_i) A r(g_j)^T = 0 \text{ for any } i, j
\]

and so we conclude that \(g_1, \ldots, g_{n-(k_1-k_2)}\) commute by the proposition ??.

Now consider the \([n, k_1-k_2]\) stabilizer code \(C(S)\) with the stabilizer \(S\). We shall show that

\[
CSS(C_1, C_2) = C(S).
\]

Since the dimension of \(CSS(C_1, C_2)\) and \(C(S)\) are same as \(2^{k_1-k_2}\), it suffices to show that \(CSS(C_1, C_2) \subset C(S)\). Recall that \(\{|x+C_2|x \in C_1\}\) forms an orthonormal basis for \(CSS(C_1, C_2)\). We will show that \(\sum_{y \in C_2} |x+y\) is stabilized by \(g_l\) for \(l = 1, \ldots, n-(k_1-k_2)\).
CHAPTER 5. STABILIZER CODES

i) \( 1 \leq i \leq k_2 \)

\[
r(g_i) = \left[ \begin{array}{c}
    i \text{ th row of } H[C_2^\perp] \\
    0 \cdots 0
  \end{array} \right] = \left[ \begin{array}{c}
    (G[C_2]e_i)^T \\
    0 \cdots 0
  \end{array} \right] \tag{5.26}
\]

and so

\[
g_i \sum_{y \in C_2} |x + y\rangle = \sum_{y \in C_2} |x + y + G[C_2]e_i\rangle
= \sum_{y \in C_2} |x + y\rangle \tag{5.27}
\]

ii) \( k_2 + 1 \leq i \leq n - (k_1 - k_2) \)

\[
r(g_i) = \left[ \begin{array}{c}
    0 \cdots 0 \\
    (i - k_2) \text{th row of } H[C_1]
  \end{array} \right] = \left[ \begin{array}{c}
    0 \cdots 0 \\
    e^T_{i-k_2} H[C_1]
  \end{array} \right] \tag{5.28}
\]

and so

\[
g_i \sum_{y \in C_2} |x + y\rangle = \sum_{y \in C_2} (-1)^{e^T_{i-k_2} H[C_1](x+y)} |x + y\rangle
= \sum_{y \in C_2} (-1)^0 |x + y\rangle
= \sum_{y \in C_2} |x + y\rangle \tag{5.29}
\]

5.4 Standard form and logical basis states

Consider a \([n, k]\) stabilizer code \(C(S)\) with the stabilizer \(S = < g_1, \cdots, g_{n-k} >\)
and let

\[
G = [G_1|G_2]
\]
CHAPTER 5. STABILIZER CODES

denote the check matrix for \(C(S)\) where \(G_1\) and \(G_2\) are \((n-k) \times 2n\) matrices.

Between actions on the check matrix \(G\) and the stabilizer code \(C(S)\), there exist following correspondence:

- swapping rows \(\iff\) relabeling generators
- swapping columns on both side \(\iff\) relabeling qubits
- adding two rows \(\iff\) multiplying generators

Using Gaussian elimination we can obtain an equivalent stabilizer code with the check matrix in the form

\[
\begin{bmatrix}
  I & A_1 & A_2 & B & 0 & C \\
  0 & 0 & 0 & D & I & E
\end{bmatrix}
\]

where \(r\) is the rank of \(G_1\). We say that a stabilizer code is in the standard form if the check matrix of the code is in the form (5.30).

Now suppose we have a \([n, k]\) stabilizer code \(C(S)\) in the standard form

\[
G = \begin{bmatrix}
  I & A_1 & A_2 & B & 0 & C \\
  0 & 0 & 0 & D & I & E
\end{bmatrix}.
\]

We will define the logical \(Z\) operators and the logical computational basis states of this code. Put

\[
G_z = \begin{bmatrix}
  0 & 0 & 0 & A_2^T & 0 & I
\end{bmatrix}
\]

and choose operators \(\tilde{Z}_1, \cdots, \tilde{Z}_k \in G_n\) with the check matrix \(G_z\). Then

\[
\begin{bmatrix}
  G \\
  G_z
\end{bmatrix} = \begin{bmatrix}
  I & A_1 & A_2 & B & 0 & C \\
  0 & 0 & 0 & D & I & E \\
  0 & 0 & 0 & A_2^T & 0 & I
\end{bmatrix}
\]
CHAPTER 5. STABILIZER CODES

has the full rank. So \( g_1, \ldots, g_{n-k}, \bar{Z}_1, \ldots, \bar{Z}_k \) are independent by the lemma 5.1.2. Also observe that

\[
G \Lambda G^T = \begin{bmatrix}
I & A_1 & A_2 & B & 0 & C \\
0 & 0 & 0 & D & I & E \\
0 & I & 0 & 0 & 0 & 0
\end{bmatrix} \begin{bmatrix}
0 & A_2^T & 0 & I
\end{bmatrix}^T
\]

(5.32)

Since \((G \Lambda G^T)_{ij} = r(g_i)Ar(\bar{Z}_j)^T\) for \( i = 1, \ldots, n-k \) and \( j = 1, \ldots, k \), the equation 5.32 implies that \( \bar{Z}_i, i = 1, \ldots, k \) commute with every generators of \( S \) by the lemma 5.1.1. Further, the operators in \( \{ \bar{Z}_i \} \) commute with one other because each operators consist of Pauli Z operators. Thus the set of operators \( \{ g_1, \ldots, g_{n-k}, \bar{Z}_1, \ldots, \bar{Z}_k \} \) is commuting and independent.

we define \( |x_1 \cdots x_k\rangle_L \) be the state stabilized by

\[ g_1, \ldots, g_{n-k}, (-1)^{x_1} \bar{Z}_1, \ldots, (-1)^{x_k} \bar{Z}_k. \]

An such state is unique up to global phase since the dimension of the space \( V_{<g_1, \ldots, g_{n-k}, (-1)^{x_1} \bar{Z}_1, \ldots, (-1)^{x_k} \bar{Z}_k>} \) is one by the theorem 5.1.1. Furthemore, if \( (x_1, \ldots, x_k) \neq (x'_1, \ldots, x'_k) \) then the states \( |x_1 \cdots x_k\rangle_L \) and \( |x'_1 \cdots x'_k\rangle_L \) are orthonormal since these states are eigenvectors with different eigenvalues for some Hermition operator \( \bar{Z}_i \). Thus \( \{|x_1 \cdots x_k\rangle_L : (x_1, \ldots, x_k) \in \mathbb{F}_2^k\} \) forms a orthonormal basis for \( C(S) \).

By the definition of the logocal basis states, the operators \( \bar{Z}_i \) play a role of the Pauli Z operators:

\[ \bar{Z}_i |x_1 \cdots x_k\rangle_L = (-1)^{x_i} |x_1 \cdots x_k\rangle \]
5.5 Encoding Stabilizer Codes

In this section, we will construct an encoding circuit for stabilizer codes. Suppose that we have \([n, k]\) stabilizer code \(C(S)\) with the stabilizer \(S = \langle g_1, \cdots, g_{n-k} \rangle\) whose check matrix is in the standard form as the equation 5.31.

**Logical X operators**

In order to use a certain unitary operator \(L \in G_n\) as a nontrivial logical operator on \(C(S)\), the following two conditions should be satisfied.

1. The operator \(L\) commutes with the generators \(\{g_1, \cdots, g_{n-k}\}\) of the stabilizer \(S\).

2. The subset \(\{L, g_1, \cdots, g_{n-k}\}\) is independent.

If the operator \(L\) anti-commute with some \(g_i\), then \(L|\psi\rangle \notin C(S)\) for any codeword \(|\psi\rangle\) since \(L|\psi\rangle\) is not stabilized by \(g_i\):

\[
g_i L|\psi\rangle = L(L^* g_i L)|\psi\rangle = L(-g_i)|\psi\rangle = -L|\psi\rangle.
\]

Also if \(L\) is represented by a product of generators of \(S\), then the operator \(L\) does not change any state in \(C(S)\). Recall that the logical \(Z\) operators in the section 5.4 satisfy the two conditions.

Now we will construct the logical \(X\) operators. Let

\[
G_x := \left[ \begin{array}{cccc} 0 & E^T & I & C^T \\ \end{array} \right] \quad \text{(5.33)}
\]

and choose \(\bar{X}_1, \cdots, \bar{X}_k \in G_n\) with the check matrix \(G_x\). Then

\[
\left[ \begin{array}{c} G \\ G_x \end{array} \right] = \left[ \begin{array}{ccc|ccc} I & A_1 & A_2 & B & 0 & C \\ 0 & 0 & 0 & D & I & E \\ 0 & E^T & I & C^T & 0 & 0 \end{array} \right] \quad \text{(5.34)}
\]
has full rank. So \( g_1, \ldots, g_{n-k}, \bar{X}_1, \ldots, \bar{X}_k \) are independent by the lemma 5.1.2. Also, the equation

\[
\begin{bmatrix}
G \\
G_x
\end{bmatrix}
\Lambda G_x^T = \begin{bmatrix}
I & A_1 & A_2 \\
0 & 0 & 0 \\
0 & E^T & I
\end{bmatrix}
\begin{bmatrix}
B & 0 & C \\
D & I & E \\
C^T & 0 & 0
\end{bmatrix}
\begin{bmatrix}
0 & I \\
I & 0
\end{bmatrix}
\begin{bmatrix}
0 \\
E \\
C \\
0 \\
0
\end{bmatrix}
\]

(5.35)

implies that \( \{g_1, \ldots, g_{n-k}, \bar{X}_1, \ldots, \bar{X}_k\} \) is a commuting set by the lemma 5.1.1. Furthermore,

\[
G_z \Lambda G_x^T = \begin{bmatrix}
0 & 0 & 0 \\
A_2^T & 0 & I
\end{bmatrix}
\begin{bmatrix}
0 & I \\
I & 0
\end{bmatrix}
\begin{bmatrix}
0 & E^T & I \\
C^T & 0 & 0
\end{bmatrix}
\]

(5.36)

Hence \( r(\bar{Z}_i)\Lambda r(\bar{X}_j)^T = (G_z \Lambda G_x^T)_{ij} = \delta_{ij} \). Thus we have

\[
\bar{X}_j \bar{Z}_i \bar{X}_j^* = (-1)^{\delta_{ij}} \bar{Z}_i
\]

(5.37)

The equation 5.37 implies that if a state \(|\psi\rangle\) is stabilized by \( \bar{Z}_i \) then the state \( \bar{X}_j |\psi\rangle \) is stabilized by \( (-1)^{\delta_{ij}} \bar{Z}_i \). Thus the operators \( \bar{X}_1, \ldots, \bar{X}_k \in G_n \) play the role of encoded Pauli \( X \) operators:

\[
\bar{X}_j |\cdots, c_j, \cdots\rangle_L = |\cdots, c_j + 1, \cdots\rangle_L
\]
CHAPTER 5. STABILIZER CODES

Construction of encoding circuit

We want to encode as

$$|c_1 \cdots c_k\rangle \rightarrow |c_1 \cdots c_k\rangle_L.$$  \hspace{1cm} (5.38)

To do this we may describe logical state $|c_1 \cdots c_k\rangle_L$ specifically. Firstly, we will show that

$$|0 \cdots 0\rangle_L = \frac{1}{\sqrt{2^r}} \prod_{i=1}^{r} (I + g_i)|0 \cdots 0\rangle.$$  \hspace{1cm} (5.39)

Since the set of generators $\{g_1, \cdots, g_{n-k}\}$ of $S$ is a commuting and independent set, any element of $S$ is written in the form $g_1^{x_1} \cdots g_{n-k}^{x_{n-k}}$ uniquely where $(x_1, \cdots, x_{n-k}) \in \mathbb{F}_2^{n-k}$. Hence

$$\sum_{g \in S} g = \sum_{(x_1, \cdots, x_{n-k}) \in \mathbb{F}_2^{n-k}} g_1^{x_1} \cdots g_{n-k}^{x_{n-k}} = \prod_{i=1}^{n-k} (I + g_i).$$

For any $g' \in S$, the equation $g' \sum_{g \in S} g = \sum_{g \in S} g' g = \sum_{g \in S} g$ holds and so $\sum_{g \in S} g|0 \cdots 0\rangle$ is stabilized by $S$. Also, recall that the logical $Z$ operators consists of only Pauli $Z$ operators and commute with generators of the stabilizer. So $\sum_{g \in S} g|0 \cdots 0\rangle$ is stabilized by $\tilde{Z}_1, \cdots, \tilde{Z}_k$. From the check matrix of $C(S)$ we can observe that $g_{r+1}, \cdots, g_{n-k}$ consist of only Pauli $Z$ operators and so these stabilize the state $|0 \cdots 0\rangle$. Therefore

$$\frac{1}{2^{n-k-r}} \prod_{i=1}^{n-k} (I + g_i)|0 \cdots 0\rangle = \prod_{i=1}^{r} (I + g_i)|0 \cdots 0\rangle.$$  \hspace{1cm} (5.39)

So far we have seen that $\prod_{i=1}^{r} (I + g_i)|0 \cdots 0\rangle$ is the vector in $C(S)$ and stabilized by the logical $Z$ operators. Note that $g_i$ flips only $i$th qubits among the first $r$ qubits for $i = 1, \cdots, r$. So $\{g_1^{x_1} \cdots g_r^{x_r}|0 \cdots 0\rangle : (x_1, \cdots, x_r) \in \mathbb{F}_2^r\}$
is an orthonormal set. Thus
\[
\frac{1}{\sqrt{2^r}} \prod_{i=1}^{r} (I + g_i)|0\cdots0\rangle = \frac{1}{\sqrt{2^r}} \sum_{\in \mathbb{F}_2^{r}} g_{x_1}^{x_1} \cdots g_{x_r}^{x_r} |0\cdots0\rangle
\]
is an unit vector and we conclude that the equation 5.39 holds.

Now we have
\[
|c_1 \cdots c_k\rangle_L = \prod_{j=1}^{k} \tilde{X}_j^{c_j} |0\cdots0\rangle_L
= \frac{1}{\sqrt{2^r}} \prod_{j=1}^{k} \tilde{X}_j^{c_j} \prod_{i=1}^{r} (I + g_i)|0\cdots0\rangle
= \frac{1}{\sqrt{2^r}} \prod_{i=1}^{r} (I + g_i) \prod_{j=1}^{k} \tilde{X}_j^{c_j} |0\cdots0\rangle.
\]
Using \((n-k)\) ancilla qubits, we will construct encoding circuit of the form in the figure 5.2. Since the check matrix of \(\tilde{X}_1, \cdots, \tilde{X}_k \in G_n\) is
\[
G_x = \begin{bmatrix} 0 & E^T & \tilde{I} & C^T & 0 & 0 \end{bmatrix},
\]
each logical operators \(\tilde{X}_i, i = 1, \cdots, k\) can be written as
\[
\tilde{X}_i = \left( \prod_{j=1}^{r} Z_j^{(C^T)_{ij}} \right) \left( \prod_{j=1}^{n-k-r} X_{r+j}^{(E^T)_{ij}} \right) X_{n-k+i}, i = 1, \cdots, k.
\]
The part of $\tilde{X}_i$ acting on first $r$ qubits, $\prod_{j=1}^{r} Z_j^{(CT)ij}$, does not change $|0\cdots0\rangle$ and so we can ignore this part for our purpose. Let $\tilde{X}_i$ denote $\prod_{j=1}^{n-k-r} X_j^{(ET)ij}$. Since the state obtained by applying $\tilde{X}_i$ to a state of the form $|\cdots c_i\cdots\rangle$ controlled on $(n-k+i)$th qubit equal $\tilde{X}_i X_{n-k+i} |\cdots 0\cdots\rangle$, we get the state $\prod_{j=1}^{k} \tilde{X}_j^{c_j} |0\cdots0\rangle$ by the circuit in the figure 5.3. Note that the first $r$ qubits of $\prod_{j=1}^{k} \tilde{X}_j^{c_j} |0\cdots0\rangle$ are still $|0\rangle$’s.

Next step is applying

$$\frac{1}{\sqrt{2^r}} \prod_{i=1}^{r} (I + g_i) = \frac{1}{\sqrt{2^r}} \sum_{(x_1,\cdots,x_r) \in \mathbb{F}_2^r} g_1^{x_1} \cdots g_r^{x_r}$$

to the state $\prod_{j=1}^{k} \tilde{X}_j^{c_j} |0\cdots0\rangle$. Let $\tilde{g}_j$ denote the operator obtained by replacing $j$th component of $g_j$ with $I$. So we may regard each $\tilde{g}_j$ as an operator not acting $j$th qubit. Recall the fact that $g_i$ flips only $i$th qubits
among the first $r$ qubits for $i = 1, \ldots, r$. Then we have

$$\left( \prod_{j=1}^{r} C_j(g_j) \right) \left( \prod_{j=1}^{r} Z^{(B)}_{jj} \right) H^{\otimes r} |0\cdots 0\cdots\rangle$$

$$= \left( \prod_{j=1}^{r} C_j(g_j) \right) \left( \prod_{j=1}^{r} Z^{(B)}_{jj} \right) \left( \frac{1}{\sqrt{2^r}} \sum_{(x_1, \ldots, x_r) \in \mathbb{F}_2^r} |x_1 \cdots x_r \cdots\rangle \right)$$

$$= \frac{1}{\sqrt{2^r}} \prod_{j=1}^{r} (I + g_j) |0\cdots 0\cdots\rangle$$

where $C_j(U)$ denote the operator that applying $U$ conditioned on $j$th qubit.

Thus we can construct an encoding circuit as the figure 5.4.
Bibliography


BIBLIOGRAPHY


국문초록

양자오류정정부호는 양자 정보를 오류로부터 보호하기 위해 사용된다. 이 논문에서 우리는 CSS부호와 안정 부호의 구조와 오류 정정 과정에 대해서 설명한다. 또한 CSS부호를 안정 부호의 맥락에서 설명하고, 안정 부호의 논리적 기저 상태와 부호화 회로에 대해서 논의한다.

주요어휘: 양자오류정정부호, CSS부호, 안정 부호
학번: 2014-22356