

QUANTUM STABILIZER CODES

by

REZA DASTBASTEH

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University

May 2017

QUANTUM STABILIZER CODES

APPROVED BY

Prof. Dr. Cem Güneri
(Thesis Supervisor)

Assoc. Prof. Dr. Kağan Kurşungöz

Assist. Prof. Dr. Seher Tutdere

DATE OF APPROVAL:

©Reza Dastbasteh 2017

All Rights Reserved

QUANTUM STABILIZER CODES

Reza Dastbasteh

Mathematics, Master Thesis, May 2017

Thesis Supervisor: Prof. Dr. Cem Güneri

Keywords: Quantum stabilizer codes, additive codes, self-orthogonal codes,
two-dimensional cyclic codes.

Abstract

We study quantum stabilizer codes and their connection to classical block codes. In addition, different constructions of quantum stabilizer codes and methods of modifying them are presented. Two-dimensional cyclic codes are recalled and a new method of obtaining quantum codes from 2-D cyclic codes is given. We also present a method of obtaining quantum stabilizer codes using additive codes over \mathbb{F}_4 .

KUANTUM SABITLEYEN KODLAR

Reza Dastbasteh

Matematik, Yüksek Lisans Tezi, Mayıs 2017

Tez Danışmanı: Prof. Dr. Cem Güneri

Anahtar Kelimeler: Kuantum sabitleyen kodlar, toplamsal kodlar, kendine dik kodlar, iki boyutlu devirsel kodlar.

Özet

Bu tezde kuantum sabitleyen kodlar ve klasik blok kodlarla ilişkileri çalışılmıştır. Çeşitli kuantum sabitleyen kod inşaları ve bu kodları dönüştürme metotları sunulmuştur. İki boyutlu devirsel kodlar yoluyla kuantum sabitleyen kodlar inşa edilmiş, bunun yanı sıra \mathbb{F}_4 üzerinde toplamsal kodlar kullanılarak kuantum sabitleyen kod inşası sunulmuştur.

To My Family

Acknowledgments

This thesis would not have been possible without the support of many people. First and foremost I would like to express my deepest gratitude to my advisor Dr. Cem Güneri whose guidance, support and assistance from the initial to the final phase has enabled me to successfully develop this thesis.

I would like to thank my committee members, Dr. Kağan Kurşungöz and Dr. Seher Tutdere who have offered their assistance throughout this period.

Finally, I would like to thank my parents, who were not here with me throughout my studies, but they motivated me to pursue the master degree and I constantly received their love and support.

Last but not the least, I would like to thank my wife, Zohreh for her love and unyielding support. Thank you god for giving me all the strength that I needed.

Table of Contents

Abstract	v
Özet	vi
Acknowledgments	viii
1 Introduction	1
1.1 History and Overview	1
1.2 Cyclic Codes	2
1.3 Two Dimensional (2-D) Cyclic Codes	3
1.4 Hermitian Dual of 2-D Cyclic Codes	4
1.5 Characterization of 2-D Cyclic Codes	7
2 Quantum Error Correction Codes	9
2.1 Binary Stabilizer Quantum Codes	9
2.2 General Constructions of Quantum Stabilizer Codes	10
2.3 Quantum Stabilizer Codes from Nearly Self-orthogonal Quaternary Linear Codes	13
2.4 Non-binary Quantum Stabilizer Codes	16
3 New Constructions of Quantum Stabilizer Codes	20
3.1 2-D Cyclic Quantum Stabilizer Codes	20
3.2 New Quantum Stabilizer Codes Construction Using 2-D Cyclic Codes .	21
3.3 General Quantum Stabilizer Codes Construction Using Classical Additive Codes	24
Bibliography	27

CHAPTER 1

Introduction

1.1. History and Overview

The correspondence between quantum codes and the classical code is a topic which has been studied during the past two decades. There are some similarities between quantum codes and classical codes and we can find a construction for quantum codes by using classical codes. As well as similarities, there are also some substantial differences. [6, 16] are good references that describe the physical and information theoretic motivations behind quantum codes.

In 1995, Shor showed the existence of quantum error-correcting codes [12]. Then, Calderbank and Shor showed that quantum codes can be obtained by using self-orthogonal classical quaternary codes [2]. Around the same time, Steane in [14, 15] discovered the existence of good quantum codes with a similar construction. In 1998, Calderbank et al. proposed the exact relation and introduced a wide range of constructions of quantum codes by using classical codes over \mathbb{F}_4 [3]. At the same time, Gottesman independently studied the quantum codes in his Ph.D. thesis and presented some new ideas of constructing quantum codes [7]. In 2001, Ashikhmin and Knill extended the construction and introduced non-binary quantum stabilizer codes (quantum codes obtained from classical self-orthogonal codes) [1]. The motivation for studying quantum stabilizer codes is due to available simple encoding and decoding algorithms. Finally, Lisonek and Singh proposed a slightly different method of constructing quantum stabilizer codes from linear codes over \mathbb{F}_4 in 2014 [10].

In this work, we only consider the quantum stabilizer codes which can be constructed from classical codes. We mostly use [1, 3, 10]. This thesis is organized as follows:

In Section 1.2, we briefly review cyclic codes and the connection between cyclic codes and polynomial rings. Section 1.3 is concerned with 2-D cyclic codes, a generalization of cyclic codes. We study the connection of 2-D cyclic codes with the polynomial rings, how to find zeros of a 2-D cyclic codes, and a method of finding the Euclidean dual of a 2-D cyclic codes. In section 1.4, we investigate the Hermitian dual of 2-D cyclic codes. Then, in Section 1.5, we give a characterization of all 2-D cyclic codes. Our contribution in this chapter is Section 1.4. The main references of this chapter are [4, 9, 11].

In chapter 2, we study the connection between quantum stabilizer codes and self-orthogonal classical codes. The definition of binary stabilizer codes is presented in Section 2.1. Next, we introduce some general methods of modifying and constructing

binary quantum stabilizer codes in Section 2.2. In Section 2.3, we explain a method of obtaining quantum codes from an arbitrary linear code over \mathbb{F}_4 . Finally, in the last section, we generalize the quantum stabilizer codes construction to the non-binary case, and propose a method of constructing non-binary quantum stabilizer codes. Our main references of this chapter are [1, 3, 5, 10].

In Chapter 3, we present some new constructions of quantum stabilizer codes. For example, we define 2-D cyclic quantum stabilizer codes and characterize all the 2-D cyclic quantum codes in Section 3.1. In Section 3.2, a new method of obtaining quantum codes from 2-D cyclic codes is proposed. Finally, we present a general method of constructing quantum stabilizer codes (both binary and non-binary) from any additive code.

1.2. Cyclic Codes

Let \mathbb{F}_q be a finite field with characteristic p . A q -ary linear code C of length n and dimension k is a k -dimensional subspace of \mathbb{F}_q^n . Each element of a linear code C is called a *codeword*. The *weight* of the codeword $v \in C$ is defined as the number of non-zero coordinates of v . The minimum nonzero weight of code C is called the *minimum distance* of C . We denote a linear code of length n , dimension k , and minimum distance d as $[n, k, d]$ code. Finally, the set of elements in \mathbb{F}_q^n which are orthogonal to all members of C , with respect to the usual (Euclidean) inner product on \mathbb{F}_q^n , is called the *dual* of the code C and is denoted by C^\perp .

Definition 1.2.1 A linear code is called *cyclic* if for every $c = (c_0, c_1, \dots, c_{n-1}) \in C$, $(c_{n-1}, c_0, \dots, c_{n-2})$ is also in C .

In other words, a linear code which is closed under cyclic shift is called cyclic. Obviously, dual of a cyclic code is also a cyclic code. We assume $(n, p) = 1$.

Note that the following map is an \mathbb{F}_q -vector space isomorphism:

$$\begin{aligned} \phi : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q[x] / \langle x^n - 1 \rangle \\ \phi((a_0, a_1, \dots, a_{n-1})) &\longmapsto \sum_{i=0}^{n-1} a_i x^i. \end{aligned}$$

Now, we have the following useful criteria for cyclic codes.

Proposition 1.2.1 A linear code C in \mathbb{F}_q^n is cyclic if and only if $\phi(C)$ is an ideal of $\mathbb{F}_q[x] / \langle x^n - 1 \rangle$.

Proof: Being closed under cyclic shift in \mathbb{F}_q^n is equivalent to being closed under multiplication by x in $\mathbb{F}_q[x] / \langle x^n - 1 \rangle$. \square

Note that the ring $\mathbb{F}_q[x] / \langle x^n - 1 \rangle$ is a principal ideal ring, so its ideals can be generated by a single polynomial. The generator polynomial of each ideal, which is a unique monic polynomial of the lowest degree, is called the *generator polynomial* of the cyclic code. If $g(x)$ is the generator polynomial of the code C , then $\dim(C) = n - \deg(g(x))$.

Remark 1.2.1 Let $g(x)$ be the generator polynomial of the code C . Then the roots of $g(x)$ in extensions of \mathbb{F}_q are called *zeros* of the code C , which are the common zeros of all codewords. The assumption $(n, p) = 1$ guarantees that $x^n - 1$, hence $g(x)$, is separable. Hence, the number of zeros is equal to the degree of $g(x)$.

1.3. Two Dimensional (2-D) Cyclic Codes

Consider the set

$$\mathbb{F}_q^{n_1 \times n_2} = \left\{ \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & \cdots & a_{0,n_2-1} \\ a_{1,0} & a_{1,1} & a_{1,2} & \cdots & a_{1,n_2-1} \\ \vdots & \vdots & \vdots & \cdots & \ddots \\ a_{n_1-1,0} & a_{n_1-1,1} & a_{n_1-1,2} & \cdots & a_{n_1-1,n_2-1} \end{bmatrix} \mid a_{i,j} \in \mathbb{F}_q \right\},$$

where n_1 and n_2 are positive integers. This set is an $n_1 n_2$ -dimensional vector space over \mathbb{F}_q .

Definition 1.3.2 A linear code $C \subseteq \mathbb{F}_q^{n_1 \times n_2}$ is called a *2-D cyclic code* of area $n_1 \times n_2$ if $(a_{i+s,j+t})$ is also in C for all s and t , where $i+s$ and $j+t$ are taken modulo n_1 and n_2 , respectively.

In other words, a two dimensional (2-D) cyclic code of area $n_1 \times n_2$ is an \mathbb{F}_q linear code $C \subseteq \mathbb{F}_q^{n_1 \times n_2}$ where C is closed under both column and row shifts. Note that similar to the cyclic case, the dual of a 2-D cyclic code is a 2-D cyclic code and also we have an alternative representation for 2-D cyclic codes. Consider the following \mathbb{F}_q -vector space isomorphism:

$$\begin{aligned} \phi : \mathbb{F}_q^{n_1 \times n_2} &\longrightarrow \mathbb{F}_q[x, y] / \langle x^{n_1} - 1, y^{n_2} - 1 \rangle \\ \phi((a_{i,j})) &\longmapsto \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a_{i,j} x^i y^j. \end{aligned}$$

Proposition 1.3.2 A linear code $C \subseteq \mathbb{F}_q^{n_1 \times n_2}$ is 2-D cyclic if and only if $\phi(C)$ is an ideal of $\mathbb{F}_q[x, y] / \langle x^{n_1} - 1, y^{n_2} - 1 \rangle$.

Proof: Being closed under row and column shifts are equivalent to being closed under multiplication by x and y , respectively. Rest of the proof is clear. \square

From now on we assume that n_1 and n_2 are relatively prime to $p = \text{char}(\mathbb{F}_q)$. Let α_1 be a primitive n_1 th root of unity and α_2 be a primitive n_2 th root of unity. We take both of these elements in the smallest extension \mathbb{F}_{q^s} of \mathbb{F}_q such that n_1 and n_2 divide $q^s - 1$. Consider the following set:

$$\Omega = \{(\alpha_1^i, \alpha_2^j) \mid 0 \leq i \leq n_1 - 1, 0 \leq j \leq n_2 - 1\}.$$

The \mathbb{F}_q -conjugacy class of (α_1^i, α_2^j) is defined as

$$[(\alpha_1^i, \alpha_2^j)] = \{(\alpha_1^i, \alpha_2^j), (\alpha_1^{iq}, \alpha_2^{jq}), (\alpha_1^{iq^2}, \alpha_2^{jq^2}), \dots, (\alpha_1^{iq^{\delta-1}}, \alpha_2^{jq^{\delta-1}})\},$$

where δ is the least common multiple of the degrees of α_1^i and α_2^j over \mathbb{F}_q . We can write Ω as a disjoint union of these \mathbb{F}_q -conjugacy classes [4].

From now on, $U \subseteq \Omega$ will be the union of some conjugacy classes. The ideal corresponding to the set U is defined as $I(U) = \{f(x, y) \in \mathbb{F}_q[x, y] \mid f(a) = 0 \text{ for any } a \in U\}$.

Remark 1.3.2 Note that for any $U \subseteq \Omega$, both of $x^{n_1}-1$ and $y^{n_2}-1$ are in $I(U)$. Therefore, $\langle x^{n_1}-1, y^{n_2}-1 \rangle \subseteq I(U)$ and we can consider $\tilde{I}(U) = I(U)/\langle x^{n_1}-1, y^{n_2}-1 \rangle$. The ideal $\tilde{I}(U)$ is called the 2-D cyclic code associated to $U \subseteq \Omega$.

Definition 1.3.3 Let $\tilde{J} = J/\langle x^{n_1}-1, y^{n_2}-1 \rangle$ be a 2-D cyclic code. Then the set

$$Z(\tilde{J}) = \{(\alpha, \beta) \in \Omega \mid f(\alpha, \beta) = 0 \text{ for any } f \in \tilde{J}\}$$

is called the zero set of the 2-D cyclic code \tilde{J} .

Example 1.3.3 Let $q = 2$, $n_1 = 3$, and $n_2 = 5$. We fix a primitive root of unity $\alpha \in \mathbb{F}_{16}$ which satisfies the equation $x^4 + x + 1 = 0$. So α^5 and α^3 are 3rd and 5th roots of unity, respectively. Put $\alpha_1 = \alpha^5$ and $\alpha_2 = \alpha^3$. Then Ω is

$$\Omega = \{(\alpha_1^i, \alpha_2^j) \mid 0 \leq i \leq 2, 0 \leq j \leq 4\}.$$

Let C be a 2-D cyclic code with the polynomial representation

$$\tilde{I} = \langle (x+1)(y^4 + y^3 + y^2 + y + 1), (y+1)(x^2 + x + 1) \rangle / \langle x^3 - 1, y^5 - 1 \rangle.$$

Then

$$Z(C) = [(1, 1)] \cup [(\alpha_1, \alpha_2)] \cup [(\alpha_1^2, \alpha_2)].$$

Now, we present the following statements without proof. See [4,9] for further details and proofs.

Proposition 1.3.4 Let $U \subseteq \Omega$. Then $Z(\tilde{I}(U)) = U$

Theorem 1.3.5 Let U be a subset of Ω and $\bar{U} = \Omega - U$. Consider the 2-D cyclic code C_U corresponding to the ideal $I(U)/\langle x^{n_1}-1, y^{n_2}-1 \rangle$. Then dimension of the code C_U is equal to $|\bar{U}|$.

Proposition 1.3.6 Let C_U be the 2-D cyclic code with the zero set U and polynomial representation $I(U)/\langle x^{n_1}-1, y^{n_2}-1 \rangle$. Then its dual is the 2-D cyclic code $C_{\bar{U}^{-1}}$, which has the zero set

$$Z(C_U^\perp) = Z(C_{\bar{U}^{-1}}) = \bar{U}^{-1} = \Omega - U^{-1},$$

where $U^{-1} = \{(\mu_1^{-1}, \mu_2^{-1}) \mid (\mu_1, \mu_2) \in U\}$.

1.4. Hermitian Dual of 2-D Cyclic Codes

In this section, we assume that \mathbb{F}_q is a finite field, where $q = p^2$ and p is a prime number. Denote the conjugate of $a \in \mathbb{F}_q$ by \bar{a} , where $\bar{a} = a^p$. For $a, b \in \mathbb{F}_q$ we denote the

Hermitian inner product of a and b with $\langle a, b \rangle = \sum_{i=1}^n a_i \bar{b}_i$. If $f(x, y) = \sum_{i=0}^s \sum_{j=0}^t a_{i,j} x^i y^j$

is a polynomial in $\mathbb{F}_q[x, y]$ we define $\overline{f(x, y)} = \sum_{i=0}^s \sum_{j=0}^t \bar{a}_{i,j} x^i y^j$.

Lemma 1.4.7 Let $f(x, y)$ and $g(x, y)$ be polynomials in $\mathbb{F}_q[x, y]$. Then the following hold:

1. $\overline{f(x, y) + g(x, y)} = \overline{f(x, y)} + \overline{g(x, y)}$.
2. $\overline{f(x, y).g(x, y)} = \overline{f(x, y)}. \overline{g(x, y)}$.
3. $\overline{\overline{f(x, y)}} = f(x, y)$

Corollary 1.4.8 For any ideal I in $F_q[x, y]$, $\bar{I} = \{\bar{f} \mid f \in I\}$ is also an ideal of $F_q[x, y]$.

It is clear that $\overline{x^{n_1} - 1} = x^{n_1} - 1$ and $\overline{y^{n_2} - 1} = y^{n_2} - 1$. So, if $\tilde{I}(U)$ is an ideal of $\mathbb{F}_q[x, y]/\langle x^{n_1} - 1, y^{n_2} - 1 \rangle$, then $\overline{\tilde{I}(U)}$ is also an ideal of $\mathbb{F}_q[x, y]/\langle x^{n_1} - 1, y^{n_2} - 1 \rangle$.

Lemma 1.4.9 Let $\tilde{I}(U)$ be an ideal of $\mathbb{F}_q[x, y]/\langle x^{n_1} - 1, y^{n_2} - 1 \rangle$. Then $\tilde{I}(U)$ and $\overline{\tilde{I}(U)}$ are isomorphic as ideals, hence as linear codes.

Proof: Consider the map

$$\begin{aligned} \phi : I(U)/\langle x^{n_1} - 1, y^{n_2} - 1 \rangle &\longrightarrow \overline{I(U)}/\langle x^{n_1} - 1, y^{n_2} - 1 \rangle \\ f(x, y) + \langle x^{n_1} - 1, y^{n_2} - 1 \rangle &\longmapsto \overline{f(x, y)} + \langle x^{n_1} - 1, y^{n_2} - 1 \rangle. \end{aligned}$$

Assume that $f(x, y)$ and $g(x, y) \in \mathbb{F}_q[x, y]$ and $f(x, y) + \langle x^{n_1} - 1, y^{n_2} - 1 \rangle = g(x, y) + \langle x^{n_1} - 1, y^{n_2} - 1 \rangle$. Then $f(x, y) - g(x, y) \in \langle x^{n_1} - 1, y^{n_2} - 1 \rangle$ and consequently we can consider it as $f(x, y) - g(x, y) = h(x, y)(x^{n_1} - 1) + k(x, y)(y^{n_2} - 1)$ for some $h(x, y)$ and $k(x, y)$ in $\mathbb{F}_q[x, y]$. Hence $\overline{f(x, y) - g(x, y)} = \overline{h(x, y)(x^{n_1} - 1) + k(x, y)(y^{n_2} - 1)}$ which means that $\overline{f(x, y)} + \langle x^{n_1} - 1, y^{n_2} - 1 \rangle = \overline{g(x, y)} + \langle x^{n_1} - 1, y^{n_2} - 1 \rangle$. This shows that the map ϕ is well defined. By similar steps we can also show that ϕ is one-to-one. Moreover, according to Lemma 1.4.7, ϕ is a ring homomorphism. Finally, ϕ is onto since the conjugation operator is an automorphism of \mathbb{F}_q . \square

Theorem 1.4.10 Let $\tilde{I}(U)$ be an ideal of $\mathbb{F}_q[x, y]/\langle x^{n_1} - 1, y^{n_2} - 1 \rangle$. Then the zero set of the ideal $\overline{\tilde{I}(U)}$ is the set $U^p = \{(\alpha^p, \beta^p) \mid (\alpha, \beta) \in U\}$.

Proof: By Lemma 1.4.9, $\dim(\tilde{I}(U)) = \dim(\overline{\tilde{I}(U)})$. Also, since p is relatively prime to both n_1 and n_2 , $|U^p| = |U|$. So it is enough to show that $U^p \subseteq Z(\overline{\tilde{I}(U)})$. Let $\overline{f(x, y)} \in \overline{\tilde{I}(U)}$, where $f(x, y) \in \tilde{I}(U)$. We have

$$\overline{f(x, y)} = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} \overline{a_{i,j}} x^i y^j = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a_{i,j}^p x^i y^j.$$

Now, suppose $(\alpha^p, \beta^p) \in U^p$. Then,

$$\overline{f(\alpha^p, \beta^p)} = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a_{i,j}^p \alpha^{ip} \beta^{jp} = \left(\sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} a_{i,j} \alpha^i \beta^j \right)^p = (f(\alpha, \beta))^p = 0.$$

Therefore, $U^p \subseteq Z(\overline{\tilde{I}(U)})$. \square

Now, we present the main theorem of this section which allows us to find the Hermitian dual of an arbitrary 2-D cyclic code.

Theorem 1.4.11 *Let C_U be the 2-D cyclic code with the zero set U . Then, the Hermitian dual of C_U is the code $C_{\overline{U}^{-p}}$, which has the zero set $\overline{U}^{-p} = \Omega - U^{-p}$.*

Proof: Let $I(U)/\langle x^{n_1} - 1, y^{n_2} - 1 \rangle$ be the polynomial representation of the 2-D cyclic code C_U . By Proposition 1.3.6, the Euclidean dual of C_U is the code $C_{\overline{U}^{-1}}$, which has the polynomial representation $I(\overline{U}^{-1})/\langle x^{n_1} - 1, y^{n_2} - 1 \rangle$. Now, let $\overline{C_{\overline{U}^{-1}}}$ be the code corresponding to the conjugate of the ideal $I(\overline{U}^{-1})/\langle x^{n_1} - 1, y^{n_2} - 1 \rangle$. By Theorem 1.4.10, we conclude that $\overline{C_{\overline{U}^{-1}}} = C_{\overline{U}^{-p}}$.

Now, we claim that the Hermitian dual of the code C_U is $\overline{C_{\overline{U}^{-1}}}$. It's because of that

$$I(U).\overline{I(\overline{U}^{-p})} \equiv I(U).I(\overline{U}^{-1}) \quad \text{mod } \langle x^{n_1} - 1, y^{n_2} - 1 \rangle$$

and since $I(\overline{U}^{-1})/\langle x^{n_1} - 1, y^{n_2} - 1 \rangle$ is the Euclidean dual of $I(U)/\langle x^{n_1} - 1, y^{n_2} - 1 \rangle$, we have:

$$I(U).I(\overline{U}^{-1}) \equiv 0 \quad \text{mod } \langle x^{n_1} - 1, y^{n_2} - 1 \rangle.$$

□

Note that in the proof of the last theorem, the fact $(\overline{U}^{-p})^p = \overline{U}^{-1}$ is used which can be easily verified.

Example 1.4.12 Let $q = 4$ and $n_1 = n_2 = 3$. We fix a primitive root of unity $\alpha \in \mathbb{F}_4 = \{0, 1, \alpha, \bar{\alpha}\}$ which satisfies the equation $x^2 + x + 1 = 0$. So we can put $\alpha_1 = \alpha_2 = \alpha$. Then Ω is

$$\Omega = \{(\alpha_1^i, \alpha_2^j) \mid 0 \leq i \leq 2, 0 \leq j \leq 2\}.$$

Let C be the 2-D cyclic code over \mathbb{F}_4 with the polynomial representation

$$\tilde{I} = \langle (x+1)(y^2 + \alpha y + 1), (y+1)(x^2 + x + 1) \rangle / \langle x^{n_1} - 1, y^{n_2} - 1 \rangle.$$

Then

$$Z(C) = \{(1, 1), (\alpha_1, \alpha_2^2), (\alpha_1, 1), (\alpha_1^2, 1), (\alpha_1^2, \alpha_2^2)\}.$$

Note that all of these elements have a singleton conjugacy class. Now, according to Theorem 1.4.11, the zero set of the Hermitian dual of C is

$$Z(C^{\perp h}) = \Omega - (Z(C))^{-2} = \{(1, \alpha_2), (1, \alpha_2^2), (\alpha_1, \alpha_2), (\alpha_1^2, \alpha_2)\}.$$

Also, this set is the zero set of the ideal

$$\langle (y + \alpha)(x + 1), (x^2 + x + 1)(y^2 + y + 1) \rangle / \langle x^{n_1} - 1, y^{n_2} - 1 \rangle.$$

Therefore, $C^{\perp h} = \langle (y + \alpha)(x + 1), (x^2 + x + 1)(y^2 + y + 1) \rangle / \langle x^{n_1} - 1, y^{n_2} - 1 \rangle$.

Now, we state another theorem which plays a critical role in finding quantum stabilizer codes in Chapter 3.

Theorem 1.4.13 *If C_U is the 2-D cyclic code with the zero set U , then $\dim(C_U^{\perp h}) - \dim(C_U \cap C_U^{\perp h}) = |U \cap U^{-p}|$.*

Proof: By Theorem 1.3.5, $\dim(C_U) = |\bar{U}| = |\Omega - U|$. Also, from Theorem 1.4.11, we can see that $Z(C_U^{\perp h}) = \bar{U}^{-p}$. It is clear that $Z(C_U \cap C_U^{\perp h}) = U \cup \bar{U}^{-p}$. So,

$$\begin{aligned} \dim(C_U^{\perp h}) - \dim(C_U \cap C_U^{\perp h}) &= |\Omega - \bar{U}^{-p}| - |\Omega - (U \cup \bar{U}^{-p})| \\ &= n_1 n_2 - |\bar{U}^{-p}| - (n_1 n_2 - |U \cup \bar{U}^{-p}|) \\ &= |U \cup \bar{U}^{-p}| - |\bar{U}^{-p}| \\ &= |U - \bar{U}^{-p}| = |U \cap U^{-p}|. \end{aligned}$$

The last equality follows from the fact that $U = (U \cap U^{-p}) \dot{\cup} (U \cap \bar{U}^{-p})$. □

1.5. Characterization of 2-D Cyclic Codes

In this Section, we give a characterization of 2-D cyclic codes using the polynomial representation of the codes [11]. For this purpose, we assume that I is an ideal of the ring $\mathbb{F}_q[x, y]/\langle x^{n_1} - 1, y^{n_2} - 1 \rangle$ and $f(x, y) \in I$. Then $f(x, y)$ can be written as

$f(x, y) = \sum_{i=0}^{n_2-1} f_i(x)y^i$, where each $f_i(x)$ belongs to $R = \mathbb{F}_q[x]/\langle x^{n_1} - 1 \rangle$. We define the set

$$I_0 = \{g_0(x) \in R \mid \text{there exists } g(x, y) \in I \text{ such that } g(x, y) = \sum_{i=0}^{n_2-1} g_i(x)y^i\}.$$

Clearly I_0 is an ideal of the ring R . Since R is a principal ideal ring, we can write $I_0 = \langle p_0^0(x) \rangle$, where $p_0^0(x) \in R$ and $p_0^0(x) \mid x^{n_1} - 1$. So for each $f(x, y) \in I$, we have $f_0(x) \in I_0$ and therefore $p_0^0(x) \mid f_0(x)$. On the other hand, $p_0^0(x) \in I_0$ which implies that there exists $p_0(x, y) = \sum_{i=0}^{n_2-1} p_i^0(x)y^i \in I$. Hence, for every $f(x, y) \in I$ we can find $q_0(x) \in R$ such that $h(x, y) = f(x, y) - q_0(x)p_0(x, y)$ belongs to I and has no constant term relative to y . This means that if $h(x, y) = \sum_{i=0}^{n_2-1} h_i(x)y^i$, then $h_0(x) = 0$. Now, put

$$I_1 = \{g_1(x) \in R \mid \text{there exists } g(x, y) \in I \text{ such that } g(x, y) = \sum_{i=1}^{n_2-1} g_i(x)y^i\}.$$

Again, I_1 is an ideal of R which is generated by $p_1^1(x)$, where $p_1^1(x) \in R$ and $p_1^1(x) \mid x^{n_1} - 1$. Moreover, $p_1^1(x) \in I_1$ which means that there exists $p_1(x, y) \in I$ such that $p_1(x, y) = \sum_{i=1}^{n_2-1} p_i^1(x)y^i$. Now, for each $f(x, y) \in I$ we can find $q_0(x)$ and $q_1(x) \in R$ such that $h'(x, y) = f(x, y) - q_0 p_0(x, y) - q_1 p_1(x, y)$ has no constant and degree one term relative to y . In other words, if $h'(x, y) = \sum_{i=0}^{n_2-1} h'_i(x)y^i$, then $h'_0 = h'_1 = 0$. Repeating this idea, we can construct $p_i(x, y) \in I$ for $i = 0, 1, 2, \dots, n_2 - 1$. Now, it is clear that

$$I = \langle p_0(x, y), p_1(x, y), \dots, p_{n_2-1}(x, y) \rangle.$$

The polynomials $p_i(x, y)$ are called the generator polynomials of I . By the above construction, we can find some conditions on $p_i(x, y)$.

Proposition 1.5.14 *Let $p_i(x, y) \in I$ for $i = 0, 1, 2, \dots, n_2 - 1$ be the polynomials obtained from the above construction. Then we have the following properties.*

(i) $p_0^0(x) \mid p_i^j(x)$ for all $0 \leq i, j \leq n_2 - 1$.

(ii) $p_{i-1}^{i-1}(x) \mid p_i^i(x)$.

(iii) $p_i^i(x) \mid \frac{x^{n_1-1}}{p_{i-1}^{i-1}}(x)p_i^{i-1}(x)$.

Proof: (i) By the definition of I_0 , we have $p_i^j(x) \in I_0$ for all $0 \leq i, j \leq n_2 - 1$. Since $p_0^0(x)$ is the generator polynomial of the ideal I_0 , we have $p_0^0(x) \mid p_i^j(x)$.

(ii) For $i \leq j$, we have $I_j \subseteq I_i$, hence $p_{i-1}^{i-1}(x) \mid p_i^i(x)$.

(iii) Let $P_{i-1}(x, y) = \sum_{j=i-1}^{n_2-1} p_j^{i-1}(x)y^j$. Consider the polynomial

$$s(x, y) = \frac{x^{n_1-1}}{p_{i-1}^{i-1}}P_{i-1}(x, y) = \sum_{j=i}^{n_2-1} p_j^{i-1}(x) \frac{x^{n_1-1}}{p_{i-1}^{i-1}}y^j.$$

We have, $s_i = \frac{x^{n_1-1}}{p_{i-1}^{i-1}}p_{i-1}^i(x) \in I_i$, so $p_i^i(x) \mid \frac{x^{n_1-1}}{p_{i-1}^{i-1}}(x)p_i^{i-1}(x)$. □

Theorem 1.5.15 *Let I be an ideal of the ring $\mathbb{F}_q[x, y] / \langle x^{n_1} - 1, y^{n_2} - 1 \rangle$ (a 2-D cyclic code). Then we have*

$$I = \langle p_0(x, y), p_1(x, y), \dots, p_{n_2-1}(x, y) \rangle,$$

where $p_i(x, y)$'s are defined as above. Moreover, the set

$$S = \bigcup_{i=0}^{n_2-1} \{P_i(x, y), xP_i(x, y), x^2P_i(x, y), \dots, x^{n_1-a_i-1}P_i(x, y)\}$$

where $a_i = \deg(p_i^i(x))$ for $0 \leq i \leq n_2 - 1$, is an \mathbb{F}_q -basis for the 2-D cyclic code.

Proof: Elements of S generate I . It is enough to show that they are linearly independent. Assume that they are linearly dependent. So there are $k_0(x), k_1(x), \dots, k_{n_2-1}(x) \in \mathbb{F}_q[x] / \langle x^{n_1} - 1 \rangle$ such that $\deg(k_i(x)) \leq n_1 - a_i - 1$ and $\sum_{i=0}^{n_2-1} k_i(x)p_i(x, y) = 0$ in $\mathbb{F}_q[x] / \langle x^{n_1} - 1 \rangle$. This means that $k_0(x)p_0^0(x) = 0$ in $\mathbb{F}_q[x] / \langle x^{n_1} - 1 \rangle$. So, $k_0(x)p_0^0(x) = t(x)(x^{n_1} - 1)$ for some $t(x) \in \mathbb{F}_q[x]$, but $\deg(k_0(x)p_0^0(x)) < n_1 - 1$ and it implies that $k_0(x) = 0$. Similarly we can show that $k_i(x) = 0$ for $0 \leq i \leq n_2 - 1$ and this completes the proof. □

CHAPTER 2

Quantum Error Correction Codes

2.1. Binary Stabilizer Quantum Codes

Let \mathbb{F}_4 be the finite field of the elements $\{0, 1, w, w^2\}$, with $w^2 = w + 1$. We define the trace map $Tr : \mathbb{F}_4 \rightarrow \mathbb{F}_2$ with $Tr(x) = x + \bar{x}$ where $\bar{x} = x^2$. An additive subgroup of \mathbb{F}_4^n is called an *additive code*. Let $C \subseteq \mathbb{F}_4^n$ be an additive code over \mathbb{F}_4 , then the Hamming weight of $v \in C$ is the number of nonzero components of v . Consequently, the distance of two vectors $u, v \in C$ is $dist(u, v) = wt(u - v)$. Now, we can define the minimum distance of the code C with $min\{dist(u, v) | u \neq v \in C\}$.

We define the *symplectic inner product* of $u, v \in C$ with

$$u * v = Tr(u \cdot \bar{v}) = (u \cdot \bar{v}) + \overline{(u \cdot \bar{v})} = \sum_{i=1}^n (u_i \bar{v}_i + \bar{u}_i v_i).$$

If C is an $(n, 2^k)$ code its symplectic dual will be $C^{\perp_s} = \{u \in \mathbb{F}_4^n | u * v = 0 \text{ for all } v \in C\}$. It is clear that C^{\perp_s} is an $(n, 2^{2n-k})$ additive code. We say C is self-orthogonal if $C \subseteq C^{\perp_s}$. Also, if $C = C^{\perp_s}$ we call the code C a self-dual code.

Lemma 2.1.1 Suppose $C \subseteq \mathbb{F}_4^n$ is an $(n, 2^{n-k})$ additive self-orthogonal code such that $d = min\{wt(u) | u \in C^{\perp_s} \setminus C\}$. Then C can be used to construct a binary $[[n, k, d]]$ quantum stabilizer code. [3]

Definition 2.1.1 From now on, for simplicity, if the block code C satisfies the conditions of Lemma 2.1.1, we call C as $[[n, k, d]]$ *quantum (stabilizer) code*. If the block code C is linear, we call the code *linear quantum code*.

We call C *pure* if there is no nonzero vector in C^{\perp_s} with weight less than d , otherwise it is called *impure*. Note that the quantum code C with parameters $[[n, 0, d]]$ is a pure quantum code. In this special case, $k = 0$, we define $d = min\{wt(u) | u \in C \setminus \{0\}\}$. In the next theorem, we show that Hermitian dual and symplectic dual are the same if C is an \mathbb{F}_4 linear code.

Theorem 2.1.2 An \mathbb{F}_4 linear code C is self-orthogonal with respect to the symplectic inner product if and only if it is self-orthogonal with respect to the Hermitian inner product.

Proof: Suppose that C is self-orthogonal linear code with respect to the symplectic inner product. Then we have $u * v = Tr(u.\bar{v}) = 0$ for all $u, v \in C$. If $u.\bar{v} = \alpha + \beta w$ with $\alpha, \beta \in \mathbb{F}_2$, then $\bar{u}.v = \bar{u}.\bar{v} = \alpha + (w+1)\beta$. Therefore, $u * v = u.\bar{v} + \bar{u}.v = \beta$ which means that $\beta = 0$. Moreover, since C is \mathbb{F}_4 linear, $wv \in C$ and $u * wv = Tr(u.\overline{wv}) = 0$. Using the same argument we see that $\alpha = 0$ and consequently $u.\bar{v} = 0$ for all u and $v \in C$. Proof of the other direction is straightforward. \square

An $(n, 2^k)$ additive code over \mathbb{F}_4 is called *even* if the weight of each codeword in C is even. Otherwise, C is called *odd*.

Theorem 2.1.3 *An even additive code is self-orthogonal. The converse is correct for linear codes.*

Proof: Let C be an additive even code and $u, v \in C$. Let S_1 and S_2 be subsets of coordinates such that u and v have the same entries at each place of S_1 and different components of them occur in all the places of S_2 . Then,

$$wt(u + v) = wt(u) + wt(v) - 2k - r,$$

where k is the number of coordinates of S_1 such that u and v are nonzero in those places, and r is the number of places of S_2 such that u and v are both nonzero and different. By definition of the symplectic inner product, we see that $r = u * v$. So

$$wt(u + v) = wt(u) + wt(v) - 2k - r \equiv wt(u) + wt(v) + u * v \pmod{2}.$$

Since the code is even, $u * v = 0$. Conversely, if C is a linear code, then $uw \in C$ for all $u \in C$. Also,

$$0 \equiv u * uw = wt(u) \pmod{2}$$

and this completes the proof. \square

2.2. General Constructions of Quantum Stabilizer Codes

In this Section, we will introduce some general methods of constructing and modifying quantum codes over \mathbb{F}_4 . We define the *direct sum* of two quantum codes as $C \oplus C' = \{uv | u \in C, v \in C'\}$. Clearly, if C and C' are $[[n, k, d]]$ and $[[n', k', d']]$ quantum codes respectively, then $C \oplus C'$ is an $[[n + n', k + k', d'']]$ quantum code, where $d'' = \min\{d, d'\}$. Additive codes which cannot be expressed as a direct sum are called *indecomposable*. The next theorem introduces other construction methods for quantum codes.

Theorem 2.2.4 *Suppose C is an $[[n, k, d]]$ quantum code.*

- (i) *If $k > 0$, then there exists a quantum code C' with parameters $[[n + 1, k, d]]$.*
- (ii) *If C is pure and $n \geq 2$, then an $[[n - 1, k + 1, d - 1]]$ quantum code exists.*
- (iii) *If $k > 1$ or if $k = 1$ and C is pure, then an $[[n, k - 1, d]]$ quantum code exists.*
- (iv) *If $n \geq 2$, then an $[[n - 1, k, d - 1]]$ quantum code exists.*
- (v) *If $n \geq 2$ and C contains a codeword of weight 1, then an $[[n - 1, k, d]]$ quantum code exists.*

Proof: (i) Let C be an $(n, 2^{n-k})$ quantum code, where $k > 0$. Consider $C' = C \oplus C_1$, where $C_1 = \{0, 1\}$. Obviously, C' is self-orthogonal with respect to the symplectic inner product, it has 2^{n-k+1} elements, and its dual can be written as $C'^{\perp} = C^{\perp} \oplus C_1$. Therefore, it is an $[[n+1, k, d]]$ quantum code. Note that this construction does not hold when $k = 0$. Since otherwise we can construct an $[[n+1, 0]]$ code. Moreover, since $0 \oplus 1 \in C'$ and the code is pure, the minimum distance is 1.

(ii) Since C is a pure code, by deleting the first coordinate of the code C^{\perp} we obtain B^{\perp} with parameters $(n-1, 2^{n+k})$ and minimum distance at least $d-1$. So, it is enough to show that $B \subseteq B^{\perp}$. We claim that $B = \{v|0v \in C\}$. By definition of symplectic inner product $\{v|0v \in C\} \subseteq B$. Also, if $u \in B$ then $0u * c = 0$ for all $c \in C^{\perp}$ and this means that $B \subseteq B^{\perp}$.

(iii) First, suppose that $k > 1$ and $v \in C^{\perp} \setminus C$. Then the code C' generated by $C' = \langle C, v \rangle$ has parameters $(n, 2^{n-k+1})$ and it is self-orthogonal with respect to the symplectic inner product. Since $C'^{\perp} \setminus C' \subseteq C^{\perp} \setminus C$, it has minimum distance $\geq d$. So, C' is an $[[n, k-1, d]]$ quantum code. Now, in case $k = 1$, since the construction ends in an $[[n, 0]]$ quantum code, which is a pure code and we cannot guarantee the minimum distance d (in pure code we calculate minimum distance differently).

(iv) Take $B = \{u|0u \text{ or } 1u \in C\}$. We show that $B^{\perp} = \{v|0v \text{ or } 1v \in C^{\perp}\}$. It is clear that if $0v$ or $1v \in C^{\perp}$, then for any $u \in B$ we have $v * u = 0$. So $\{v|0v \text{ or } 1v \in C^{\perp}\} \subseteq B^{\perp}$. Conversely, suppose that $v \in B^{\perp}$ and, both of $0v$ and $1v$ are not in C^{\perp} . First, since $0v \notin C^{\perp}$, then there exist $s = (s_1, s_2, \dots, s_n) \in C$ such that $s_1 \in \{w, w+1\}$ and $0v * s \equiv 1 \pmod{2}$. So $(s_2, s_3, \dots, s_n) * v \equiv 1 \pmod{2}$. Next, since $1v \notin C^{\perp}$, there exists $r = (r_1, r_2, \dots, r_n) \in C$ such that $r_1 \in \{w, w+1\}$ and $1v * r \equiv 1 \pmod{2}$. Therefore, $(r_2, r_3, \dots, r_n) * v \equiv 0 \pmod{2}$. Now, $s + r = (z_1, z_2, \dots, z_n) \in C$, where $z_1 \in \{0, 1\}$. Hence, $(z_2, z_3, \dots, z_n) \in B$, which means that $v * (z_2, z_3, \dots, z_n) \equiv 0 \pmod{2}$. But, $v * (z_2, z_3, \dots, z_n) = v * (s_2, s_3, \dots, s_n) + v * (r_2, r_3, \dots, r_n) \equiv 1 + 0 \equiv 1 \pmod{2}$, and this is a contradiction. So, $B^{\perp} = \{v|0v \text{ or } 1v \in C^{\perp}\}$.

Now, if there is a vector with first coordinate w or $w+1$ in C , then $|B| \leq 2^{n-k-1}$. Otherwise, if $0u$ ($1v$) is a vector in C , then $1u$ ($0v$) is also a vector of C^{\perp} and again we conclude that $|B| \leq 2^{n-k-1}$. Moreover, since $C \subseteq C^{\perp}$ we can see that $|B^{\perp}| \leq 2^{n+k-1}$. On the other hand, $\dim(B) + \dim(B^{\perp}) = 2n - 2$. Hence, $|B| = 2^{n-k-1}$. Now we consider the minimum distance. If $t \in C^{\perp} \setminus C$, t starts with 1, and has weight d , then t after truncation is a codeword in $B^{\perp} \setminus B$ and has weight $\leq d-1$. This is why the minimum distance of new code is $d-1$.

(v) Suppose $v \in C$ such that for some $1 \leq i \leq n$, $v_i = a \neq 0$ and $v_j = 0$ for $i \neq j$. Note that for any $u \in C^{\perp}$, $u_i = 0$ or a . So by deleting the i th coordinate of C and C^{\perp} , we obtain subspaces B and B' such that $B' = B^{\perp}$. This is because of the fact that if $s \in C$ and $t \in C^{\perp}$, the symplectic inner product of i th coordinate is always equal to zero. Also, $\dim(B) \leq \dim(C) - 1$ and $\dim(B^{\perp}) \leq \dim(C^{\perp}) - 1$. On the other hand, $\dim(B) + \dim(B^{\perp}) = 2n - 2$. So B is an $[[n-1, k]]$ quantum code. Moreover, if $t \in C^{\perp} \setminus C$ with $wt(t) = d$, then $t + v \in C^{\perp} \setminus C$, so the i th coordinate of t is zero and this means $t \in B^{\perp} \setminus B$. This completes the proof. \square

Lemma 2.2.5 *Let C be a linear quantum code over \mathbb{F}_4 . Suppose that S is a subset of coordinates such that S meets each vector of C in an even weight vector. Then, the code obtained by deleting the coordinates S is also a linear quantum code.*

Proof: By Theorem 2.1.3, C is an even code. Therefore, deleting coordinates corresponding to S , we obtain another even code, which is self-orthogonal by Theorem

2.1.3. Hence, the resulting code is a quantum code again. \square

Theorem 2.2.6 *Suppose C is a linear quantum code with parameters $[[n, k, d]]$. Then there exists an $[[n - m, k', d']]$ linear quantum code, where $k' \geq k - m$ and $d' \geq d$, if there exists a codeword of weight m in the dual of the binary code which is generated by the support coordinates of the code C .*

Proof: Let v be the mentioned codeword in the dual of the binary code generated by the supports of the code C . Assume that the set of nonzero coordinates of v is equal to S . Then by Lemma 2.2.5, the code C' obtained by deleting the coordinates of S is self-orthogonal and has more than 2^{n-k+m} vectors. Moreover, if there exists a codeword $u \in C^{\perp_s} \setminus C$ with $wt(u) = d'$, then we replace the removed coordinate with zero in u and clearly it is a codeword in C with weight $\leq d'$. Therefore, $d \leq d'$. \square

Now, we present another result which generalizes the direct sum construction of two quantum stabilizer codes.

Theorem 2.2.7 *Let C_1 and C_2 be two quantum stabilizer codes with the parameters $[[n_1, k_1, d_1]]$ and $[[n_2, k_2, d_2]]$, respectively. If $k_2 \leq n_1$, we can construct an $[[n_1 + n_2 - k_2, k_1, d]]$ quantum stabilizer code with $d \geq \min\{d_1, d_1 + d_2 - k_2\}$.*

Proof: Let $C_1, C_1^{\perp_s}$ be additive codes with parameters $(n_1, 2^{n_1-k_1}), (n_1, 2^{n_1+k_1})$ and $C_2, C_2^{\perp_s}$ be additive codes with the parameters $(n_2, 2^{n_2-k_2}), (n_2, 2^{n_2+k_2})$, respectively. Let N be the natural map from $C_2^{\perp_s}$ to $C_2^{\perp_s}/C_2$ and F be a bijection from C_2^{\perp}/C_2 to $\mathbb{F}_4^{k_2}$ that preserves the inner product. Let $\phi = F \circ N$ be the composition of F and N . Consider the code $C = \{uv | v \in C_2^{\perp}, u\phi(v) \in C_1\}$. Obviously, the length of C is $n_2 + n_1 - k_2$. $\dim(C) = n_2 + n_1 - k_2 - k_1$ because if $v \in C_2$, then $0v \in C$ so we have $n_2 - k_2$ linearly independent vectors. Also, since $\phi(C_2^{\perp}/C_2) = \mathbb{F}_4^{k_2}$ then we can find new $n_1 - k_1$ linear independent vectors. We easily see that $C^{\perp} = \{uv | v \in C_2^{\perp}, u\phi(v) \in C_1^{\perp}\}$. Now, if $uv \in C^{\perp}$ and $\phi(v) \neq 0$, $wt(v) \geq d_2$ and $wt(u) \geq d_1 - k_2$. So $wt(uv) \geq d_2 + d_1 - k_2$. If $\phi(v) = 0$, $wt(u) \geq d_1$ and consequently $wt(uv) \geq d_1$. This completes the proof. \square

For example, if C_1 and C_2 are $[[n_1, k_1, d_1]]$ and $[[1, 0, 1]]$ quantum stabilizer codes, respectively, then the code obtained by Theorem 2.2.7 is an $[[n_1 + 1, k_1, d_1]]$ which is the same as the code obtained by Theorem 2.2.4 part *i*.

Now, we present another construction which is based on combining binary linear codes.

Theorem 2.2.8 *Let C_1 be an $(n, 2^{k_1})$, C_2 be an $(n, 2^{k_2})$ binary linear codes such that $C_1 \subseteq C_2$, and $w \neq 0, 1$ be an element of \mathbb{F}_4 . Then the code $C = wC_1 + \bar{w}C_2^{\perp}$ is an $[[n, k_2 - k_1, d]]$ quantum stabilizer code, where $d = \min\{d(C_2 \setminus C_1), d(C_1^{\perp} \setminus C_2^{\perp})\}$.*

Proof: Since C_2 is a binary code, $\dim(C_2^{\perp}) = n - k_2$. Therefore, $\dim(C) = k_1 + n - k_2$. Let $wx + \bar{w}y$ and $wx' + \bar{w}y'$ be elements of C . Then

$$\begin{aligned} (wx + \bar{w}y) * (wx' + \bar{w}y') &= wx * wx' + wx * \bar{w}y' + \bar{w}y * wx' + \bar{w}y * \bar{w}y' \\ &= wx * \bar{w}y' + \bar{w}y * wx' = x * y' + x' * y. \end{aligned}$$

Since $C_1 \subseteq C_2$ we can conclude that $(wx + \bar{w}y) * (wx' + \bar{w}y') = 0$. Therefore, C is an $[[n, k_2 - k_1]]$ quantum code and $C^{\perp} = \bar{w}C_1^{\perp} + wC_2$. Now, if $u \in C^{\perp} \setminus C$, then $u = (u_1, u_2)$, where $u_1 \in wC_2 \setminus wC_1 \cup \{0\}$ and $u_2 \in \bar{w}C_1^{\perp} \setminus \bar{w}C_2^{\perp} \cup \{0\}$. Thus, $d = \min\{d(C_2 \setminus C_1), d(C_1^{\perp} \setminus C_2^{\perp})\}$. \square

In the next theorem, we explain an analog of the $(u|u+v)$ construction for quantum codes. This construction is also known as the Plotkin sum of two codes.

Theorem 2.2.9 *Suppose that C_1 is a pure $[[n, k_1, d_1]]$ stabilizer code, and C_2 is a pure $[[n, k_2, d_2]]$ stabilizer code such that $C_1 \subseteq C_2$. Then the code $C = \{(u|u + v) : u \in C_2^\perp, v \in C_1\}$ is an $[[2n, k_1 - k_2, d]]$ stabilizer code, where $d = \min\{2d_1, \delta\}$, $\delta = d(C_2)$.*

Proof: Let $C_1 \subseteq C_2$. Then, $\dim(C) = n + k_2 + n - k_1$. Also, if $(u|u + v)$ and $(x|x + y) \in C$, then

$$(u|u + v) * (x|x + y) = u * x + u * x + u * y + v * x + v * y = u * y + v * x + v * y = 0.$$

Thus, C is an $[[2n, k_1 - k_2]]$ stabilizer code and $C^\perp = \{(u|u + v) : u \in C_1^\perp, v \in C_2\}$. Assume that $(u|u + v) \in C^\perp$. If $u \neq 0$, $wt(u|u + v) \geq 2d_1$ and if $u = 0$, $wt(u|u + v) \geq d(C_2)$. \square

For instance, by combining the pure codes $[[14, 8, 3]]$ and $[[14, 0, 6]]$, we obtain an $[[28, 8, 6]]$ quantum stabilizer code.

2.3. Quantum Stabilizer Codes from Nearly Self-orthogonal Quaternary Linear Codes

In this Section, we introduce another method of constructing new quantum codes. The construction is based on construction X and its variants [13], and we use linear codes as our source code. So, we will apply the Hermitian inner product which is equivalent to the symplectic inner product in the case code is linear 2.1.2. We will denote the Hermitian inner product of $u, v \in \mathbb{F}_4^n$ by $\langle u, v \rangle$.

For $u \in \mathbb{F}_4^n$, note that the norm of u is $\|u\| = \langle u, u \rangle = \sum_{i=0}^n u_i^3$. If $u_i \neq 0$ then $u_i^3 = 1$, so $wt(u) = \|u\|$ and by the proof of Theorem 2.1.3 we see that

$$\|u + v\| = \|u\| + \|v\| + Tr(\langle u, v \rangle).$$

A set $S \subseteq \mathbb{F}_4^n$ is called an *orthonormal* set if $\langle u, v \rangle = 0$ for $u \neq v \in S$ and $\|u\| = 1$ for all $u \in S$.

Proposition 2.3.10 *Let D be a linear subspace of \mathbb{F}_4^n and the set M be a basis for $D \cap D^\perp$. Then there exists a set B which is orthonormal and $M \cup B$ is a basis for D .*

Proof: First, suppose that R is a subspace of \mathbb{F}_4^n and there exist $u, v \in R$ such that $\langle u, v \rangle \neq 0$. Then, for $\gamma \in \mathbb{F}_4^*$,

$$\|\gamma u + v\| = \|\gamma u\| + \|v\| + Tr(\gamma \langle u, v \rangle).$$

So we can find γ such that $\|\gamma u + v\| = 1$. Now, let W be a subspace of \mathbb{F}_4^n such that

$$D = (D \cap D^\perp) \oplus W. \tag{2.1}$$

We will assume that W is not self-orthogonal, since otherwise $D = (D \cap D^\perp)$ and in this case we can turn M into an orthonormal basis as described above. Let $r := \dim(W)$. For each $0 \leq i \leq r$ we will construct a set S_i which is an orthonormal basis of T_i , where T_i is a subspace of W with

$$W = T_i \oplus (T_i^\perp \cap W). \tag{2.2}$$

The steps are iterative. Take $S_0 = \emptyset$ and suppose that for some $0 \leq i < r$ there is an orthonormal basis S_i of T_i , where $\dim(T_i) = i$ and it satisfies (2.2). Let u be a nonzero vector in $T_i^\perp \cap W$. Then there exists a vector $v \in T_i^\perp \cap W$ such that $\langle u, v \rangle \neq 0$.

Note that there exists such v , because W is not self-orthogonal. According to the first paragraph of the proof, there exists $\gamma \in \mathbb{F}_4^*$ such that $\|\gamma u + v\| = 1$. Let $z = \gamma u + v$. Then the set $S_{i+1} = S_i \cup \{z\}$ is an orthonormal set and $z \notin T_i$, hence $\dim(T_{i+1}) = i + 1$. Now, we show that

$$W = T_{i+1} \oplus (T_{i+1}^\perp \cap W). \quad (2.3)$$

First we prove that $T_{i+1} \cap (T_{i+1}^\perp \cap W) = \{0\}$. Suppose $x \in T_{i+1} \cap (T_{i+1}^\perp \cap W)$. Since $x \in T_{i+1}$, we have $x = y + \alpha z$ where $y \in T_i$ and $\alpha \in \mathbb{F}_4$. Moreover, since $x = y + \alpha z \in T_{i+1}^\perp$ for all $w \in T_i$ and $\beta \in \mathbb{F}_4$, we have

$$0 = \langle y + \alpha z, w + \beta z \rangle = \langle y, w \rangle + \bar{\beta} \langle y, z \rangle + \alpha \langle z, w \rangle + \alpha \bar{\beta} \|z\|^2 = \langle y, w \rangle + \alpha \bar{\beta}.$$

Therefore, $\alpha = 0$, because otherwise we can find a $\beta \in \mathbb{F}_4$ such that $\langle y, w \rangle + \alpha \bar{\beta} \neq 0$, which is a contradiction. So, $\langle y, w \rangle = 0$ and since $w \in T_i$, we conclude that $y \in T_i^\perp$. Moreover, $x = y$ also belongs to T_i . Hence, $x \in T_i \cap T_i^\perp = \{0\}$ and it shows $T_{i+1} \cap (T_{i+1}^\perp \cap W) = \{0\}$. Next we prove that $W = T_{i+1} + (T_{i+1}^\perp \cap W)$. Let $w \in W$. Since $W = T_i \oplus (T_i^\perp \cap W)$ there are $x \in T_i$ and $y \in T_i^\perp \cap W$ such that $w = x + y$. Now, let $x' = x + \langle y, z \rangle z$ and $y' = y - \langle y, z \rangle z$. Obviously $x' \in T_{i+1}$ and for any $s = u + \alpha z \in T_{i+1}$ with $u \in T_i, \alpha \in \mathbb{F}_4$. We have

$$\begin{aligned} \langle y', s \rangle &= \langle y - \langle y, z \rangle z, u + \alpha z \rangle \\ &= \langle y, u \rangle + \bar{\alpha} \langle y, z \rangle - \langle y, z \rangle \langle z, u \rangle - \bar{\alpha} \langle y, z \rangle \|z\|^2 \\ &= \bar{\alpha} (\langle y, z \rangle - \langle y, z \rangle) = 0. \end{aligned}$$

Therefore, $y' \in T_i^\perp \cap W$ and $x' + y' = x + y = w$. So (2.2) implies (2.3) and by repeating this approach we can achieve the desired goal. \square

Now we state the main theorem of this Section.

Theorem 2.3.11 *Suppose that C is an $[n, k]_4$ linear code and $e := n - k - \dim(C \cap C^{\perp_s})$. Then there exist a quantum code with parameters $[[n + e, 2k - n + e, d]]$ with $d \geq \min\{d(C), d(C + C^{\perp_s}) + 1\}$.*

Proof: First, note that $\dim(C^{\perp_s}) = n - k$ and we have $\dim(C + C^{\perp_s}) = \dim(C) + \dim(C^{\perp_s}) - \dim(C \cap C^{\perp_s})$. So $e = \dim(C + C^{\perp_s}) - \dim(C)$. Let $s := \dim(C \cap C^{\perp_s})$. Consider the block matrix G

$$G = \begin{bmatrix} M_{s \times n} & 0_{s \times e} \\ A_{(n-e-2s) \times n} & 0_{(n-e-2s) \times e} \\ B_{e \times n} & I_{e \times e} \end{bmatrix},$$

where the indices show the size of blocks, and $0, I$ are the zero and identity matrices, respectively. We denote the rows of a matrix P by $r(P)$. The matrix G is constructed such that $r(M)$ is a basis for $C \cap C^{\perp_s}$, $r(M) \cup r(A)$ is a basis for C and $r(M) \cup r(B)$ is a basis for C^{\perp_s} . Note that according to Proposition 2.3.10 we can choose B as an orthonormal set and $r(M) \cup r(A) \cup r(B)$ is a basis for $(C + C^{\perp_s})$.

Let E be the linear code of length $n + e$ generated by the matrix G . Now consider the matrix T

$$T = \begin{bmatrix} M_{s \times n} & 0_{s \times e} \\ B_{e \times n} & I_{e \times e} \end{bmatrix}.$$

By construction, each row of T is orthogonal to every row of G . So $r(T) \subseteq E^{\perp s}$. Moreover, since the vectors in $r(T)$ are self-orthogonal and $\dim(E^{\perp s}) = n+e-(n-s) = e+s$, we conclude that $r(T)$ is a basis for $E^{\perp s}$ and consequently $E^{\perp s} \subseteq E$. So $E^{\perp s}$ generates a self-orthogonal code. Since $E^{\perp s}$ has $2^{2(s+e)}$ elements, by Definition 2.1.1 it yields a quantum stabilizer code of dimension $n+e-2(s+e) = 2k-n+e$.

Now let x be a nonzero vector in E . So x is linear combination of rows of G and we can write $x = (x_1|x_2)$ where $x_1 \in \mathbb{F}_4^n$ and $x_2 \in \mathbb{F}_4^e$. If there is no vectors from the last e rows of G , then $x_1 \in C$ and $x_2 = 0$ and therefore $wt(x) \geq d(C)$. Otherwise, some of the vectors in the last e rows of G are included in the linear combination and $wt(x_1) \geq d(C+C^{\perp s})$ and $wt(x_2) \geq 1$. Hence, $wt(x) \geq d(C+C^{\perp s})+1$. This completes the proof. \square

In Theorem 2.3.11, the construction is based on a linear source code. So it is possible to choose our source code from any class linear codes. For example, we can replace linear codes with cyclic codes or 2-D cyclic codes. We will explain the cyclic construction in this Section and 2-D cyclic code construction in the next Chapter. First, we need the following proposition.

Proposition 2.3.12 *Suppose C is a quaternary cyclic code with length n , where n is an odd number. Let Z be the defining set of the code C . Then $\dim(C^{\perp s}) - \dim(C \cap C^{\perp s}) = |Z \cap -2Z|$, where $-2Z := \{-2z \pmod{n} | z \in Z\}$.*

Proof: Let β be a primitive n th root of unity, $\bar{Z} := Z_n - Z$ and

$$g(x) = \prod_{k \in Z} (x - \beta^k)$$

be the generator polynomial of code C . Then its Hermitian (symplectic) dual generator will be

$$h(x) = \prod_{k \in -2\bar{Z}} (x - \beta^k),$$

and the generator polynomial of $C \cap C^{\perp s}$ is

$$k(x) = \prod_{k \in Z \cup -2\bar{Z}} (x - \beta^k).$$

Then,

$$\begin{aligned} \dim(C^{\perp s}) - \dim(C \cap C^{\perp s}) &= (n - |-2\bar{Z}|) - (n - |Z \cup -2\bar{Z}|) \\ &= |Z \cup -2\bar{Z}| - |-2\bar{Z}| \\ &= |Z - 2\bar{Z}| = |Z \cap -2Z|. \end{aligned}$$

\square

Note that if n is an odd number which is divisible by 3, then $\{0\}$, $\{\frac{n}{3}\}$, and $\{\frac{2n}{3}\}$ have singleton cyclotomic cosets modulo n and are closed under multiplication by -2 modulo n . So if C is a cyclic code with defining set $Z \subseteq \{0, \frac{n}{3}, \frac{2n}{3}\}$, then by Proposition 2.3.12, $\dim(C^{\perp s}) - \dim(C \cap C^{\perp s}) = |Z|$.

Theorem 2.3.13 *Suppose that n is an odd integer which is divisible by 3 and let C be an $[n, k]_4$ cyclic code with the defining set Z where $Z \cap -2Z \subseteq \{0, \frac{n}{3}, \frac{2n}{3}\}$. Then there exists a quantum code with parameters $[[n+e, 2k-n+e, d]]$ with*

$$d \geq \min\{d(C_U) + |U|\}$$

where $U \subseteq Z \cap -2Z$, C_U is a cyclic code with defining set $Z \setminus U$, and $e = |Z \cap -2Z|$.

Proof: Let $r := \frac{n}{3}$ and β be a primitive n th root of unity in \mathbb{F}_{4^m} , where m is order of 4 modulo n , then $\omega = \beta^r$ is a primitive cube root of unity in \mathbb{F}_4 . We define

$$b_t(x) := \frac{x^n - 1}{x - \beta^{tr}} = \frac{x^n - 1}{x - \omega^t} = \sum_{i=0}^{r-1} x^{3i+2} + \omega^t x^{3i+1} + \omega^{2t} x^{3i}$$

where $t \in \{0, 1, 2\}$. So, we can consider each b_t as a codeword in the form $(a_0, a_1, \dots, a_{n-1})$ in \mathbb{F}_4^n . Since n is odd, $\langle b_t, b_t \rangle = n \equiv 1 \pmod{2}$. By construction, if $t \neq t'$ then $\langle b_t, b_{t'} \rangle = 0$. So the set $\{b_1, b_2, b_3\}$ is an orthonormal set. Now, we can use the construction in Theorem 2.3.11. The difference here is that in the last e rows we use b_i 's. Therefore, using Proposition 2.3.12 and Theorem 2.3.11, we have the matrix G

$$G = \begin{bmatrix} M_{s \times n} & 0_{s \times e} \\ A_{(n-e-2s) \times n} & 0_{(n-e-2s) \times e} \\ B_{e \times n} & I_{e \times e} \end{bmatrix},$$

where $r(M)$ is a basis for $C \cap C^{\perp_s}$, $r(M) \cup r(A)$ is a basis for C , and $r(M) \cup r(B)$ is a basis for C^{\perp_s} . Let E be the code generated by the matrix G . Clearly, the code generated by the matrix

$$T = \begin{bmatrix} M_{s \times n} & 0_{s \times e} \\ B_{e \times n} & I_{e \times e} \end{bmatrix}$$

is E^{\perp_s} and therefore $E^{\perp_s} \subseteq E$. Let x be a nonzero codeword in E . We can write $x = (x_1 | x_2)$ where $x_1 \in \mathbb{F}_4^n$ and $x_2 \in \mathbb{F}_4^e$. If no row from $r(B)$ occurs in the linear combination of rows defining x , then $wt(x) \geq d(C)$. If there are some rows of $r(B)$ in the linear combination, then $wt(x) \geq d(\text{Span}(C, U) + |U|)$, where $U = \{b_i\}$ for all b_i occurring in the linear combination, and $\text{Span}(C, \{b_i\})$ is exactly the cyclic code C_U . Therefore, $wt(x) \geq \min\{d(C_U) + |U|\}$, where $U \subseteq Z \cap -2Z$. □

2.4. Non-binary Quantum Stabilizer Codes

Denote by \mathbb{F}_{p^m} the finite field of p^m elements, where p is a prime number and m is a positive integer. Let $Tr : \mathbb{F}_{p^m} \rightarrow \mathbb{F}_p$ be the standard trace function which is an \mathbb{F}_p linear map and defined by $Tr(a) = \sum_{i=0}^{m-1} a^{p^i}$. Let $a, b \in \mathbb{F}_{p^m}^n$, and consider the Euclidean inner product of a and b

$$\langle a, b \rangle = \sum_{i=1}^n a_i b_i.$$

Definition 2.4.2 Let $(a, b), (a', b') \in \mathbb{F}_{p^m}^{2n}$. We define the *symplectic inner product* of (a, b) and (a', b') as

$$(a, b) * (a', b') = \text{Tr}(\langle a, b' \rangle - \langle a', b \rangle).$$

Also, the *symplectic weight* of (a, b) will be denoted by

$$\text{swt}((a, b)) = |\{1 \leq k \leq n | (a_k, b_k) \neq (0, 0)\}|.$$

For an \mathbb{F}_p additive code $C \subseteq \mathbb{F}_{p^m}^{2n}$ we denote the symplectic dual of C with

$$C^{\perp_s} = \{(c, d) \in \mathbb{F}_{p^m}^{2n} | (a, b) * (c, d) = 0 \text{ for all } (a, b) \in C\}.$$

Remark 2.4.1 If there exists an additive code $C \subseteq \mathbb{F}_q^{2n}$ such that $|C| = q^{n-k}$, $C \subseteq C^{\perp_s}$, and $d = \text{swt}(C^{\perp_s} \setminus C)$, then an $[[n, k, d]]_q$ quantum stabilizer code exists.

Similar to the binary case if $k = 0$, which implies $C = C^{\perp_s}$, then we define $d = \min\{\text{swt}(u) | 0 \neq u \in C\}$. Let u, v be elements of $\mathbb{F}_{p^2}^n$, then the Hermitian inner product of u and v is defined as follow

$$\langle u, v \rangle = \sum_{i=1}^n a_i \bar{b}_i,$$

where $\bar{x} = x^p$. The following analogue of Theorem 2.1.2 hold for characteristic p too.

Theorem 2.4.14 *An \mathbb{F}_{p^2} linear code C is self-orthogonal with respect to the symplectic inner product if and only if it is self-orthogonal with respect to the Hermitian inner product.*

Theorem 2.4.15 *If there exists an \mathbb{F}_{p^2} -linear $[n, k, d]_{p^2}$ code C such that $C^{\perp_h} \subseteq C$, then there exists an $[[n, 2k - n, d]]$ quantum stabilizer code where $d = \text{swt}(C \setminus C^{\perp_h})$*

For proofs of Theorem 2.4.14 and 2.4.15, we refer to [1].

Now, we extend the construction X to obtain quantum stabilizer codes over finite fields of order p^2 . Almost all of the results will be generalizations of the results in Section 2.3, so we skip some of the proofs. For more information we refer to [5]

Lemma 2.4.16 *Let D be a linear subspace of $\mathbb{F}_{p^2}^n$ and M be a basis for $D \cap D^{\perp_h}$. Then there exists an orthonormal set B such that $M \cup B$ is a basis for D .*

The proof is a generalization of the proof of Theorem 2.3.10 and therefore we omit it. In the rest of this chapter we assume that p is a prime number such that $p - 1 = 4k$ for some integer k .

Theorem 2.4.17 *Suppose that C is an \mathbb{F}_{p^2} linear code with parameters $[n, k]_{p^2}$. Let $e = n - k - \dim(C \cap C^{\perp_h})$. Then there exists an $[[n + e, 2k - n + e, d]]_{p^2}$ quantum code where $d \geq \min\{d(C), d(C + C^{\perp_h}) + 1\}$.*

Proof: First, we prove that there exist a nonzero element γ in \mathbb{F}_{p^2} such that $\gamma^2 + 1 = 0$. We know that $\mathbb{F}_{p^2}^*$ is a cyclic group. Let β be a generator for this group. Then, $\beta^{p^2-1} = 1$. Moreover, $p^2 - 1 = 4k$, where k is an integer. Therefore, $\beta^{\frac{p^2-1}{2}} = -1$. Now, consider the matrix

$$G = \begin{bmatrix} M_{s \times n} & 0_{s \times e} \\ A_{(n-e-2s) \times n} & 0_{(n-e-2s) \times e} \\ B_{e \times n} & \beta^{\frac{p-1}{4}} I_{e \times e} \end{bmatrix},$$

where $s = \dim(C \cap C^{\perp h})$. The size of each block is determined by the index, and 0 and I denote the zero matrix and identity matrix, respectively. Here, for matrix P , $r(P)$ denotes the rows of matrix P . In G , $r(M)$ is a basis for $C \cap C^{\perp h}$, $r(M) \cup r(A)$ is a basis for C , $r(M) \cup r(B)$ is a basis for $C^{\perp h}$, and finally $r(B)$ is the orthonormal set which is obtained by Lemma 2.4.16.

Let E be the linear code with the generator matrix G . Now, consider the matrix S which is defined as follows:

$$S = \begin{bmatrix} M_{s \times n} & 0_{s \times e} \\ B_{e \times n} & \beta^{\frac{p-1}{4}} I_{e \times e} \end{bmatrix}$$

By construction, each of the first s vectors in $r(S)$ is orthogonal to each row of G . Also, if $v = (v_1, v_2)$ is one of the vectors from the last e rows of S , then v is orthogonal to first $n - e - s$ rows of G . Now we consider the inner product of $v = (v_1, v_2)$ and $u = (u_1, u_2)$, where u, v are in the last e rows of S . If $u \neq v$, then by construction $\langle u, v \rangle = 0$. Otherwise, if $u = v$,

$$\begin{aligned} \langle u, v \rangle &= \langle v, v \rangle = \|v\|^2 = \sum_{i=1}^{n+e} v_i^{p+1} = \sum_{i=1}^n v_i^{p+1} + \sum_{i=n+1}^{n+e} v_i^{p+1} \\ &= 1 + \beta^{\frac{p-1}{4}p+1} = 1 + \beta^{\frac{(p-1)(p+1)}{4}} = 1 + \beta^{\frac{p^2-1}{4}} = 1 - 1 = 0. \end{aligned}$$

So, each vector from S belongs to $E^{\perp h}$. Rest of the proof is similar to the proof of Theorem 2.3.11. \square

Next, we will explain another method of constructing quantum codes using cyclic codes. First, we need the following Lemma.

Lemma 2.4.18 *Let C be a cyclic code over \mathbb{F}_{p^2} with the defining set $Z \subseteq \mathbb{Z}_n$. Then, $\dim(C^{\perp h}) - \dim(C \cap C^{\perp h}) = |Z \cap -pZ|$.*

Proof: Similar to Proposition 2.3.12. \square

Theorem 2.4.19 *Assume that n is divisible by $p^2 - 1$ and C be an $[n, k]_{p^2}$ cyclic code with the defining set Z where $Z \cap -pZ \subseteq T = \{\frac{nk}{p^2-1} | 1 \leq k \leq p^2 - 1\}$. If $e = |Z \cap -pZ|$, then there exists an $[[n+e, 2k-n+e, d]]_{p^2}$ quantum code with $d \geq \min\{d(C), d(C_u) + 1, d(C + C^{\perp h}) + 2\}$, where $u \in Z \cap -pZ$ and C_u is a cyclic code with defining set $Z \setminus \{u\}$.*

Proof: First we show that each element in T has a singleton cyclotomic coset. Assume that $1 \leq k \leq p^2 - 1$. Then

$$\frac{nk}{p^2-1}p^2 = \frac{p^2nk}{p^2-1} = \frac{p^2nk - nk + nk}{p^2-1} = nk + \frac{nk}{p^2-1} \equiv \frac{nk}{p^2-1} \pmod{n}.$$

Next, let $q = p^2 - 1$, $n = (p^2 - 1)l = ql$ and ω be a $(p^2 - 1)$ th root of unity. Consider the polynomials

$$b_t(x) = \frac{x^n - 1}{x - \omega^t} = \sum_{i=1}^{l-1} (x^{qi+q-1} + \omega^t x^{qi+q-2} + \dots + \omega^{(q-1)t} x^{qi}),$$

for $0 \leq t \leq l$. We show the corresponding codewords with b_t . Now, we show that the set $\{b_j | 0 \leq j \leq l\}$ is an orthonormal set. This is because

$$\langle b_u, b_v \rangle = q \sum_{i=0}^{l-1} \omega^{i(u+vp)} = q \sum_{i=0}^{l-1} \omega^{i(u-vp)} = \begin{cases} ql & u = v \\ 0 & u \neq v \end{cases}.$$

Rest of the proof is similar to the proof of Theorem 2.3.13. □

CHAPTER 3

New Constructions of Quantum Stabilizer Codes

In Chapter 2, we presented some methods of constructing new quantum codes using classical codes or extending primary quantum codes. In this Chapter, first we will introduce 2-D cyclic quantum stabilizer codes and construct new quantum codes based on classical 2-D cyclic codes. Next, we introduce a method of constructing quantum codes over \mathbb{F}_{p^2} by using arbitrary classical additive codes over \mathbb{F}_{p^2} , where p is an odd prime number.

3.1. 2-D Cyclic Quantum Stabilizer Codes

By Theorem 2.4.15, for an $[n, k]_{p^2}$ linear code C such that $C^{\perp_h} \subseteq C$ we can find a quantum code with parameters $[[n, 2k - n, d]]$, where $d = \min\{wt(u) | u \in C \setminus C^{\perp_h}\}$.

Definition 3.1.1 Suppose there exists a 2-D cyclic code C with the parameters $[n_1 \times n_2, k, d]_{p^2}$ such that $C^{\perp_h} \subseteq C$. Then we call C a 2-D cyclic quantum code.

Now, let $C = I(U) / \langle x^{n_1} - 1, y^{n_2} - 1 \rangle$ be a 2-D cyclic code with the zero set U . Then by Theorem 1.5.15, we can find $G = \{p_0(x, y), p_1(x, y), \dots, p_{n_2-1}(x, y)\}$ which is the set of the generator polynomials for C . Then C is a 2-D cyclic quantum code if and only if

$$p_i(x, y) \cdot \overline{p_j(x, y)} \equiv 0 \pmod{\langle x^{n_1} - 1, y^{n_2} - 1 \rangle} \text{ for all } p_i(x, y), p_j(x, y) \in G.$$

So we have the following Proposition.

Proposition 3.1.1 Suppose that $C = I(U) / \langle x^{n_1} - 1, y^{n_2} - 1 \rangle$ is a 2-D cyclic code which is generated by the polynomials $p_0(x, y), p_1(x, y), \dots, p_{n_2-1}(x, y)$, and $p_0^0(x) \cdot \overline{p_0^0(x)} \equiv 0 \pmod{\langle x^{n_1} - 1 \rangle}$. Then C is a 2-D cyclic quantum code.

Proof: By Proposition 1.5.14, $p_0^0(x) \mid p_i^j(x)$ for all $0 \leq i, j \leq n_2 - 1$. Then $p_i^j(x) \cdot \overline{p_i^j(x)} \equiv 0 \pmod{\langle x^{n_1} - 1 \rangle}$ for all $0 \leq i, j \leq n_2 - 1$. It means that for all $0 \leq i \leq n_2 - 1$ we have

$$p_i(x, y) \cdot \overline{p_i(x, y)} \equiv 0 \pmod{\langle x^{n_1} - 1 \rangle}.$$

Therefore, $C \subseteq C^{\perp_h}$, which means that C is a 2-D cyclic quantum code. \square

Example 3.1.2 Consider the quaternary 2-D cyclic code C with the parameters $[15, 8]_2$ and the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & w^2 & w^2 & 0 & 0 & 0 & 0 & 0 & w & 0 & w & 1 & 1 \\ w & 0 & w & 1 & 1 & 0 & 0 & 0 & 0 & 0 & w^2 & 0 & w^2 & w & w \\ 0 & 1 & w^2 & w^2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & w & 1 & 1 & w \\ 0 & w & 1 & 1 & w & 0 & 0 & 0 & 0 & 0 & 0 & w^2 & w & w & w^2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & w^2 & w^2 & w^2 & 0 & w^2 & w & w \\ 0 & 0 & 0 & 0 & 0 & w & 0 & w & 1 & 1 & 1 & 0 & 1 & w^2 & w^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & w^2 & w^2 & 1 & 0 & w^2 & w & w & w^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & w & 1 & 1 & w & 0 & 1 & w^2 & w^2 & 1 \end{bmatrix},$$

where $w \neq 0, 1$ is an element of \mathbb{F}_4 . The code is self-orthogonal with respect to the Hermitian inner product and consequently we can find a $[[15, 7]]$ quantum code. Using Magma, we can see that $\min\{wt(u)|u \in C^{\perp_h} \setminus C\} = 3$. Therefore, C is an $[[15, 7, 3]]$ quantum code. According to the best known quantum code's table [8], this code reaches the optimum minimum distance.

3.2. New Quantum Stabilizer Codes Construction Using 2-D Cyclic Codes

Now, we introduce a new method of constructing quantum stabilizer codes which is based on construction X. Our main aim is to replace the code C in Theorem 2.4.17 with a 2-D cyclic code. In this Section, we assume that p is a prime number such that $p = 4k + 1$ for some integer k .

Lemma 3.2.3 *Let n_1, n_2 be two positive integers such that $p^2 - 1$ divides both n_1 and n_2 . Then the \mathbb{F}_{p^2} conjugacy class of (α_1^i, α_2^j) is a singleton, if $i \in T_1 = \{\frac{n_1 k}{p^2 - 1} | k \in \{1, 2, \dots, p^2 - 1\}\}$ and $j \in T_2 = \{\frac{n_2 k'}{p^2 - 1} | k' \in \{1, 2, \dots, p^2 - 1\}\}$.*

Proof: It is enough to show that $(\alpha_1^{ip^2}, \alpha_2^{jp^2}) = (\alpha_1^i, \alpha_2^j)$ for all $i \in T_1$ and $j \in T_2$. Suppose $i = \frac{n_1 k}{p^2 - 1}, j = \frac{n_2 k'}{p^2 - 1}$ we have:

$$\begin{aligned} (\alpha_1^{ip^2}, \alpha_2^{jp^2}) &= (\alpha_1^{\frac{n_1 k}{p^2 - 1} p^2}, \alpha_2^{\frac{n_2 k'}{p^2 - 1} p^2}) = (\alpha_1^{\frac{p^2 \cdot n_1 \cdot k}{p^2 - 1}}, \alpha_2^{\frac{p^2 \cdot n_2 \cdot k'}{p^2 - 1}}) \\ &= (\alpha_1^{\frac{p^2 \cdot n_1 \cdot k + n_1 \cdot k - n_1 \cdot k}{p^2 - 1}}, \alpha_2^{\frac{p^2 \cdot n_2 \cdot k' + n_2 \cdot k' - n_2 \cdot k'}{p^2 - 1}}) = (\alpha_1^{n_1 k} \alpha_1^{\frac{n_1 k}{p^2 - 1} p^2}, \alpha_2^{n_2 k'} \alpha_2^{\frac{n_2 k'}{p^2 - 1} p^2}) \\ &= (\alpha_1^i, \alpha_2^j). \end{aligned}$$

□

Theorem 3.2.4 *Suppose that n_1 and n_2 are divisible by $p^2 - 1$ and let C be an $[[n_1 \times n_2, k]]_{p^2}$ 2-D cyclic code with the zero set U such that $U \cap U^{-p} \subseteq \{(\alpha_1^i, \alpha_2^j) | (i, j) \in T_1 \times T_2\}$, where T_1, T_2 are defined as in Lemma 3.2.3. If $e = |U \cap U^{-p}|$, then there exists an $[[n_1 \times n_2 + e, 2k - n_1 \times n_2 + e, d]]_p$ quantum code with $d \geq \min\{d(C), d(C_V) + r\}$, where the minimum is taken over all the 2-D cyclic codes C_V with the zero set $V \subseteq U \cap U^{-p}$ and $r = |V|$.*

Proof: We prove the theorem in two steps. First step: Let $q = p^2 - 1$, $n_1 = qh$, $n_2 = qh'$, and ω be a $(p^2 - 1)$ th root of unity. Then, we claim that the set of codewords corresponding to the elements of the set $T = \{b_{i,j} = \frac{x^{n_1-1}}{x-\omega^i} \times \frac{y^{n_2-1}}{y-\omega^j} | 0 \leq i \leq h, 0 \leq j \leq h'\}$ is an orthonormal set.

Let $b_{i,j} \in T$ be of the form

$$b_{i,j} = \left(\sum_{s=0}^{h-1} (x^{qs+q-1} + \omega^i x^{qs+q-2} + \dots + \omega^{(q-1)i} x^{qs}) \right) \times \left(\sum_{k=0}^{h'-1} (y^{qk+q-1} + \omega^j y^{qk+q-2} + \dots + \omega^{(q-1)j} x^{qk}) \right).$$

We can express all the coefficients of the product

$$(x^{qs+q-1} + \omega^i x^{qs+q-2} + \dots + \omega^{(q-1)i} x^{qs})(y^{qk+q-1} + \omega^j y^{qk+q-2} + \dots + \omega^{(q-1)j} x^{qk})$$

as a $q \times q$ matrix

$$W_{i,j} = \begin{bmatrix} \omega^{(q-1)j} \omega^{(q-1)i} & \omega^{(q-1)j} \omega^{(q-2)i} & \omega^{(q-1)j} \omega^{(q-3)i} & \dots & \omega^{(q-1)j} \\ \omega^{(q-2)j} \omega^{(q-1)i} & \omega^{(q-2)j} \omega^{(q-2)i} & \omega^{(q-2)j} \omega^{(q-3)i} & \dots & \omega^{(q-2)j} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \omega^{(q-1)i} & \omega^{(q-2)i} & \omega^{(q-3)i} & \dots & 1 \end{bmatrix}.$$

So we can represent each $b_{i,j}$ as a matrix with hh' blocks, where all of the blocks are $W_{i,j}$. We will show that

$$\langle W_{i,j}, W_{i',j'} \rangle = \begin{cases} = 0, & \text{if } W_{i,j} \neq W_{i',j'} \\ \neq 0, & \text{if } W_{i,j} = W_{i',j'} \end{cases},$$

and consequently

$$\langle b_{i,j}, b_{i',j'} \rangle = h \cdot h' \langle W_{i,j}, W_{i',j'} \rangle = \begin{cases} = 0, & \text{if } b_{i,j} \neq b_{i',j'} \\ \neq 0, & \text{if } b_{i,j} = b_{i',j'} \end{cases},$$

which completes the proof.

Let $\omega^{(q-t)j}(\omega^{(q-1)i}, \omega^{(q-2)i}, \dots, \omega^i)$ and $\omega^{(q-t)j'}(\omega^{(q-1)i'}, \omega^{(q-2)i'}, \dots, \omega^{i'})$ be the t -th rows of $W_{i,j}$ and $W_{i',j'}$. Then

$$\begin{aligned} & \omega^{(q-t)j}(\omega^{(q-1)i}, \omega^{(q-2)i}, \dots, \omega^i) \cdot \overline{\omega^{(q-t)j'}(\omega^{(q-1)i'}, \omega^{(q-2)i'}, \dots, \omega^{i'})} \\ &= (\omega^{(q-t)j})(\omega^{(q-1)i}, \omega^{(q-2)i}, \dots, \omega^i) \cdot (\omega^{(q-t)j'p})(\omega^{(q-1)i'p}, \omega^{(q-2)i'p}, \dots, \omega^{i'p}). \end{aligned}$$

Now since the conjugacy class of $b_{i,j} = (\omega^{i'}, \omega^{j'})$ is a singleton class and $U \cap U^{-p} \subseteq \{(\alpha_1^i, \alpha_2^j) | (i, j) \in T_1 \times T_2\}$, we can replace $\omega^{i'p}$ and $\omega^{j'p}$ with $\omega^{-i'}$ and $\omega^{-j'}$, respectively. Therefore, we have

$$\begin{aligned} & (\omega^{(q-t)j})(\omega^{(q-1)i}, \omega^{(q-2)i}, \dots, \omega^i) \cdot (\omega^{(q-t)j'p})(\omega^{(q-1)i'p}, \omega^{(q-2)i'p}, \dots, \omega^{i'p}) \\ &= (\omega^{(q-t)j})(\omega^{(q-1)i}, \omega^{(q-2)i}, \dots, \omega^i) \cdot (\omega^{(q-t)-j'}) (\omega^{(q-1)-i'}, \omega^{(q-2)-i'}, \dots, \omega^{-i'}) \\ &= (\omega^{(q-t)(j-j')}) \sum_{s=1}^q \omega^{(q-s)(i-i')} = \begin{cases} 0 & i \neq i' \\ q(\omega^{(q-t)(j-j')}) & i = i' \end{cases}. \end{aligned}$$

So if $i \neq i'$, $\langle W_{i,j}, W_{i',j'} \rangle = 0$. Finally, if $i = i'$ we have

$$\langle W_{i,j}, W_{i',j'} \rangle = \sum_{k=1}^q \omega^{(q-k)(j-j')} = \begin{cases} 0 & j \neq j' \\ q^2 & j = j' \end{cases}.$$

Again if $j \neq j'$, $\langle W_{i,j}, W_{i',j'} \rangle = 0$. Otherwise, $\langle W_{i,j}, W_{i',j'} \rangle = q^2$ and consequently

$$\langle b_{i,j}, b_{i',j'} \rangle = h.h' \langle W_{i,j}, W_{i',j'} \rangle = \begin{cases} 0 & i \neq i' \& j \neq j' \\ h.h'q^2 = n_1.n_2 & i = i' \& j = j' \end{cases}.$$

In the case $i = i'$ and $j = j'$, $n_1 n_2$ is a non zero element and if we multiply each $b_{i,j}$ by a proper constant we can change the norm to 1.

Second step: Let $s = \dim(C \cap C^{\perp h})$, β be a $(p^2 - 1) = (4k)$ th root of unity, and G be the matrix

$$G = \begin{bmatrix} M_{s \times (n_1 \times n_2)} & 0_{s \times e} \\ A_{((n_1 \times n_2) - e - 2s) \times (n_1 \times n_2)} & 0_{((n_1 \times n_2) - e - 2s) \times e} \\ B_{e \times (n_1 \times n_2)} & \beta^{\frac{p-1}{4}} I_{e \times e} \end{bmatrix},$$

where the rows of M are basis for $C \cap C^{\perp h}$, rows of A and M are basis for C , and the set of rows of B is a subset of codewords corresponding to T . Moreover, the union of rows of B and M is a basis for $C^{\perp h}$. Let E be the linear code generated by the matrix G . By the first step of the proof, one can easily see that all the rows of matrix

$$S = \begin{bmatrix} M_{s \times (n_1 \times n_2)} & 0_{s \times e} \\ B_{e \times (n_1 \times n_2)} & \beta^{\frac{p-1}{4}} I_{e \times e} \end{bmatrix}$$

are orthogonal to each row of G . For example, if b_i and b_j are rows in matrix B , then the Hermitian inner product is

$$\langle b_i, b_j \rangle = \sum b_{i,k} \cdot \overline{b_{j,k}} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}.$$

Now since $\beta^{\frac{p-1}{4}} \cdot \overline{\beta^{\frac{p-1}{4}}} = \beta^{\frac{p-1}{4}} \cdot \beta^{\frac{p(p-1)}{4}} = \beta^{\frac{p^2-1}{4}} = -1$, we can guarantee the orthogonality of the last e rows of S . Therefore, we are left to show the claim on the minimum distance.

Suppose that x is a codeword generated by the matrix G . We have 3 cases:

1. If no row from B occurs in the linear combination of x , then $wt(x) \geq d(C)$.
2. If exactly one row of B , for example $b_{i,j}$, is in the linear combination with a non-zero coefficient, then $wt(x) \geq d(\text{Span}(C, b_{i,j}))$ and $\text{Span}(C, b_{i,j})$ is exactly the 2-D cyclic code with the zero set $U \setminus \{(\alpha_1^{\frac{in_1}{p^2-1}}, \alpha_2^{\frac{jn_2}{p^2-1}})\}$.
3. Finally, if more than one row of B occur in the linear combination, we can extend case 2 in order to find the appropriate result. \square

3.3. General Quantum Stabilizer Codes Construction Using Classical Additive Codes

In this Section, we introduce a new method of constructing additive quantum codes, which is a generalization of Theorems 2.3.11 and 2.4.17.

Lemma 3.3.5 *Let C be an $[n, l]$ additive code over \mathbb{F}_4 such that $\dim(C) - \dim(C \cap C^{\perp_s}) = 2k + i$, where $i \in \mathbb{Z}_2$. Then, we can extend C to a new code Q , where Q is an $[n + k, l]$ self-orthogonal ($Q \subseteq Q^{\perp_s}$) additive code over \mathbb{F}_4 .*

Proof: Case 1: $i = 0$. Suppose C is an additive code with the mentioned properties and $\dim(C) - \dim(C \cap C^{\perp_s}) = 2k$. Let M be the matrix generator of the code C , where the last $2k$ rows are in $C \setminus C \cap C^{\perp_s}$ and other rows form a basis for $C \cap C^{\perp_s}$. We denote the last $2k$ rows of M with m_1, m_2, \dots, m_{2k} . Since $m_1 \notin C \cap C^{\perp_s}$, there exists at least one m_i , $2 \leq i \leq 2k$ such that $m_1 * m_i = 1$. Without loss of generality, let us assume that $m_1 * m_2 = 1$. If there is another m_j where $3 \leq j \leq 2k$ such that $m_1 * m_j = 1$, then we change m_j with $m_j + m_2$. Moreover, if there exists m_z where $3 \leq z \leq 2k$ such that $m_z * m_2 = 1$, we change m_z with $m_z + m_1$. Now, by considering these changes we can find a new format for the last $2k$ rows of M , such as $m_1, m_2, m'_1, m'_2, \dots, m'_{2k-2}$ such that $m_1 * m_2 = 1$ and for any m'_t where $1 \leq t \leq 2k - 2$ we have $m'_t * m_1 = m'_t * m_2 = 0$. Now, we repeat the above method on $m'_1, m'_2, \dots, m'_{2k-2}$. By continuing this procedure we can find vectors M_1, M_2, \dots, M_{2k} in the last $2k$ rows such that $M_{2i-1} * M_{2i} = 1$ and $M_{2i-1} * M_p = M_{2i} * M_q = 0$ for $1 \leq i \leq k$, $p \neq 2i$, and $q \neq 2i - 1$.

Now, let T be a matrix such that $T_{2s-1, s} = 1$ and $T_{2s, s} = \omega$ for $1 \leq s \leq k$, and the other entries of T are zero. The matrix

$$G = \begin{bmatrix} M_{s \times n} & 0_{s \times k} \\ A_{2k \times n} & T_{2k \times k} \end{bmatrix},$$

where $s = \dim(C \cap C^{\perp_s})$ is the generator matrix of an $[n + k, l]$ additive code Q over \mathbb{F}_4 and one can easily see that $Q \subseteq Q^{\perp_s}$.

Case 2: $i = 1$. Let us assume that $\dim(C) - \dim(C \cap C^{\perp_s}) = 2k + 1$. Using similar steps, we are able to find the vectors $M_1, M_2, \dots, M_{2k}, M_{2k+1}$ for the last $2k + 1$ rows such that $M_{2i-1} * M_{2i} = 1$ and $M_{2i-1} * M_p = M_{2i} * M_q = 0$ for $1 \leq i \leq k$, $p \neq 2i$, and $q \neq 2i - 1$, and M_{2k+1} is orthogonal to all other vectors. In this case, let T' be the the vertical join of matrix T and one zero row. Now, the matrix

$$G = \begin{bmatrix} M_{s \times n} & 0_{s \times k} \\ A_{2k+1 \times n} & T'_{2k+1 \times k} \end{bmatrix}$$

is the generator matrix of the code Q and clearly $Q \subseteq Q^{\perp_s}$. □

Now, we state our main result.

Theorem 3.3.6 *Let C be an $[n, k]$ additive code over \mathbb{F}_4 and $e = \lceil \frac{2n-k - (\dim(C \cap C^{\perp_s}))}{2} \rceil$. If $2n - k - (\dim(C \cap C^{\perp_s}))$ is an odd integer, then there exists an $[[n+e, k-n+e+1, d]]$ quantum code over \mathbb{F}_4 with $d \geq \min\{d(C+v), (d(C+C^{\perp_s})+1)\}$ for all $v \neq 0 \in C^{\perp_s}$. If $2n - k - (\dim(C \cap C^{\perp_s}))$ is an even integer, then there exists an $[[n+e, k-n+e, d]]$ quantum code over \mathbb{F}_4 with $d \geq \min\{d(C), (d(C+C^{\perp_s})+1)\}$.*

Proof: Let C be an additive code with dimension k and C^{\perp_s} be its dual with respect to the symplectic inner product ($\dim(C^{\perp_s}) = 2n - k$ over \mathbb{F}_2). Let $e = \lceil \frac{2n-k - (\dim(C \cap C^{\perp_s}))}{2} \rceil$, and $\dim(C \cap C^{\perp_s}) = s$. We consider two cases.

Case 1. Assume that $2n - k - (\dim(C \cap C^{\perp_s}))$ is an odd integer. Consider the matrix

$$G = \begin{bmatrix} M_{s \times n} & 0_{s \times e} \\ A_{k-s \times n} & 0_{k-s \times e} \\ B_{2e \times n} & T_{2e \times e} \\ v & 0_{1 \times e} \end{bmatrix},$$

where $r(M)$ is a basis for $C \cap C^{\perp_s}$, $r(A) \cup r(M)$ is a basis for C , $r(B) = M_1, M_2, \dots, M_{2e}$, and $v = M_{2e+1}$, where M_i 's satisfy in second part of the proof of Lemma 3.3.5. Finally, the set $r(B) \cup \{v\} \cup r(M)$ is a basis for C^{\perp_s} , and T is the matrix which was introduced in the proof of Lemma 3.3.5. Let E be the additive code generated by the matrix G . Now, consider the code generated by

$$S = \begin{bmatrix} M_{s \times n} & 0_{s \times e} \\ B_{2e \times n} & T_{2e \times e} \end{bmatrix}.$$

By the construction and the above lemma, rows of S are orthogonal to the rows of G . Moreover, $\dim(E) = 2n - s$ and $\dim(E^{\perp_s}) = s + 2e$. Therefore, S is the generator matrix of the code E^{\perp_s} and $E^{\perp_s} \subseteq E$.

Assume $x = (x_1, x_2) \in E$ where $x_1 \in \mathbb{F}_4^n$ and $x_2 \in \mathbb{F}_4^e$. So x is linear combination of rows of G . If no row of B appears in the linear combination, then $wt(x) \geq d(C + v)$. If some of the rows of B enter this linear combination $wt(x) \geq d((C + C^{\perp_s}) + 1)$.

Case 2. Assume that $2n - k - (\dim(C \cap C^{\perp_s}))$ is even. then

$$G = \begin{bmatrix} M_{s \times n} & 0_{s \times e} \\ A_{k-s \times n} & 0_{k-s \times e} \\ B_{2e \times n} & T_{2e \times e} \end{bmatrix}$$

is the matrix generator of the code E and its dual is generated by the matrix S . Rest of the proof is similar to the case 1. □

Using Theorem 3.3.6 we are able to construct a quantum code from an additive code. Note that this construction can easily be extended to \mathbb{F}_q additive codes over \mathbb{F}_{q^2} .

Corollary 3.3.7 *Let C be an $[n, k]_q$ additive code over \mathbb{F}_{q^2} and $e = \lceil \frac{2n-k - (\dim(C \cap C^{\perp_s}))}{2} \rceil$. If $2n - k - (\dim(C \cap C^{\perp_s}))$ is an odd integer, then there exists an $[[n + e, k - n + e + 1, d]]_q$ quantum code over \mathbb{F}_{q^2} with $d \geq \min\{d(C + v), (d(C + C^{\perp_s}) + 1)\}$ for some $v \neq 0 \in C^{\perp_s}$.*

If $2n - k - (\dim(C \cap C^{\perp_s}))$ is an even integer, then there exists an $[[n + e, k - n + e, d]]_q$ quantum code over \mathbb{F}_{q^2} with $d \geq \min\{d(C), (d(C + C^{\perp_s}) + 1)\}$.

Corollary 3.3.8 *Let C be an $[n, k]_q$ linear code over \mathbb{F}_{q^2} and $e' = n - k - (\dim(C \cap C^{\perp_s}))$. Then there exists an $[[n + e', 2k - n + e', d]]$ quantum code with $d \geq \min\{d(C), (d(C + C^{\perp_s}) + 1)\}$.*

Proof: Let C and $C \cap C^{\perp_s}$ be $[n, k]$ and $[n, s]$ linear codes over \mathbb{F}_{q^2} , respectively. We can consider them as $[n, 2k]$ and $[n, 2s]$ additive code over \mathbb{F}_{q^2} . Now, by Corollary 3.3.7 we have

$$e = \left\lceil \frac{2n-k-(\dim(C \cap C^{\perp_s}))}{2} \right\rceil = \left\lceil \frac{2n-2k-2s}{2} \right\rceil = n - k - s = e',$$

and there exists an $[[n + e', 2k - n + e', d]]$ quantum code with $d \geq \min\{d(C), (d(C + C^{\perp_s}) + 1)\}$. \square

Example 3.3.9 In this Example we explain how to use Lemma 3.3.5 and Theorem 3.3.6 to obtain a quantum stabilizer code with a good minimum distance. Let us start with an $[33, 16, 11]$ linear code C which is the best known linear code over \mathbb{F}_4 with these parameters.

Using Magma, we see that $C \cap C^{\perp_s}$ is a $[33, 15]$ linear code which means that $e = 1$. By Theorem 3.3.6 we can obtain a $[[34, 2, 10]]$ quantum code which has the optimum minimum distance (see [8]).

Example 3.3.10 The following table presents some good quantum codes obtained from Theorem 3.3.6.

Parameters of the codes	
Codes over \mathbb{F}_4	Codes over \mathbb{F}_9
$[[34, 2, 10]]$	$[[10, 1, 4]]$
$[[35, 1, 11]]$	$[[11, 1, 5]]$
$[[46, 8, 9]]$	$[[28, 22, 3]]$
$[[47, 7, 10]]$	$[[30, 22, 3]]$
$[[51, 3, 13]]$	$[[32, 20, 4]]$
$[[52, 2, 14]]$	$[[32, 22, 4]]$
$[[53, 1, 15]]$	$[[34, 18, 6]]$
$[[58, 4, 14]]$	$[[41, 25, 6]]$
$[[61, 1, 17]]$	$[[41, 33, 4]]$

Bibliography

- [1] Ashikhmin A, Knill E. Nonbinary quantum stabilizer codes. *IEEE Transactions on Information Theory*. 2001 Nov;47(7):3065-72.
- [2] Calderbank AR, Shor PW. Good quantum error-correcting codes exist. *Physical Review A*. 1996 Aug 1;54(2):1098.
- [3] Calderbank AR, Rains EM, Shor PM, Sloane NJ. Quantum error correction via codes over GF (4). *IEEE Transactions on Information Theory*. 1998 Jul;44(4):1369-87.
- [4] Güneri C. Artin-Schreier curves and weights of two-dimensional cyclic codes. *Finite Fields and Their Applications*. 2004 Oct 1;10(4):481-505.
- [5] Degwekar A, Guenda K, Gulliver TA. Extending construction X for quantum error-correcting codes. In *Coding Theory and Applications 2015* (pp. 141-152). Springer International Publishing.
- [6] Dieks DG. Communication by EPR devices. *Physics Letters A*. 1982 Nov 22;92(6):271-2.
- [7] Gottesman D. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Physical Review A*. 1996 Sep 1;54(3):1862.
- [8] Grassl M. Bounds on the minimum distance of linear codes and quantum codes (2007). Online available at <http://www.codetables.de>. Accessed on 2017-04-30.
- [9] Imai H. A theory of two-dimensional cyclic codes. *Information and Control*. 1977 May 1;34(1):1-21.
- [10] Lisonk P, Singh V. Quantum codes from nearly self-orthogonal quaternary linear codes. *Designs, Codes and Cryptography*. 2014 Nov 1;73(2):417-24.
- [11] Sepasdar Z. Some notes on the characterization of two dimensional skew cyclic codes. *Journal of Algebra and Related Topics*. 2016 Dec 20;4(2):1-8.
- [12] Shor PW. Scheme for reducing decoherence in quantum computer memory. *Physical review A*. 1995 Oct 1;52(4):R2493.
- [13] MacWilliams FJ, Sloane NJ. *The Theory of Error-Correcting Codes*. Elsevier; 1977.
- [14] Steane AM. Simple quantum error-correcting codes. *Physical Review A*. 1996 Dec 1;54(6):4741.

- [15] Steane A. Multiple-particle interference and quantum error correction. In Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 1996 Nov 8 (Vol. 452, No. 1954, pp. 2551-2577). The Royal Society.
- [16] Wootters WK, Zurek WH. A single quantum cannot be cloned. Nature. 1982 Oct 28;299(5886):802-3.