QUANTUM BICYCLIC CODES

A Project Report

submitted by

RAYUDU SANKARA SAI CHAITHANYA

in partial fulfilment of the requirements
for the award of the degree of

BACHELOR OF TECHNOLOGY
AND
MASTER OF TECHNOLOGY

DEPARTMENT OF ELETCRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY MADRAS.

MAY 2019

THESIS CERTIFICATE

This is to certify that the thesis titled **Quantum Bicyclic Codes**, submitted by **Rayudu Sankara Sai Chaithanya**, to the Indian Institute of Technology, Madras, in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology and Master of Technology**, is a bona fide record of the research work done by him under our supervision. The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Prof. Pradeep Kiran Sarvepalli
Research Guide
Dept. of Electrical Engineering
IIT-Madras, 600 036

Place: Chennai

Date: May 2019

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my guide Dr. Pradeep Kiran Sarvepalli for the continuous support of my Masters thesis and related research, for his patience, and motivation. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better guide.

I would like to thank my family: my parents, my brother, my uncles for supporting me throughout my five years of journey at IIT Madras. Finally I would like to thank all my friends who made my time at IIT Madras fun, interesting and worthwhile.

ABSTRACT

Bicyclic codes are a generalization of the one dimensional (1D) cyclic codes to two dimensions (2D). Similar to the 1D case, in some cases, 2D cyclic codes can also be constructed to guarantee a specified minimum distance. Many aspects of these codes are yet unexplored. Motivated by the problem of constructing quantum codes, in this thesis we study some structural properties of certain bicyclic codes. We show that a primitive bicyclic hyperbolic code of length n^2 contains its dual if and only if its design distance is lower than $n - \Delta$, where $\Delta = \mathcal{O}(\sqrt{n})$. We also show that over quadratic extension fields, a primitive bicyclic hyperbolic code of length n^2 contains its Hermitian dual if and only if its design distance is lower than $n-\Delta_h$, where $\Delta_h = \mathcal{O}(\sqrt{n})$. Our results are analogous to some structural results known for BCH and Reed-Solomon codes. They further our understanding of bicyclic codes. We also give an application of these results by constructing two classes of quantum bicyclic codes.

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATIONS

CSS	Calderbank-Shor-Steane
BCH	Bose-Chaudhuri-Hocquenghem

NOTATION

$\mathbb{Z}$	Set of integers
$\mathbf{F}$	Finite field
$\mathbf{F}_q$	Finite field with q elements
$\mathcal{C}$	Linear code/Cyclic code/Bicyclic code
$\mathcal{C}^{\perp}$	Euclidean dual code of $\mathcal{C}$
$\mathcal{C}^{\perp_h}$	Hermitian dual code of $\mathcal{C}$

CHAPTER 1

Introduction

Cyclic codes are an important class of error correcting codes. Many popular codes such as BCH codes and Reed-Solomon codes are cyclic codes. Some cyclic codes can be constructed with a large minimum distance. Many subclasses of cyclic codes also have efficient decoders. It is known that a classical code can be used to construct quantum code, Steane (1996); Calderbank and Shor (1996); Calderbank *et al.* (1998); Ashikhmin and Knill (2001), if the code contains its (Euclidean or Hermitian) dual. Using these constructions many (cyclic) quantum codes have been proposed: Grassl *et al.* (1997, 2004); Ketkar *et al.* (2006). Grassl *et al.* (1997) gave a simple test for identifying cyclic codes that contain their duals. Important structural results have been shown for some classes of cyclic codes such as BCH codes. For instance, Steane (1999) gave a condition based on the designed distance to check whether a primitive binary BCH contains its Euclidean dual. Subsequently, Aly *et al.* (2007) extended this to result in the higher alphabet as well as non-primitive codes. They proved that one dimensional primitive BCH code of length n contain their dual when their design distance is less than $\delta = \mathcal{O}(\sqrt{n})$. However, most of the previous work has been limited to one dimension even though classically, cyclic codes have been generalized to higher dimensions.

Two dimensional (2D) cyclic codes, also called bicyclic codes, are a generalization of one-dimensional cyclic codes to two dimensions. In the case of one-dimensional cyclic codes, codewords can be viewed as vectors. The codewords of bicyclic codes can be viewed as matrices. A general theory of 2D cyclic codes was introduced by Imai (1977). Since then, there has been extensive work on bicyclic codes, see Blahut (2008) for a good overview of related work and references. However, there does not appear to be much work on quantum bicyclic codes.

There are many important differences between cyclic and bicyclic codes which makes the analysis of these codes much more challenging than cyclic codes. For instance, bicyclic codes do not have a unique generator polynomial, unlike the cyclic codes. Furthermore, the division of polynomials by bivariate polynomials does not lead to unique remainders. All these reasons motivate our study of quantum bicyclic codes.

Our main contributions are as follows:

i) We give necessary and sufficient condition for a bicyclic hyperbolic code to contain its Euclidean dual.

ii) For a bicyclic hyperbolic code, defined over a quadratic extension field, we also give a necessary and sufficient condition for it to contain its Hermitian dual.

iii) We construct new quantum bicyclic codes.

iv) Our analysis of the cyclotomic cosets of cyclic codes could be of independent interest and use in the study of cyclic codes over higher dimensions.

This thesis is organized as follows. After a brief review of the necessary background in Chapter 2, we prove structural results on bicyclic codes in Chapter 3. We also study the application of these results to quantum codes in Chapter 3. We will finally conclude this thesis with some directions for future research in Chapter 4.

CHAPTER 2

Bicyclic Codes

In this chapter, we will first briefly review the topic of bicyclic code and their characterization using common zeros of the code in polynomial representation. We will rely on this characterization of bicyclic codes heavily in this thesis to prove all our results. We will also review the topic of biyclic hyperbolic code.

2.1 Bicyclic Codes

Let $\mathcal{C}$ be a linear code of length $n_1 n_2$ over a field $\mathbf{F}$, whose codewords are written as two dimensional array of length $n_1 \times n_2$. If $\mathcal{C}$ is closed under both circular right shift of columns and circular down shift of rows then $\mathcal{C}$ is called a bicyclic code of length $n_1 \times n_2$ over $\mathbf{F}$. we will denote codewords with c and i^{th} row, j^{th} column element with $c_{i,j}$.

$$c = \begin{bmatrix} c_{0,0} & c_{0,1} & c_{0,2} & \cdots & c_{0,n_2-1} \\ c_{1,0} & c_{1,1} & c_{1,2} & \cdots & c_{1,n_2-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n_1-1,0} & c_{n_1-1,1} & c_{n_1-1,2} & \cdots & c_{n_1-1,n_2-1} \end{bmatrix}$$

we will denote the codeword obtained by circular right shift of columns with $c^{(0,1)}$ and codeword obtained by circular down shift of rows with $c^{(1,0)}$.

$$c^{(0,1)} = \begin{bmatrix} c_{0,n_2-1} & c_{0,0} & c_{0,1} & \cdots & c_{0,n_2-2} \\ c_{1,n_2-1} & c_{1,0} & c_{1,1} & \cdots & c_{1,n_2-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n_1-1,n_2-1} & c_{n_1-1,0} & c_{n_1-1,1} & \cdots & c_{n_1-1,n_2-2} \end{bmatrix}$$

$$c^{(1,0)} = \begin{bmatrix} c_{n_1-1,0} & c_{n_1-1,1} & c_{n_1-1,2} & \cdots & c_{n_1-1,n_2-1} \\ c_{0,0} & c_{0,1} & c_{0,2} & \cdots & c_{0,n_2-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n_1-2,0} & c_{n_1-2,1} & c_{n_1-2,2} & \cdots & c_{n_1-2,n_2-1} \end{bmatrix}$$

2.2 Polynomial Representation

Codewords of a bicyclic codes can be also represented as polynomials of two variables, say u, v over a field $\mathbf{F}$ where $c_{i,j}$ will be the coefficient of the polynomial term $u^i v^j$.

$$c(u,v) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} c_{i,j}\ u^i v^j$$

Then the polynomial representation of codeword obtained by taking right circular shift of columns in the matrix representation is obtained by multiplying $c(u,v)$ with u and taking modulo $u^{n_1} - 1$.

$$c^{(1,0)}(u,v) = uc(u,v) \bmod (u^{n_1} - 1)$$

Similarly for the polynomial representation of codeword obtained by taking the down circular shift of rows in the matrix representation is obtained by multiplying $c(u,v)$ with v and taking modulo $v^{n_2} - 1$.

$$c^{(0,1)}(u,v) = vc(u,v) \bmod (v^{n_2} - 1)$$

Let $\mathbf{F}[u,v]$ denote the ring of polynomials over field $\mathbf{F}$. Since bicyclic codes are also linear the following condition holds true for bicyclic codes.

$$c(u,v) \in \mathcal{C} \implies \big[(a(u,v)c(u,v)) \bmod (u^{n_1} - 1, v^{n_2} - 1)\big] \in \mathcal{C}$$

for all $a(u,v)$ in polynomial ring $\mathbf{F}[u,v]$. Therefore bicyclic codes can be considered as ideals of quotient polynomial ring $R := \mathbf{F}[u,v]/\langle u^{n_1} - 1, v^{n_2} - 1\rangle$.

2.3 Characterization

One dimensional cyclic code of length n over a finite field $\mathbf{F}_q$ with q elements, is completely characterized by a unique monic generator polynomial when n and q are co-prime. In the case of bicyclic codes, direct division is not possible among polynomials with two variables. Therefore there need not always exist a unique generator polynomial for a bicyclic code.

Another way of looking at it is that one dimensional cyclic are characterized by common zeros of all the codeword polynomials and $u^n - 1$. This can be extended to bicyclic code as well. Common zeros of all the codeword polynomials, $u^{n_1} - 1$ and $v^{n_2} - 1$ completely characterizes a bicyclic code of length $n_1 \times n_2$ over $\mathbf{F}_q$ when q is co-prime to both n_1 and n_2. Common zeros will be of the form (α^i, β^j) where α and β are the n_1^{th} and n_2^{th} primitive roots of unity. Therefore set of all such possible zeros is

$$\Omega = \left\{(\alpha^i, \beta^j) \mid 0 \leq i < n_1, 0 \leq j < n_2\right\}. \tag{2.1}$$

It is easy to keep track of zeros just by the exponents of α and β. Therefore we will define the **defining set** of a code $\mathcal{C}$ as the following

$$\mathcal{Z} = \{(x, y) \mid (\alpha^x, \beta^y) \text{ is a common zero of code } \mathcal{C}\} \tag{2.2}$$

Observe that since the codewords are over the field $\mathbf{F}_q$ and α and β may lie in an extended field of $\mathbf{F}_q$, if (x, y) is in the defining set of code $\mathcal{C}$ then all the points of the form (xq^l, yq^l) for $l \in \mathbb{Z}, l \geq 0$, should also be in the defining set code $\mathcal{C}$. Set of all such points are called q-ary cyclotomic coset of (x, y), represented with $\text{Coset}(x, y)$.

$$\text{Coset}(x, y) = \left\{(xq^l \bmod n_1, yq^l \bmod n_2) \mid l \in \mathbb{Z}, l \geq 0\right\} \tag{2.3}$$

Any polynomial which vanishes at the common zeros of a bicyclic code is a codeword of that bicyclic code. This is an implication of *discrete nullstellensatz* theorem from algebraic geometry. For the sake of completeness we will prove the following theorem.

Theorem 1. *Suppose n_1, n_2 are positive integers and q is a power prime such that*

$gcd(n_1, q) = gcd(n_2, q) = 1$. Let I be an ideal of quotient polynomial ring $R := \mathbf{F}[u, v]/\langle u^{n_1} - 1, v^{n_2} - 1\rangle$. Let $\mathcal{Z}$ be the defining set of ideal I. Then a polynomial $p(u, v)$ belong to I if and only if $p(\alpha^x, \beta^y) = 0 \; \forall \; (x, y) \in \mathcal{Z}$ where α and β are the n_1^{th} and n_2^{th} roots of unity.

Proof: The necessary condition that $p(\alpha^x, \beta^y) = 0 \; \forall \; (x, y) \in \mathcal{Z}$ if $p(u, v) \in I$ is obvious from the definition of defining set $\mathcal{Z}$. The proof of sufficiency conditions is as follows. For every Coset$(x, y) \not\subset \mathcal{Z}$, there exists a $s(u, v) \in I$ such that $s(\alpha^{x'}, \beta^{y'}) \neq 0 \; \forall \; (x', y') \in$ Coset(x, y). Furthermore there exists an element $a(u, v) \in R$ such that the following condition holds true.

$$a(\alpha^{x'}, \beta^{y'})s(\alpha^{x'}, \beta^{y'}) = \begin{cases} 1 \text{ if } (x', y') \in \text{Coset}(x, y) \\ 0 \text{ if } (x', y') \notin \text{Coset}(x, y) \end{cases}$$

For every Coset$(x, y) \not\subset \mathcal{Z}$, it is possible to find $\gamma^{x,y}(u, v) = a(u, v)s(u, v)$ which satisfies the above condition. But the polynomials $\{\gamma^{x,y}(u, v)\}$ constructed in this manner forms a vector space basis for an ideal I' which has all polynomials that vanish at (α^x, β^y) when $(x, y) \in \mathcal{Z}$. This implies $I' = I$. □

2.4 Bicyclic Hyperbolic codes

One dimensional BCH codes are well-known codes in classical coding theory as they provide a convenient way to construct codes with the minimum distance of the code a design parameter. The construction of one-dimensional BCH codes can be generalized to two dimensions as well.

A bicyclic code $\mathcal{C}$ of length $n_1 \times n_2$ over $\mathbf{F}_q$, where q is co-prime to both n_1 and n_2, is called a bicyclic hyperbolic code with designed distance δ if the defining set of $\mathcal{C}$ is of the following form

$$\mathcal{Z} = \bigcup_{(x,y) \in \mathcal{Z}_{des}} \text{Coset}(x, y) \tag{2.4}$$

$$\mathcal{Z}_{des} = \{(a + x \bmod n_1, b + y \bmod n_2) \mid xy < \delta\} \tag{2.5}$$

where $1 \leq x \leq n_1$, $1 \leq y \leq n_2$. The codes constructed using the above definition are guaranteed have a minimum distance greater than or equal to δ. Note that we have freedom in choosing a and b in the above definition of bicyclic hyperbolic codes. Let us call $\mathcal{Z}_{des}$ the designed set of bicyclic hyperbolic code $\mathcal{C}$. Note that $\mathcal{Z}_{des}$ is only a subset of $\mathcal{Z}$ but it enough to completely characterize a bicyclic hyperbolic code. Analogous to one dimensional case we will define the following.

- Primitive: when $n_1 = n_2 = n = q^m - 1$.
- Narrow-sense: when $a = b = 0$

In this thesis we will look at narrow-sense bicyclic hyperbolic codes with $n_1 = n_2 = n$. We denote such a bicyclic code of design distance d by $\mathcal{H}(n \times n, q; d)$.

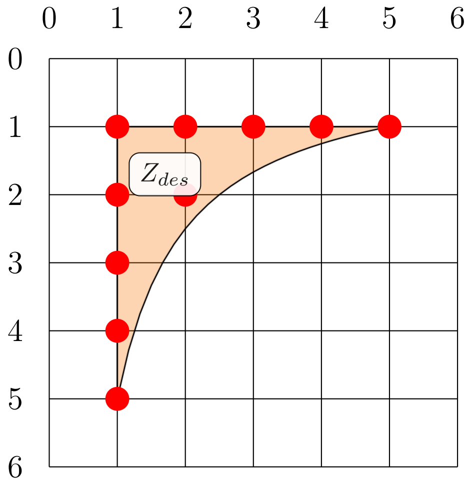

Figure 2.1: Hyperbolic shape: $\mathcal{Z}_{des}$ of a primitive narrow-sense bicyclic hyperbolic code of length 7×7 code with $\delta = 6$.

The characterization of bicyclic hyperbolic codes in terms of common zeros or designed/defining set gives us a useful handle to further analyze several other properties of bicyclic hyperbolic codes which is a central topic of this thesis.

CHAPTER 3

Quantum Bicyclic Codes

In the previous chapter, we reviewed the topic of bicyclic codes and their characterization in terms of common zeros or defining set. Using this characterization, We reviewed the topic of bicyclic hyperbolic codes. To further our understanding of bicyclic hyperbolic codes, we will prove some results on the structure of cyclotomic cosets which will be used to prove the existence of Euclidean dual containing and Hermitian dual containing bicyclic hyperbolic codes.

3.1 Structural Results on Cyclotomic Cosets

In this section, we will prove some results on the structure of cyclotomic cosets. These proofs for these results involve some simple numerical arguments and are very easy follow.

Lemma 2. *Suppose $n = q^m - 1$, $m > 3$ and the sets $\mathcal{Z}_{des}$ and $\mathcal{Z}_{des,k}$ are defined as follows where $0 \leq k \leq (m-1)/2$.*

$$Z_{des} = \left\{(x, y) \;\middle|\; xy < q^m - 1 - q^{\lfloor m/2 \rfloor}, 1 \leq x, y \leq n\right\} \tag{3.1}$$

$$Z_{des,k} = \left\{(x, y) \;\middle|\; q^k - 1 < x \leq q^{k+1} - 1, (x, y) \in Z\right\} \tag{3.2}$$

Then the following equations hold true for $l \in \{0, 1, 2 \ldots m-1\}$.

1.

$$\min_{\substack{(x,y)\in Z_{des,k} \\ l \neq m-k-1}} (-xq^l \ mod\ n)(-yq^l \ mod\ n) \quad = \quad q^m - 1 - q^{\lceil m/2 \rceil - 1} \tag{3.3}$$

2.

$$\min_{\substack{(x,y)\in Z_{des,k} \\ l = m-k-1}} (-xq^l \ mod\ n)(-yq^l \ mod\ n) \quad \begin{cases} = & (q^{\lfloor m/2 \rfloor} - 1)^2 \quad when\ k = m/2 - 1 \\ \\ \geq & q^m - 1 \quad otherwise \end{cases} \tag{3.4}$$

Proof: Let $(x, y) \in \mathcal{Z}_{des,k}$. Since $xy < q^m - 1$, (x, y) should have the following q-ary form.

$$x = \sum_{i=0}^{k} x_i q^i, \; x_k \neq 0 \qquad y = \sum_{j=0}^{m-k-1} y_j q^j \tag{3.5}$$

where $0 \leq x_i, y_j \leq q - 1$. Note that y_{m-k-1} need not be non-zero here. Consequesntly $(n - x, n - y)$ will have the following q-ary form.

$$(n - x) = \sum_{i=0}^{k} (q - 1 - x_i) q^i + \sum_{i=k+1}^{m-1} (q - 1) q^i, \; x_k \neq 0 \tag{3.6a}$$

$$(n - y) = \sum_{j=0}^{m-k-1} (q - 1 - y_j) q^i + \sum_{j=m-k}^{m-1} (q - 1) q^j \tag{3.6b}$$

q-ary form of $(-xq^l \bmod n)$ and $(-yq^l \bmod n)$ are obtained by taking the l^{th} right circular shift of q-ary coefficients of $(n - x)$ and $(n - y)$ respectively.

1. **When $\boldsymbol{0 \leq l < m - k - 1}$:**

$$\begin{aligned}(-xq^l \bmod n) = &\left(\sum_{i=0}^{l-1} (q - 1) q^i\right) + q^l \left(\sum_{i=0}^{k} (q - 1 - x_i) q^i\right) \\ &+ \left(\sum_{i=k+l+1}^{m-1} (q - 1) q^i\right)\end{aligned} \tag{3.7}$$

When $l < m - k - 1$, $(m - 1)^{th}$ q-ary coefficient of $\left(-xq^l \bmod n\right)$ is equal to $(q - 1)$. Let us assume that the minimum value of $\left(-xq^l \bmod n\right)\left(-yq^l \bmod n\right)$ is less than $q^m - 1$. This is possible only if $\left(-yq^l \bmod n\right) = 1$, or equivalently if $y = q^m - 1 - q^{m-l}$. Given that $xy < q^m - 1 - q^{\lfloor m/2 \rfloor}$, $y = q^m - 1 - q^{m-l}$ implies $l \leq \lceil m/2 \rceil - 1$ and $x = 1$. Under these conditions minimum value of $\left(-xq^l \bmod n\right)$ occurs when $l = \lceil m/2 \rceil - 1$ which is equal to $q^m - 1 - q^{\lceil m/2 \rceil - 1}$.

2. **When $\boldsymbol{l = m - k - 1}$:**

$$(-xq^l \bmod n) = \left(\sum_{i=0}^{m-k-2} (q-1)q^i\right) + q^{m-k-1}\left(\sum_{i=0}^{k}(q-1-x_i)q^i\right) \tag{3.8a}$$

$$\begin{aligned}(-yq^l \bmod n) = &\left(\sum_{j=0}^{m-2k-2} (q-1-y_{j+k+1})q^j\right) + \left(\sum_{j=m-2k-1}^{m-k-2} (q-1)q^j\right)\\ &+ q^{m-k-1}\left(\sum_{j=0}^{k}(q-1-y_j)q^j\right)\end{aligned} \tag{3.8b}$$

Let us assume that the minimum value of $\left(-xq^l \bmod n\right)\left(-yq^l \bmod n\right)$ is less than $q^m - 1$. If $k = 0$ then $\left(-xq^l \bmod n\right)$ is greater than or equal to $q^{m-1} - 1$ and, since $y < q^m - 1 - q^{\lfloor m/2 \rfloor}$, $(-yq^l \bmod n)$ is greater than or equal to $q^{\lfloor m/2 \rfloor + 1}$. Therefore the product $\left(-xq^l \bmod n\right)\left(-yq^l \bmod n\right)$ is greater than $q^m - 1$. When $k \neq 0$, both $\left(-xq^l \bmod n\right)$ and $\left(-yq^l \bmod n\right)$ are greater than or equal to q^{m-k-2} which implies the product $\left(-xq^l \bmod n\right)\left(-yq^l \bmod n\right)$ is greater than or equal to $q^{2m-2k-4}$. Combining this with $\left(-xq^l \bmod n\right)\left(-yq^l \bmod n\right) < q^m - 1$, we get $k \geq (m-3)/2$. we also have the inequality $k \leq (m-1)/2$. This implies the possible values of k are $(m-3)/2$, $(m-1)/2$ when m is odd and $m/2 - 1$ when m is even.

(a) When $k = (m-3)/2$,

$$(-xq^l \bmod n) = \left(\sum_{i=0}^{(m-1)/2} (q-1)q^i\right) + q^{(m+1)/2}\left(\sum_{i=0}^{(m-3)/2} (q-1-x_i)q^i\right) \tag{3.9a}$$

$$\begin{aligned}(-yq^l \bmod n) = &\left(\sum_{j=0}^{1}(q-1-y_{j+(m-1)/2})q^j\right) + \left(\sum_{j=2}^{(m-1)/2} (q-1)q^j\right)\\ &+ q^{(m+1)/2}\left(\sum_{i=0}^{(m-3)/2} (q-1-y_j)q^j\right)\end{aligned} \tag{3.9b}$$

If at all $(-xq^l \bmod n)(-y \bmod n)$ is less than $q^m - 1$, then all the x_i,y_j must be equal to $q-1$ for $0 \leq i, j \leq (m-3)/2$. This implies both $y_{(m-1)/2}$ and $y_{(m+1)/2}$ cannot be equal to $q-1$ as xy is less than $q^m - 1 - q^{(m-1)/2}$. Then the product $(-xq^l \bmod n)(-yq^l \bmod n) \geq \left(q^{(m-1)/2} - 1\right)\left(q^2(q^{(m-3)/2} - 1) + 1\right)$ cannot be less than $q^m - 1$.

(b) When $k = (m-1)/2$,

$$(-xq^l \bmod n) = \left(\sum_{i=0}^{(m-3)/2} (q-1)q^i \right) + q^{(m-1)/2} \left(\sum_{i=0}^{(m-1)/2} (q-1-x_i)q^i \right) \tag{3.10a}$$

$$(-yq^l \bmod n) = \left(\sum_{j=0}^{(m-3)/2} (q-1)q^j \right) + q^{(m-1)/2} \left(\sum_{j=0}^{(m-1)/2} (q-1-y_j)q^j \right) \tag{3.10b}$$

Since xy is less than $(q^m - 1 - q^{\lfloor m/2 \rfloor})$, at least on of the $\{x_{(m-3)/2},\ y_{(m-3)/2},\ x_{(m-1)/2},\ y_{(m-1)/2}\}$ must be equal to zero. This implies at least one of the $\{(-xq^l \bmod n), (-yq^l \bmod n)\}$ must be greater than or equal to $q^{(m-1)/2} - 1 + q^{m-2}$ and the product $\{(-xq^l \bmod n)(-yq^l \bmod n)\} \geq (q^{(m-1)/2} - 1)(q^{(m-1)/2} - 1 + q^{m-2})$ cannot be less than $q^m - 1$.

(c) When $k = m/2 - 1$,

$$(-xq^l \bmod n) = \left(\sum_{i=0}^{m/2-1} (q-1)q^i \right) + q^{m/2} \left(\sum_{i=0}^{m/2-1} (q-1-x_i)q^i \right) \tag{3.11a}$$

$$\begin{aligned}(-yq^l \bmod n) = \big(q-1-y_{m/2}\big) + &\left(\sum_{j=1}^{m/2-1} (q-1)q^j \right) \\ &+ q^{m/2} \left(\sum_{j=0}^{m/2-1} (q-1-y_j)q^j \right)\end{aligned} \tag{3.11b}$$

Since xy is less than $(q^m - 1 - q^{\lfloor m/2 \rfloor})$, at least on of the $\{x_{m/2-2},\ x_{m/2-1},\ y_{m/2},\ y_{m/2-1}\}$ must be equal to zero. Therefore, from the above equations, minimum value of $\big(-xq^l \bmod n\big)\ \big(-yq^l \bmod n\big)$ occurs when $(y_{m/2}) = 0$, and the minimum value is equal to $(q^{m/2} - 1)^2$

3. **When $\boldsymbol{m-k-1<l\leq m-1}$:**

$$
\begin{aligned}
(-xq^l \bmod n) &= \left(\sum_{i=0}^{l-(m-k)} (q-1-x_{i+m-l})q^i\right) + \left(\sum_{i=l-(m-k-1)}^{l-1} (q-1)q^i\right) \\
&\qquad + q^l\left(\sum_{i=0}^{m-l-1} (q-1-x_i)q^i\right) \qquad (3.12a) \\
(-yq^l \bmod n) &= \left(\sum_{j=0}^{l-k-1} (q-1-y_{j+m-l})q^j\right) + \left(\sum_{j=l-k}^{l-1} (q-1)q^j\right) \\
&\qquad + q^l\left(\sum_{j=0}^{m-l-1} (q-1-y_j)q^j\right) \qquad (3.12b)
\end{aligned}
$$

$(-xq^l \bmod n) \geq q^{l-m+k+1}(q^{m-k-1}-1)$ and $(-yq^l \bmod n) \geq q^{l-k}(q^k-1)$. Assume that the minimum value of $\left(-xq^l \bmod n\right)\left(-yq^l \bmod n\right)$ is less than q^m-1. Then $2l-2$ must be less than m. Additionally the inequalities $m-k-1<l$ and $k \leq (m-1)/2$ imply $l=(m+1)/2$ and $k=(m-1)/2$. Subsequently the following inequality holds true.

$$
\begin{aligned}
(-xq^l \bmod n)(-yq^l \bmod n) &\geq q^2\left(q^{(m-1)/2}-1\right)^2 \\
&> q^m-1 \qquad (3.13)
\end{aligned}
$$

□

The above lemma will be useful in proving results on existence of Euclidean dual containing bicyclic hyperbolic code which are given in the next section.

Corollary 3. *Suppose $n=q^{2m}-1$, $m>3$ and $\mathcal{Z}_{des}$ and $\mathcal{Z}_{des,k}$ are defined as follows, where $k \leq (2m-1)/2$*

$$\mathcal{Z}_{des} = \left\{(x,y) \mid xy < q^{2m}-1-q^m, 1 \leq x,y \leq n\right\} \qquad (3.14)$$

$$\mathcal{Z}_{des,k} = \left\{(x,y) \mid q^k-1 < x \leq q^{k+1}-1, (x,y) \in Z\right\} \qquad (3.15)$$

Then the following equations hold true for $l \in \{1,3,5\ldots 2m-1\}$.

1.

$$\min_{\substack{(x,y\in Z_{des,k} \\ l\neq 2m-k-1}} (-xq^l \ mod\ n)(-yq^l \ mod\ n) \quad = \quad q^{2m}-1-q^{m-1} \qquad (3.16)$$

2.

$$\min_{\substack{(x,y)\in Z_{des,k}\\ l=2m-k-1}} (-xq^l \ \textit{mod } n)(-yq^l \ \textit{mod } n) \begin{cases} = & (q^m-1)^2 \quad {\scriptstyle \textit{when } m \textit{ is odd} \atop \textit{and } k=m-1} \\ \geq & q^{2m}-1 \quad \textit{otherwise} \end{cases} \tag{3.17}$$

Proof: The proof follows from lemma 2. By replacing m with $2m$ in lemma 2, we will get Eq. (3.16) directly. For Eq. (3.17), we need to use the additional constraint that we are limiting l to $\{1,3,5....2m-1\}$ and not the whole set of $\{1,2,3....2m\}$. Replacing m with $2m$ in Lemma 2 and restating Eq. (3.4), we will get the following result.

$$\min_{\substack{(x,y)\in Z_{des,k}\\ l=2m-k-1}} (-xq^l \bmod n)(-yq^l \bmod n) \begin{cases} = & (q^m-1)^2 \quad \text{when } k=m-1 \\ \geq & q^{2m}-1 \quad \text{otherwise} \end{cases} \tag{3.18}$$

But in this case when m is even, $k=m-1$ implies $l=m \notin \{1,3,5...2m-1\}$. Therefore we get the following condition

$$\min_{\substack{(x,y)\in Z_{des,k}\\ l=2m-k-1}} (-xq^l \bmod n)(-yq^l \bmod n) \begin{cases} = & (q^m-1)^2 \quad {\scriptstyle \text{when } m \text{ is odd} \atop \text{and } k=m-1} \\ \geq & q^{2m}-1 \quad \text{otherwise} \end{cases} \tag{3.19}$$

□

The above corollary will be useful in proving results on existence of Hermitian dual containing bicyclic hyperbolic which are given in a later section.

3.2 Euclidean Dual Containing Codes

The Euclidean dual code $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ is defined as $\{c' \mid c'.c = 0 \ \forall \ c \in \mathcal{C}\}$. In the case of cyclic linear code, this condition can be simplified and can be given in terms of the zeros of the cyclic code. Suppose $\mathcal{Z}$ is the defining set of cyclic code $\mathcal{C}$ of length $n \times n$ over the field $\mathbf{F}_q$ and $\gcd(n,q) = 1$ then the defining set of $\mathcal{C}^\perp$ is $\mathcal{Z}_{tot} - \mathcal{Z}^{-1}$

where $\mathcal{Z}_{tot} = \{(x,y) \,|0 \leq x, y \leq n-1\}$ and $\mathcal{Z}^{-1} = \{(-x,-y) \text{ mod } n \mid (x,y) \in \mathcal{Z}\}$. In this context, the following lemma gives a condition to verify if a cyclic code contains its Euclidean dual code in terms of defining set $\mathcal{Z}$.

Lemma 4. *Let $\mathcal{C}$ be the bicyclic code of length $n \times n$ over $\mathbf{F}_q$ such that $gcd(n,q) = 1$ and $\mathcal{Z}$ be the defining set of $\mathcal{C}$. Then the code contains its Euclidean dual if and only if*

$$\mathcal{Z} \cap \mathcal{Z}^{-1} = \phi \tag{3.20}$$

where $\mathcal{Z}^{-1} = \{(-x,-y) \text{ mod } n \,|\, (x,y) \in \mathcal{Z}\}$.

Proof: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two bicyclic cyclic codes with defining sets $\mathcal{Z}_1$ and $\mathcal{Z}_2$. If $\mathcal{C}_1$ is contained in $\mathcal{C}_2$ then all codewords that are in $\mathcal{C}_1$ are also in $\mathcal{C}_2$. This implies defining set (or common zero set) of $\mathcal{C}_2$ is contained in that of $\mathcal{C}_1$. Since $\mathcal{Z}_{tot} - \mathcal{Z}^{-1}$ is the defining set of dual code $\mathcal{C}^{\perp}$, $\mathcal{C}^{\perp}$ is contained in $\mathcal{C}$ if and only if $\mathcal{Z} \subset \mathcal{Z}_{tot} - \mathcal{Z}^{-1}$.

$$\mathcal{Z} \subset \mathcal{Z}_{tot} - \mathcal{Z}^{-1} \implies \mathcal{Z} \cap \mathcal{Z}^{-1} = \phi$$

□

The above condition for Euclidean dual containing can be further simplified in the case of bicyclic hyperbolic codes as the defining set $\mathcal{Z}$ is completely characterized by the designed set $\mathcal{Z}_{des}$.

Lemma 5. *Let $\mathcal{C}$ be a bicyclic hyperbolic code of length $n \times n$ over $\mathbf{F}_q$ such that $gcd(n,q) = 1$. Let $\mathcal{Z}_{des}$ and $\mathcal{Z}$ be the designed set and defining set of $\mathcal{C}$ respectively. The code $\mathcal{C}$ contains its Euclidean dual if and only if*

$$\mathcal{Z}_{des} \cap \mathcal{Z}^{-1} = \phi \tag{3.21}$$

where $\mathcal{Z}^{-1} = \{(-x,-y) \text{ mod } n \mid (x,y) \in \mathcal{Z}\}$.

Proof: Based on lemma 4, $\mathcal{Z} \cap \mathcal{Z}^{-1} = \phi$ must be true for a bicyclic cyclic code to contain its Euclidean dual. If at all there is a common element, say (x,y), between $\mathcal{Z}$ and $\mathcal{Z}^{-1}$, then q-ary cyclotomic coset of (x,y) must be there in both $\mathcal{Z}$ and $\mathcal{Z}^{-1}$.

Therefore $Z \cap \mathcal{Z}^{-1} = \phi$ is true if and only if there is no common coset between $\mathcal{Z}$ and $\mathcal{Z}^{-1}$. Since every coset in $\mathcal{Z}$ contains at least one element from $\mathcal{Z}_{des}$, $\mathcal{Z} \cap \mathcal{Z}^{-1} = \phi$ is true if and only if $\mathcal{Z}_{des} \cap \mathcal{Z}^{-1} = \phi$. □

For a bicyclic hyperbolic code, designed set and defining set depend on the designed distance of the code. As the designed distance increases, the sizes of $\mathcal{Z}_{des}$ and $\mathcal{Z}$ increases. Therefore, after a certain designed distance, it is not possible for the bicyclic hyperbolic code to contain its Euclidean dual code as the intersection between $\mathcal{Z}_{des}$ and $\mathcal{Z}^{-1}$ will no longer be empty. The following theorem gives an easy condition based on the designed distance to verify if a primitive narrow-sense bicyclic hyperbolic code contains its Euclidean dual.

Theorem 6. *Primitive narrow-sense bicyclic hyperbolic code of length $n \times n$ over $GF(q)$, where $n = q^m - 1$, contains its Euclidean dual if and only if the design distance d satisfies $2 \leq d \leq \delta$, where*

$$\delta = \begin{cases} (q^m - 1) - 2(q^{m/2} - 1) & m \text{ is even} \\ (q^m - 1) - (q^{\frac{m-1}{2}}) & m \text{ is odd} \end{cases} \tag{3.22}$$

Proof: For proving $\mathcal{H}(n \times n, q; d)^{\perp} \subseteq \mathcal{H}(n \times n, q; d)$ when $d \leq \delta$, it is enough to show that $\mathcal{H}(n \times n, q; \delta)^{\perp} \subseteq \mathcal{H}(n \times n, q; \delta)$ since $\mathcal{H}(n \times n, q; d)$ contains $\mathcal{H}(n \times n, q; \delta)$. From lemma 5, our goal is to prove that $\mathcal{Z}_{des} \cap \mathcal{Z}^{-1} = \phi$ for $\mathcal{H}(n \times n, q; \delta)$. Following is the designed set for a primitive narrow-sense bicyclic hyperbolic code of designed distance δ.

$$\mathcal{Z}_{des} = \{(x, y) \mid xy < \delta,\ 1 \leq x, y \leq n - 1\} \tag{3.23}$$

From equation (3.21) and equation (3.23), since Z is a union of q-ary cyclotomic cosets of elements in $\mathcal{Z}_{des}$, we can restate our goal as to prove the following inequality.

$$(-xq^l \bmod n)(-yq^l \bmod n) \geq \delta \qquad \forall\ (x, y) \in \mathcal{Z}_{des},\quad l \in \{0, 1, 2...m - 1\} \tag{3.24}$$

Let $(x, y) \in \mathcal{Z}_{des}$. If q-ary coefficients x_i of x are equal to zero for $i > k$ and $x_k \neq 0$ then q-ary coefficients y_j of y must be equal to zero for $j > m - 1 - k$. This follows from the condition that all the points in $\mathcal{Z}_{des}$ satisfy $xy < q^m - 1$. Therefore all the points in $\mathcal{Z}_{des}$

must be of the following form, for some $k \in \{0, 1, 2, ..., m-1\}$.

$$x = \sum_{i=0}^{k} x_i q^i, \ x_k \neq 0 \quad \text{and} \quad y = \sum_{j=0}^{m-1-k} y_j q^j \tag{3.25}$$

Based on this, let us partition the points in $\mathcal{Z}_{des}$ into disjoints sets $\mathcal{Z}_{des,0} \cup \mathcal{Z}_{des,1} ... \cup \mathcal{Z}_{des,m-1}$ as follows.

$$\mathcal{Z}_{des,k} = \left\{(x,y) \mid q^k - 1 < x \leq q^{k+1} - 1, (x,y) \in \mathcal{Z}\right\} \tag{3.26}$$

For every point (x, y) in $\mathcal{Z}_{des}$, (y, x) is also in $\mathcal{Z}_{des}$. Therefore, in trying to prove inequality (3.24) it is enough to restrict to points in $\mathcal{Z}_{des}$ where $x \leq y$. This implies, from equation (3.25) and (3.26), instead of considering all points in $\mathcal{Z}_{des}$, it is enough to consider just the following points

$$(x,y) \in \mathcal{Z}_{des,k}, \ \text{where } k \leq (m-1)/2 \tag{3.27}$$

- When m is even: Let us try to find a bound on the value of $(-xq^l \bmod n)(-yq^l \bmod n)$ for $(x, y) \in \mathcal{Z}_{des,k}$, $k \leq (m-1)/2$ and $l \in \{0, 1, ..., m-1\}$. Since $\delta < q^m - 1 - q^{\lfloor m/2 \rfloor}$, based on lemma 2, when can say that

$$\begin{aligned}\min_{\substack{(x,y)\in Z_{des}\\ 0\leq l\leq m-1}} (-xq^l \bmod n)(-yq^l \bmod n) &= \min\left\{q^m - 1 - q^{\lceil m/2 \rceil - 1}, (q^{m/2} - 1)^2\right\} \\ &= (q^{m/2} - 1)^2 = \delta \ (\text{when } m \text{ is even})\end{aligned} \tag{3.28}$$

- When m is odd: $\delta = q^m - 1 - q^{\lfloor m/2 \rfloor}$. Based on lemma 2, we can say that

$$\begin{aligned}\min_{\substack{(x,y)\in Z_{des}\\ 0\leq l\leq m-1}} (-xq^l \bmod n)(-yq^l \bmod n) &= q^m - 1 - q^{\lfloor m/2 \rfloor} \\ &= \delta \ (\text{when } m \text{ is odd})\end{aligned} \tag{3.29}$$

Seeking a contradiction let us assume that $\mathcal{H}(n \times n, q; d)^{\perp} \subset \mathcal{H}(n \times n, q; d)$ for some $d > \delta$.

- When m is even, consider the point $(x, y) = (\sqrt{\delta}, \sqrt{\delta})$. Since $\delta < d$, $(\sqrt{\delta}, \sqrt{\delta}) \in \mathcal{Z}_{des}$.

Now let us consider $\big((-xq^l \bmod n), (-yq^l \bmod n)\big) \in \mathcal{Z}^{-1}$ when $l = m/2$.

$$\begin{aligned}(-xq^l \bmod n)(-yq^l \bmod n) &= (n - \sqrt{\delta}q^{m/2})(n - \sqrt{\delta}q^{m/2}) \\ &= \Big(\frac{n}{q^{m/2}+1}\Big)\Big(\frac{n}{q^{m/2}+1}\Big) \\ &= (q^{m/2}-1)^2 = \delta < d \qquad (3.30)\end{aligned}$$

- When m is odd, consider the point $(x, y) = (\delta, 1)$. Since $\delta < d$, $(\delta, 1)$. Now let us consider $\big((-xq^l \bmod n), (-yq^l \bmod n)\big) \in \mathcal{Z}^{-1}$ when $l = \frac{m+1}{2}$.

$$\begin{aligned}-xq^l \bmod n &= -(q^m - 1 - q^{\frac{m-1}{2}})q^{\frac{m+1}{2}} \bmod (q^m - 1) \\ &= 1 \qquad (3.31a) \\ -yq^l \bmod n &= -q^{\frac{m+1}{2}} \bmod (q^m - 1) \\ &= (q^m - 1 - q^{\frac{m+1}{2}}) < \delta < d \qquad (3.31b)\end{aligned}$$

$(-xq^l \bmod n)(-yq^l \bmod n) < d$ implies $\big((-xq^l \bmod n), (-yq^l \bmod n)\big) \in \mathcal{Z}_{des}$. Therefore $\mathcal{Z}_{des} \cap \mathcal{Z}^{-1} \neq \phi$. This implies $\mathcal{H}(n \times n, q; d)$ cannot contain its Euclidean dual for $d > \delta$. □

The sufficiency result in the above theorem can be further generalized to the case of non-primitive bicyclic hyperbolic codes.

Theorem 7. *Suppose $m = ord_n(q)$. Narrow-sense bicyclic hyperbolic code of length $n \times n$ over $\mathbf{F}_{q^2}$ contains its Euclidean dual if the design distance d satisfies $2 \leq d \leq \Delta$, where*

$$\Delta = \begin{cases} \Big(\frac{n^2}{(q^m-1)^2}\Big)\Big[(q^m-1) - 2(q^{m/2}-1)\Big] & m \text{ is even} \\ \Big(\frac{n^2}{(q^m-1)^2}\Big)\Big[(q^m-1) - (q^{\frac{m-1}{2}})\Big] & m \text{ is odd} \end{cases} \qquad (3.32)$$

Proof: Similar to above theorem, it is enough to show that $\mathcal{H}(n \times n, q; \Delta)^{\perp} \subseteq \mathcal{H}(n \times n, q; \Delta)$. Let $\overline{\mathcal{Z}}$ be the defining set for narrow-sense bicyclic hyperbolic code. From lemma 5, our goal is to prove that

$$(-\overline{x}q^l \bmod n)(-\overline{y}q^l \bmod n) \geq \Delta \qquad \forall\ (\overline{x}, \overline{y}) \in \overline{\mathcal{Z}}_{des},\ l \in \{0, 1, ..., m-1\} \qquad (3.33)$$

Let $(\overline{x}, \overline{y}) \in \overline{\mathcal{Z}}_{des}$. Since $0 \leq \overline{x} < n$ and $0 \leq \overline{y} < n$, they can be written in the following form

$$\overline{x} = \frac{n}{q^m - 1}\left(\frac{q^m - 1}{n}(\overline{x})\right) = \frac{n}{q^m - 1}(x) \tag{3.34a}$$

$$\overline{y} = \frac{n}{q^m - 1}\left(\frac{q^m - 1}{n}(\overline{y})\right) = \frac{n}{q^m - 1}(y) \tag{3.34b}$$

where $0 \leq x < q^m - 1$, $0 \leq y < q^m - 1$. Correspondingly

$$(-\overline{x}q^l \bmod n) = \left(\frac{n}{q^m - 1}\right)(-xq^l \bmod (q^m - 1)) \tag{3.35a}$$

$$(-\overline{y}q^l \bmod n) = \left(\frac{n}{q^m - 1}\right)(-yq^l \bmod (q^m - 1)) \tag{3.35b}$$

From above equations, we can say that $\overline{xy} < \Delta$ implies $xy < \delta$, where δ is from theorem 6 and $(-xq^l \bmod (q^m-1))(yq^l \bmod (q^m-1)) \geq \delta$ implies $(-\overline{x}q^l \bmod n)(-\overline{y}q^l \bmod n) \geq \Delta$. Therefore from theorem 6, we can say that equation (3.33) is true. □

Now that we have conditions for Euclidean dual containing bicyclic codes, the CSS constructions allow us to construct quantum stabilizer codes.

Proposition 8 (Calderbank-Shor-Steane (CSS) construction, Calderbank *et al.* (1998))**.** *If there exists an $[n, k, d]$ dual containing classical linear code C over $\mathbb{F}_q$, then there exists an $[[n, 2k - n, d]]$ stabilizer code over $\mathbb{F}_q$.*

Corollary 9 (Quantum bicylic codes I)**.** *Let n be a postiove integer and q be a power of prime such that $gcd(n, q) = 1$ and $d < \delta$ as in Theorem 7. Then there exists a quantum bicyclic code of length n^2 and distance $\geq d$.*

3.3 Hermitian Dual Containing Code

Suppose C is a linear code of size $n \times n$ over $\mathbf{F}_{q^2}$. The Hermitian dual code $C^{\perp_h}$ of the linear code C is defined as $\left\{c' \in \mathbf{F}_{q^2}^{n\times n} \;\middle|\; c'^q.c = 0 \;\forall\; c \in C\right\}$. For a cyclic code this condition can be given in terms of defining set of the cyclic code. Suppose Z is the defining set of bicyclic code C of length $n \times n$ over the field $\mathbf{F}_q$ and $\gcd(n, q) = 1$ then the defining set of $C^{\perp_h}$ is $Z_{tot} - Z^{-q}$, where $Z^{-q} = \{(-xq, -yq) \bmod n \mid (x, y) \in Z\}$. In this context, the following theorem gives a easy condition to verify if a bicyclic code contains its Hermitian dual code.

Lemma 10. *Suppose C be the bicyclic code of length $n \times n$ over $\mathbf{F}_q$ and $gcd(n, q) = 1$. Let Z be the defining set of C. Then the code C contains its Hermitian dual if and only if*

$$Z_{des} \cap Z^{-q} = \phi \tag{3.36}$$

where $Z^{-q} = \{(-qx, -qy) \ mod \, n \mid (x, y) \in Z\}$.

Proof: Let $C^{\perp_h}$ be the Hermitian dual code of C. If Z is the defining set of C then the defining set of $C^{\perp_h}$ is $Z_{total} - Z^{-q}$. $C^{\perp_h}$ is contained in C if and only if the defining set of C is contained in defining set of $C^{\perp_h}$.

$$Z \subset Z_{tot} - Z^{-q} \implies Z \cap Z^{-1} = \phi \tag{3.37}$$

$Z \cap Z^{-q} = \phi$ is true if and only if there is no common coset between Z and Z^{-q}. Since every coset in Z contains at least one element from Z_{des}, $Z \cap Z^{-q} = \phi$ is true if and only if $Z_{des} \cap Z^{-q} = \phi$. □

Similar to the Euclidean case, following theorem gives a easy condition based on the designed distance to verify if a primitive narrow-sense bicyclic hyperbolic code contains its Hermitian dual.

Theorem 11. *Primitive narrow-sense bicyclic hyperbolic code of length $n \times n$ over $\mathbf{F}_{q^2}$, where $n = q^{2m} - 1$, contains its Hermitian dual if the design distance d satisfies $2 \leq d \leq \delta_h$, where*

$$\delta_h = \begin{cases} (q^m - 1)^2 & m \text{ is odd} \\ q^{2m} - 1 - q^{m-1} & m \text{ is even} \end{cases}$$

Proof: The outline of the proof is very much similar to that of Euclidean dual case. Few differences include

- Range of x and y will be from 0 to $q^{2m} - 1$ and therefore there will be $2m$ q-ary coefficients for x and y compared to m q-ary coefficients in Euclidean case.

- Since the code is over field $\mathbf{F}_{q^2}$, we need to consider q^2-ary cyclotomic coset instead of q-ary cyclotomic coset. q^2-ary cyclotomic coset of (x, y) is

$$\left\{(xq^l, yq^l) \mid l \in \{2, 4...2m\}\right\}$$

For proving $\mathcal{H}(n \times n, q; d)^{\perp_h} \subseteq \mathcal{H}(n \times n, q; d)$ when $d \leq \delta_h$, it enough to show that $\mathcal{H}(n \times n, q; \delta_h)^{\perp_h} \subseteq \mathcal{H}(n \times n, q; \delta_h)$ since $\mathcal{H}(n \times n, q; d)$ contains $\mathcal{H}(n \times n, q; \delta_h)$. Therefore our goal is to show that

$$(-xq^l \bmod n)(-yq^l \bmod n) \geq \delta_h \quad \forall\ (x, y) \in Z_{des}, \quad l \in \{1, 3, 5...2m-1\} \tag{3.38}$$

The domain of l is $\{1, 3, 5...2m-1\}$ instead of $\{0, 2, 4...2m-2\}$ because there is an additional q multiplied in Hermitian dual case. Similar to the Euclidean case, we will divide the points in Z_{des} into disjoint sets $Z_{des,0} \cup Z_{des,1} \cup ... \cup Z_{des,2m-1}$. Since for every (x, y) in Z_{des}, (y, x) is also in Z_{des}. This implies it is enough to just consider the following points instead of Z_{des}.

$$(x, y) \in Z_{des,k}, \text{ where } k \leq (2m-1)/2 \tag{3.39}$$

1. When $\boldsymbol{m}$ is even: From lemma 2, When $l < 2m - k - 1$, minimum value of $(-xq^l \bmod n)(-yq^l \bmod n)$ occurs when $l = m - 1$ and is equal to $q^{2m} - 1 - q^{m-1}$. When $2m - k - 1 \leq l$, $(-xq^l \bmod n)(-yq^l \bmod n)$ is less than $q^{2m} - 1$ only for $l = m$. But l is restricted only odd numbers. Therefore minimum value of $(-xq^l \bmod n)(-yq^l \bmod n)$ is equal to $q^{2m} - 1 - q^{m-1}$ for $(x, y) \in Z_{des}$ and $l \in \{1, 3, 5...2m-1\}$.

$$\begin{aligned} \min_{\substack{(x,y)\in Z_{des} \\ l\in\{1,3..2m-1\}}} (-xq^l \bmod n)(-yq^l \bmod n) &= q^{2m} - 1 - q^{m-1} \\ &= \delta_h \end{aligned} \tag{3.40}$$

2. When $\boldsymbol{m}$ is odd: From lemma 2, as $2m$ is even, we can say that

$$\min_{\substack{(x,y)\in Z_{des}\\ l\in\{1,3..2m-1\}}} (-xq^l \bmod n)(-yq^l \bmod n) = \min\left\{q^{2m}-1-q^{m-1},(q^m-1)^2\right\}$$
$$= (q^m-1)^2 = \delta_h \tag{3.41}$$

Since we already proved that $\mathcal{H}(n\times n,q;\delta_h)^{\perp_h} \subset \mathcal{H}(n\times n,q;\delta_h)$, seeking a contradiction lets assume that $\mathcal{H}(n\times n,q;d)^{\perp_h} \subset \mathcal{H}(n\times n,q;d)$ for some $d>\delta_h$.

1. When m is odd, consider the point $(x,y)=(\sqrt{\delta_h},\sqrt{\delta_h})$. Since $\delta_h<d$, $(\sqrt{\delta_h},\sqrt{\delta_h})\in Z_{des}$. When $l=m-1$

$$\begin{aligned}(n-qx^{(l)})(n-qy^{(l)}) &= (n-\sqrt{\delta_h}q^m)(n-\sqrt{\delta_h}q^m)\\ &= (q^m-1)^2\\ &= \delta_h < d\end{aligned}$$

2. When m is odd, consider the point $(x,y)=(\delta_h,1)$. when $l=m$

$$\begin{aligned}-qx^{(l)} \bmod n &= -(q^{2m}-1-q^{m-1})q^{m+1} \bmod (q^{2m}-1)\\ &= 1\\ -y^{(l)} \bmod n &= -q^{m+1} \bmod (q^m-1)\\ &= (q^{2m}-1-q^{m+1}) < \delta_h < d\end{aligned}$$

Based on equations and , we can say that $Z_{des}\cap Z^{-1}\neq\phi$ when $d>\delta_h$. This implies $\mathcal{H}(n\times n,q;d)$ cannot contain its Hermitian dual when $d>\delta_h$.

□

The sufficiency result in the above theorem can be further generalized to the case of non-primitive bicyclic hyperbolic codes.

Theorem 12. *Suppose $m=ord_n(q)$. Narrow-sense bicyclic hyperbolic code of length $n\times n$ over $\mathbf{F}_{q^2}$ contains its Hermitian dual if the design distance d satisfies $2\le d\le\Delta_h$,* *where*

$$\Delta_h = \begin{cases} \left(\frac{n^2}{(q^m-1)^2}\right)(q^m-1)^2 & m \textit{ is even} \\ \\ \left(\frac{n^2}{(q^m-1)^2}\right)(q^{2m}-1-q^{m-1}) & m \textit{ is odd} \end{cases} \tag{3.43}$$

The proof for this theorem involves exactly the same arguments as the proof of theorem 7 in the euclidean dual containing case.

Equipped with conditions on Hermitian dual containing bicyclic codes, Hermitian constructions allows us to construct quantum stabilizer codes.

Proposition 13 (Hermitian construction Calderbank *et al.* (1998); Ashikhmin and Knill (2001))**.** *Let C be an $[n, k, d]$ over $\mathbb{F}_{q^2}$ such that $C^{\perp_h} \subseteq C$, then there exists an $[[n, 2k - n, d]]$ stabilizer code over $\mathbb{F}_q$.*

Corollary 14 (Quantum bicyclic codes II)**.** *Let q be a prime power, $n = q^{2m} - 1$ for $m > 3$ and $d < \delta$ as in Theorem 6. Then there exist bicyclic quantum codes of length n^2 and distance $\geq d$.*

CHAPTER 4

Conclusion

In this thesis, we gave brief review of bicyclic codes, bicyclic hyperbolic codes and their corresponding characterization using common zeros or defining sets. We proved some results on the structure of cyclotomic cosets which the constitute the defining set. Using these results we were able to give a easy condition for when a primitive bicyclic hyperbolic code contains its Euclidean dual code. We also gave an easy condition for when a primitive bicyclic hyperbolic code contains its Hermitian dual code. Using these results we were able to construct quantum bicyclic codes.

There are other interesting structural properties of bicyclic codes worth further investigation. The number theoretic techniques that are used in this thesis to analyze the structure of cosets in two dimensions can be generalized to higher dimensions and therefore can be used to study the structure of cyclotomic cosets in higher dimensions. One natural direction would be to compute the dimension and distance of these codes. Another possibility would be to study non-narrow sense variants of bicyclic hyperbolic codes. Quasi-cyclic codes are a generalization of cyclic codes which has been of lot interest recently in quantum error correction. It would interesting see if the results in this thesis can be extended to quasi cyclic codes as well. The theory of bicyclic codes is very rich and we hope this work will motivate further research in quantum bicyclic codes.

REFERENCES

1. **Aly, S. A.**, **A. Klappenecker**, and **P. K. Sarvepalli** (2007). On quantum and classical BCH codes. *IEEE Transactions on Information Theory*, **53**(3), 1183–1188.

2. **Ashikhmin, A.** and **E. Knill** (2001). Nonbinary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, **47**(7), 3065–3072.

3. **Blahut, R. E.**, *Algebraic Codes on Lines, Planes and Curves*. University Press, Cambridge, 2008.

4. **Bose, R.** and **D. Ray-Chaudhuri** (1960*a*). Further results on error correcting binary group codes. *Information and Control*, **3**(3), 279 – 290.

5. **Bose, R.** and **D. Ray-Chaudhuri** (1960*b*). On a class of error correcting binary group codes. *Information and Control*, **3**(1), 68 – 79.

6. **Calderbank, A. R.**, **E. M. Rains**, **P. M. Shor**, and **N. J. A. Sloane** (1998). Quantum error correction via codes over GF(4). *IEEE Trans. on Inform. Theory*, **44**(4), 1369–1387. ISSN 0018-9448.

7. **Calderbank, A. R.** and **P. W. Shor** (1996). Good quantum error-correcting codes exist. *Phys. Rev. A*, **54**, 1098–1105.

8. **Grassl, M.**, **T. Beth**, and **T. Pellizzari** (1997). Codes for the quantum erasure channel. *Phys. Rev. A*, **56**, 33–38. URL https://link.aps.org/doi/10.1103/PhysRevA.56.33.

9. **Grassl, M.**, **T. Beth**, and **M. Rötteler** (2004). On optimal quantum codes. *Internat. J. Quantum Information*, **2**(1), 757–775.

10. **Hocquenghem, A.** (1959). Codes Correcteurs d'Erreurs. *Chiffres (Paris)*, **2**, 147–156.

11. **Imai, H.** (1977). A theory of two-dimensional cyclic codes. *Information and Control*, **34**(1), 1 – 21.

12. **Ketkar, A.**, **A. Klappenecker**, **S. Kumar**, and **P. K. Sarvepalli** (2006). Nonbinary stabilizer codes over finite fields. *IEEE Transactions on Information Theory*, **52**(11), 4892–4914.

13. **Nielsen, M. A.** and **I. L. Chuang**, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 2011, 10th edition. ISBN 1107002176, 9781107002173.

14. **Steane, A. M.** (1996). Error correcting codes in quantum theory. *Phys. Rev. Lett.*, **77**, 793–797.

15. **Steane, A. M.** (1999). Enlargement of Calderbank-Shor-Steane quantum codes. *IEEE Transactions on Information Theory*, **45**(7), 2492–2495.