8-2010

Quantum codes from two-point Hermitian codes

Justine Hyde-volpe
Clemson University, jchasma@clemson.edu

Quantum Codes from Two-point Hermitian Codes

A Thesis
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
Mathematical Sciences

---

by
Justine C. Hyde-Volpe
August 2010

Accepted by:
Dr. Gretchen Matthews, Committee Chair
Dr. Shuhong Gao
Dr. Matthew Macauley

Acknowledgments

I would like to acknowledge the dedication and guidance of Dr. Gretchen Matthews. Without her help, this Master's thesis would not have been possible.

Abstract

We provide background on error-correcting codes, including linear codes and quantum codes from curves. Then, we consider the parameters of quantum codes constructed from two-point Hermitian codes.

Table of Contents

Chapter 1

Introduction

Quantum error-correcting codes serve to protect quantum information from noise and are essential for quantum computation. The first such code was discovered in 1995 by Peter Shor, prompting researchers to seek quantum codes that are efficient and correct many errors [16]. One year later, Shor and Calderbank discovered the first family of quantum error-correcting codes [3]. Then, in 1998, it was shown how to construct quantum codes from binary linear codes [2]. This was extended to codes from larger alphabets in 2001 by Rains [15] and Ashikhmin and Knill [1] who studied non-binary quantum codes. This thesis studies quantum error-correcting codes constructed using algebraic geometry. In particular, we obtain estimates for the parameters of a large class of non-binary quantum codes. The codes are obtained from two-point codes on the Hermitian curve, and the parameters provide measures of the efficiency and error-correcting capabilities of the codes. Quantum codes from one-pont Hermitian codes have been studied in [10]. Up to this point, most quantum codes have been designed for binary alphabets, meaning alphabets with two symbols. The codes considered here enable quantum error-correction for larger alphabets.

This thesis is organized as follows. In Chapter 2 we provide background on error-correcting codes, including linear codes and quantum codes from curves. In Chapter 3,

we consider the parameters of quantum codes constructed from two-point Hermitian codes. This thesis concludes with Chapter 4, a discussion of future work on quantum codes from Hermitian curves.

Chapter 2

Preliminaries

2.1 Introduction to error-correcting codes

A qubit, short for quantum bit, is a quantum analog of a bit, the classical unit of information, and can be expressed as a complex linear combination of 0 and 1. Specifically while a qubit may be represented by a vector in $\mathbb{C}^2$, it is typically written as

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

where $\alpha, \beta \in \mathbb{C}$ and $\mathbb{C}$ denotes the complex numbers. It is often assumed that $|\alpha|^2 + |\beta|^2 = 1$. This idea can be generalized to larger alphabets, such as $\mathbb{F}_q$, the finite field with q elements where q is a power of a prime number. This leads to the notion of a qudit, or quantum digit. Here, a qudit is considered the unit of information and can be viewed as

$$\textstyle\sum_{a \in \mathbb{F}_q} \alpha_a \mid a\rangle$$

where $\alpha_a \in \mathbb{C}$. While a classical q-ary linear code of length n is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$, a length n q-ary quantum code is a complex subspace of

$$(\mathbb{C}^q)^{\otimes n} := \underbrace{\mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q}_{n} \cong \mathbb{C}^{q^n}.$$

Definition 1. The dimension k of a linear code C is defined to be the dimension of C as a vector space over $\mathbb{F}$.

Definition 2. Given a linear code C of length n and codewords $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in C$, the Hamming distance between x and y is

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

The minimum distance of C is

$$d := \min\{d(c, c') : c, c' \in C, c \neq c'\}.$$

Classical linear codes over $\mathbb{F}_q$ of length n, dimension k, and minimum distance d are called $[n, k, d]$ or $[n, k, d]_q$ codes. Next, we define the parameters of a quantum code.

Definition 3. A q-ary quantum code C of length n is said to be of dimension k provided C is a q^k-dimension subspace of $\mathbb{C}^{q^n}$.

To define the minimum distance of a quantum code, we need the additional concepts described below, taken from [1, 10, 11]. Let $\mathbb{F}^{m\times n}$ denote the set of $m \times n$ matrices over a field $\mathbb{F}$. Given $A \in \mathbb{F}^{m\times n}$, A_{ij} or $[A]_{i,j}$ denotes the entry of A in the i-th row and j-th column. We would like to describe the types of errors possible for a q-ary n-qudit case and when these errors are correctable. Let $p = char\mathbb{F}_q$ be the characteristic of the field $\mathbb{F}_q$. Fix a basis $\{\gamma_1, ..., \gamma_m\}$ for $\mathbb{F}_q$ as an $\mathbb{F}_p$-vector space. Let $\xi = e^{\frac{2\pi i}{p}}$ be a p-th root of unity. Consider matrices T and R with entries given by

$$[T]_{i,j} = \delta_{i,j-1 \ mod \ p}$$

and

$$[R]_{i,j} = \xi^i \delta_{i,j}$$

with

$$\delta_{i,j} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{otherwise;} \end{cases}$$

that is,

$$T = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}, \; R = \begin{bmatrix} \xi & 0 & \cdots & 0 & 0 \\ 0 & \xi^2 & 0 & \cdots & 0 \\ 0 & 0 & \xi^3 & \ddots & 0 \\ 0 & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & \xi^{p-1} \end{bmatrix} \in \mathbb{C}^{p \times p}.$$

Given $a, b \in \mathbb{F}_q$, there exist $a_1, ..., a_m, b_1, ..., b_m \in \mathbb{F}_p$ such that

$$a = \textstyle\sum_{i=1}^{m} a_i \gamma_i$$

and

$$b = \textstyle\sum_{i=1}^{m} b_i \gamma_i.$$

Let

$$T_a := T^{a_1} \otimes T^{a_2} \otimes \cdots \otimes T^{a_m}$$

and

$$R_b := R^{b_1} \otimes R^{b_2} \otimes \cdots \otimes R^{b_m}.$$

Given, $a, b \in \mathbb{F}_q^n$, we can consider errors on an n state system. Let $E_{a,b} := T_a R_b$. Then $E_{a,b} = T_{a_1} R_{b_1} \otimes \cdots T_{a_n} R_{b_n}$. The error group is

$$G_n := \{\xi^i E_{a,b} : a, b \in \mathbb{F}_q^n, 0 \leq i \leq q-1\}.$$

Definition 4. The weight of an error $\xi^i E_{a,b} \in G_n$ is

$$\mathrm{wt}(\xi^i E_{a,b}) := n - |\{i : a_i = b_i = 0\}|.$$

The quantum shorthand for bra-ket notation is

$$\langle u \mid v \rangle = \sum_{i=1}^{n} u_i^* v_i$$

where $\langle u \mid = (u_1^*, ..., u_n^*)$, $\mid v \rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$, and u_i^* denotes the complex conjugate of u_i. Similarly,

$$\langle u \mid A \mid v \rangle = \sum_i \sum_j u_i^* A_{ij} v_j$$

which can be written in matrix notation as

$$\begin{pmatrix} u_1^* & u_2^* & \cdots & u_n^* \end{pmatrix} \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}.$$

Definition 5. The minimum distance of a length n q-ary quantum code C is defined as

$$d = \max \left\{ d : \begin{array}{r} \langle u \mid v \rangle = 0 \text{ and } \mathrm{wt}(E) \leq d-1 \Rightarrow \langle u \mid E \mid v \rangle = 0 \\ \forall \mid u \rangle, \mid v \rangle \in C \text{ and } \forall E \in G_n \end{array} \right\}.$$

A q-ary quantum code of length n, dimension k, and minimum distance d is called an $[[n, k, d]]_q$ code or an $[[n, k, d]]$ code. We use the notation $[n, k]$ (resp., $[[n, k]]_q$) to describe a linear (resp., quantum) code of length n and dimension k. At times, we only have a lower bound on the minimum distance of a code. Hence, it is convenient to use the notation $[n, k, \geq t]$ or $[[n, k, \geq t]]$ to mean a code of length n, dimension k, and minimum distance at least t. A linear or quantum code of minimum distance d can correct any $\lfloor \frac{d-1}{2} \rfloor$ errors. These parameters will be discussed in detail later.

Suppose C is a $[n, k]$ code over $\mathbb{F}_q$. Then, the dual of C is

$$C^{\perp} := \{v \in \mathbb{F}_q^n : c \cdot v = 0, \ \forall c \in C\},$$

where $c \cdot v := c^T v$ denotes the usual dot product of vectors. Then, $C^\perp$ is an $[n, n-k]$ code over $\mathbb{F}_q$. If $C \subseteq C^\perp$, then C is said to be self-orthogonal or weakly self-dual. If $C = C^\perp$, then C is called self-dual.

2.2 Codes from curves

In this section, we describe both classical and quantum codes constructed from curves over finite fields. For more details, the reader may consult [11] or [21].

2.2.1 Linear codes from curves

In this subsection, we consider linear codes defined from curves over finite fields. This construction is due to Goppa [4]. Many of the definitions are taken from [21].

Given a field $\mathbb{F}$ and a positive integer n, n-dimensional projective space over $\mathbb{F}$ is

$$\mathbb{P}^n_{\mathbb{F}} := \{(a_1 : a_2 : \cdots : a_{n+1}) : (a_1, a_2, \ldots, a_{n+1}) \in \mathbb{F}^{n+1} \setminus \{(0, 0, \ldots, 0)\}\}$$

where $(a_1 : a_2 : \cdots : a_{n+1})$ is the equivalence class of $(a_1, a_2, \ldots, a_{n+1})$ with respect to the relation $\sim$ defined by

$$(a_1, \ldots, a_{n+1}) \sim (b_1, \ldots, b_{n+1})$$

if and only if there exists $\lambda \in \mathbb{F} \setminus \{0\}$ with $a_i = \lambda b_i$ for all $1 \leq i \leq n+1$. Hence, given $a_1, a_2, \ldots, a_{n+1} \in \mathbb{F}$ not all zero,

$$(a_1 : a_2 : \cdots : a_{n+1}) := \{\lambda(a_1, a_2, \ldots, a_{n+1}) : \lambda \in \mathbb{F} \setminus \{0\}\}.$$

We say that the points of $\mathbb{P}^n_{\mathbb{F}}$ are the equivalence classes $(a_1 : \cdots : a_{n+1})$, where $a_i \in \mathbb{F}$ and $a_i \neq 0$ for at least one i, $1 \leq i \leq n+1$. In this paper we consider curves in the projective plane, $\mathbb{P}^2_{\mathbb{F}}$. The next example discusses points in the projective plane.

Example 1. In this example, we consider the points of the projective plane $\mathbb{P}^2_{\mathbb{F}}$. Suppose $a, b, c \in \mathbb{F}$ so that at least one of a, b, c is nonzero. Then $(a : b : c) \in \mathbb{P}^2_{\mathbb{F}}$, meaning $(a : b : c)$ is a point in the projective plane over $\mathbb{F}$. If $c \neq 0$, then

$$\begin{aligned}(a : b : c) &= (c^{-1}a : c^{-1}b : c^{-1}c) \\ &= (c^{-1}a : c^{-1}b : 1).\end{aligned}$$

Suppose $c = 0$. Then we have $(a : b : c) = (a : b : 0)$. If $b \neq 0$,

$$\begin{aligned}(a : b : 0) &= (b^{-1}a : b^{-1}b : 0) \\ &= (b^{-1}a : 1 : 0).\end{aligned}$$

If $b = 0$, then $(a : 0 : 0) = (1 : 0 : 0)$. Thus,

$$\mathbb{P}^2_{\mathbb{F}} = \{(a : b : 1) : a, b \in \mathbb{F}\} \cup \{(a : 1 : 0) : a \in \mathbb{F}\} \cup \{(1 : 0 : 0)\}.$$

The points written as $(a : b : 1)$ are considered affine points while $(a : 1 : 0)$ and $(1 : 0 : 0)$ are called points at infinity.

Definition 6. Let $F(x, y, z) \in \mathbb{F}[x, y, z]$ be a homogeneous polynomial. The projective curve X defined by F is

$$X := \{(x : y : z) \in \mathbb{P}^2_{\bar{\mathbb{F}}} : F(x, y, z) = 0\} \subseteq \mathbb{P}^2_{\bar{\mathbb{F}}},$$

where $\bar{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$.

Remark 1. Given the curve X as in Definition 6, $(x : y : z) \in X$ with $x, y, z \in \mathbb{F}$ is called an $\mathbb{F}$-rational point. All curves considered in this thesis are plane curves, meaning they are of the form given in Definition 6. . Hence, we say X is a curve to mean X is a plane curve. Also, we often say a polynomial $f(x, y) \in \mathbb{F}[x, y]$ defines a curve X to mean that X is the curve defined by the homogenization of $f(x, y)$.

The divisor group $\operatorname{Div} X$ on a curve X over $\mathbb{F}$ is

$$\operatorname{Div} X := \{\textstyle\sum_{i=1}^{n} a_i P_i : n \in \mathbb{Z}^+,\ a_i \in \mathbb{Z},\ P_i \text{ is a point on X}\}$$

where $\mathbb{Z}$ is the set of integers and $\mathbb{Z}^+$ is the set of positive integers. Hence, $\operatorname{Div} X$ is the free abelian group on points of X. The elements of $\operatorname{Div} X$ are called divisors. The support of a divisor $\sum_{i=1}^{n} a_i P_i$ is the set of points P_i with $a_i \neq 0$, denoted $suppD$. The degree of a divisor $D = \sum_{i=1}^{n} a_i P_i$ whose support consists only of points P_i in $\mathbb{P}^2_{\mathbb{F}}$ is

$$\deg D = \textstyle\sum_{i=1}^{n} a_i.$$

There is a partial order $\leq$ on $\operatorname{Div} X$ given by

$$\textstyle\sum_{i=1}^{n} a_i P_i \leq \sum_{i=1}^{n} a_i' P_i$$

if and only if $a_i \leq a_i'$ for all $i, 1 \leq i \leq n$.

A point P is a singular point on a curve X if and only if P is a point on X and

$$(\partial x F)(P) = (\partial y F)(P) = (\partial z F)(P) = 0.$$

If a curve X has at least one singular point, then it is called singular. Otherwise, the curve is nonsingular. The genus of a nonsingular curve with defining polynomial $F(x, y)$ of degree d is

$$g = \frac{(d-1)(d-2)}{2}.$$

We now check to see if the Hermitian curve is nonsingular and determine its genus.

Example 2. Consider the Hermitian curve X defined by $f(x, y) := y^q + y - x^{q+1}$ over $\mathbb{F}_{q^2}$. Here X is defined by the homogeneous polynomial $F(x, y, z) = y^q z + y z^q - x^{q+1}$. Note that the degree of F is $d = q + 1$. Now taking the partial derivatives with respect to x, y, and z

gives

$$\partial xF = -(q+1)x^q,$$
$$\partial yF = qzy^{q-1} + z^q,$$

and

$$\partial zF = y^q + qyz^{q-1}.$$

Considering the affine point $P_{ab} = (a : b : 1)$ gives

$$(\partial xF)(P_{ab}) = -(q+1)a^q,$$
$$(\partial yF)(P_{ab}) = qb^{q-1} + 1 = 1,$$

and

$$(\partial zF)(P_{ab}) = b^q + qb.$$

Thus, there is no affine point P with $(\partial yF)(P) = 0$. Hence, no affine point P is a singular point on X.

Considering the point at infinity $P_\infty := (0 : 1 : 0)$ yields

$$(\partial xF)(P_\infty) = -(q+1) \cdot 0^q = 0,$$
$$(\partial yF)(P_\infty) = q \cdot 0 \cdot 1^{q-1} + 0^q = 0,$$

and

$$(\partial zF)(P_\infty) = 1^q + q \cdot 1 \cdot 0^{q-1} = 1,$$

indicating that $P_\infty = (0 : 1 : 0)$ is not a singular point on X. Thus, X is nonsingular. As a result, the genus of X is $g = \frac{q(q-1)}{2}$.

Now, we consider functions on a curve X and how they are defined.

Definition 7. Let $F(X, Y, Z) \in \mathbb{F}[X, Y, Z]$ be a homogeneous polynomial which defines a nonsingular projective plane curve X over a field $\mathbb{F}$. The field of rational functions on X is

$$\mathbb{F}(X) = \left(\left\{ \frac{f(X,Y,Z)}{g(X,Y,Z)} : \begin{array}{l} f, g \in \mathbb{F}(X, Y, Z), \deg\ f = \deg\ g, \\ f, g \text{ homogeneous, and } g \neq 0 \end{array} \right\} \cup \{0\} \right) / \sim$$

where

$$\frac{f}{g} \sim \frac{f'}{g'}$$

if and only if

$$fg' - f'g \in \langle F \rangle \subseteq \mathbb{F}[X, Y, Z]$$

meaning $fg' - f'g$ is in the ideal generated by F.

Given $f \in \mathbb{F}(X) \setminus \{0\}$, we denote the divisor of f by (f). Given a point P on X, $v_P(f)$ is the coefficient of P in (f). Given a divisor A, $\mathcal{L}(A)$ denotes the set of rational functions f on X over $\mathbb{F}$ with divisor $(f) \geq -A$, together with the zero function, that is

$$\mathcal{L}(A) = \{f \in \mathbb{F}(X) : (f) \geq -A\} \cup \{0\}.$$

It can be shown that $\mathcal{L}(A)$ is a vector space over $\mathbb{F}$ and that $\dim_{\mathbb{F}} \mathcal{L}(A)$ is finite. Let

$$\ell(A) := \dim_{\mathbb{F}} \mathcal{L}(A).$$

A divisor $K \in \operatorname{Div} X$ is said to be canonical if and only if $\deg K = 2g-2$ and $\ell(K) = g$.

Given divisors $D = \sum_{i=1}^{n} Q_i$ and $G = \sum_{i=1}^{r} \alpha_i P_i$ on a curve X over a field $\mathbb{F}$ of genus g where

$$\{Q_1, \ldots, Q_n\} \cap \{P_1, \ldots, P_r\} = \emptyset$$

and the support of the D consists of n distinct $\mathbb{F}$-rational points on X, we can construct an algebraic geometry code $C_{\mathcal{L}}(D, G)$ by setting

$$C_{\mathcal{L}}(D, G) := \{(f(Q_1), \cdots, f(Q_n)) : f \in \mathcal{L}(G)\} \subseteq \mathbb{F}^n.$$

Clearly, $C_{\mathcal{L}}(D, G)$ is a code of length n. If $\deg G < n$, then $C_{\mathcal{L}}(D, G)$ has dimension $k = \ell(G)$ and minimum distance $d \geq n - \deg G$. Hence, $C_{\mathcal{L}}(D, G)$ is an $[n, \ell(G), \geq n - \deg G]$ code. If $A \leq B$ and $\operatorname{supp} B \cap \operatorname{supp} D = \emptyset$ where $D = P_1 + \cdots + P_n$, then $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ and $C_{\mathcal{L}}(D, A) \subseteq C_{\mathcal{L}}(D, B)$.

The dual of $C_{\mathcal{L}}(D, G) \subseteq \mathbb{F}^n$,

$$C_{\Omega}(D, G) := C_{\mathcal{L}}(D, G)^{\perp},$$

is also called an algebraic geometry code. The length of $C_{\Omega}(D, G)$ is n. If $2g-2 < \deg G < n$, then $C_{\Omega}(D, G)$ has dimension $k = \ell(K+D-G)$, where K is a canonical divisor, and minimum distance $d \geq \deg G - (2g-2)$. If $A \leq B$, then $C_{\Omega}(D, B) \subseteq C_{\Omega}(D, A)$ provided D is the sum of distinct rational points, none of which are in the supports of A and B . We call $C_{\mathcal{L}}(D, G)$ and $C_{\Omega}(D, G)$ r-point codes, given that G has support consisting of r distinct $\mathbb{F}$-rational points. As convention directs, we will construct r-point codes by letting D be the sum of all $\mathbb{F}$-rational points not in the support of G. A one-point code has the form $C_{\mathcal{L}}(D, G)$ or $C_{\Omega}(D, G)$ with $D = \sum_{i=1}^{n} P_i$ and $G = mQ$ such that G and D have disjoint support (see [10]). Likewise, a two-point code is of the form $C_{\mathcal{L}}(D, G)$ or $C_{\Omega}(D, G)$ with $D = \sum_{i=1}^{n} P_i$ and $G = m_1 Q + m_2 Q$ such that G and D have disjoint support.

2.2.2 Quantum codes from curves

In [2] it was shown how quantum codes can be constructed from classical binary codes. This construction is known as the CSS construction in honor of Calderbank, Shor, and Steane (see [2, 3, 16, 17]). The CSS construction was generalized to q-ary codes where $q > 2$ by Ashikmin and Knill [1]. In [9], the authors apply this to algebraic geometry codes and obtain quantum codes from curves as described in Theorem 1 below. To describe this result, we need the notion of minimum weight.

Given codes C, C' such that $C' \subseteq C$, let

$$d(C \setminus C') = \min\{\mathrm{wt}(c) : c \in C \setminus C'\}$$

where $\mathrm{wt}(c) =\mid \{c_i \neq 0\} \mid$ is the weight of $c \in C$.

Theorem 1. *Let A, B, and $D = P_1 + \cdots + P_n$ be divisors on a smooth, projective, absolutely irreducible curve X of genus g over $\mathbb{F}_q$ where the support of D consists of distinct $\mathbb{F}$-rational points. Assume that $A \leq B$ and $(\operatorname{supp} A \cup \operatorname{supp} B) \cap \operatorname{supp} D = \emptyset$ and $\deg B < n$. Then there exists an $[[n, \ell(B) - \ell(A), d]]_q$ code where*

$$\begin{aligned} d &\geq \min\{d(C_{\mathcal{L}}(D, B) \setminus C_{\mathcal{L}}(D, A)), d(C_\Omega(D, A) \setminus C_\Omega(D, B))\} \\ &\geq \min\{d(C_{\mathcal{L}}(D, B)), d(C_\Omega(D, A))\} \\ &\geq \min\{n - \deg B, \deg A - (2g - 2)\}. \end{aligned}$$

We apply Theorem 1 to Hermitian codes, taking A and B to be divisors supported by exactly two points. Our approach is described in Chapter 3. To prepare for this, we review the Hermitian curve in the next section.

2.3 Hermitian curve

In Chapter 3, we take X to be the Hermitian curve over $\mathbb{F}_{q^2}$ and A and B to be divisors supported by two points. To better understand the resulting codes, both linear and quantum, we next provide details on the Hermitian curve.

Recall that the Hermitian curve is defined over $\mathbb{F}_{q^2}$ by

$$y^q + y = x^{q+1}.$$

Then $X := \{(a : b : c) \in \mathbb{P}^2_{\mathbb{F}_{q^2}} : b^q + bc^q = a^{q+1}\} \subset \mathbb{P}^2_{F_{q^2}}$. Over $\mathbb{F}_{q^2}$, the affine points on the Hermitian curve are of the form

$$P_{ab} := \{(a : b : 1) : b^q + b = a^{q+1}\},$$

while there is a single point at infinity,

$$P_\infty := \{(0 : 1 : 0)\}.$$

Now, we consider functions on the Hermitian curve and how they are defined.

Example 3. Consider the Hermitian curve X over $\mathbb{F}_{q^2}$. Then

$$\frac{y^q z + y z^q}{z^{q+1}}, \frac{x^{q+1}}{z^{q+1}} \in \mathbb{F}_{q^2}(X) \tag{2.1}$$

In fact,

$$\frac{y^q z + y z^q}{z^{q+1}} = \frac{x^{q+1}}{z^{q+1}}$$

since $z^{q+1}(y^q z + y z^q - x^{q+1})$ is a multiple of the defining equation $F(x, y, z) = y^q z + y z^q - x^{q+1}$.

Chapter 3

Quantum two-point Hermitian codes

3.1 Review of CSS construction

To review the CSS construction, we need the additional concepts described below, taken from [1, 2, 3, 15]. We will use [1, 9, 15] to extend to nonbinary quantum error-correcting codes. The following theorem gives a construction of a q-ary quantum code from any two $\mathbb{F}_q$-linear codes $C_1 \subseteq C_2 \subseteq F_q^n$. First, we will present a proposition that will be used to give this construction. Let $x, y \in \mathbb{F}_{q^2}^n$ and consider the $\mathbb{F}_q$-bilinear map $x \circ y := \sum(x_i y_i^q - x_i^q y_i)$. For any $\gamma_0 \in \mathbb{F}_q$, there exists $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $\gamma^q = \gamma_0 - \gamma$.

Proposition 2. *[9] Let $C_1 \subseteq C_2 \subseteq \mathbb{F}_q^n$ be $\mathbb{F}_q$-linear codes, so that $C_2^\perp \subseteq C_1^\perp$, where $C_i^\perp$ is the dual of C_i under the usual inner product. Let ω be the primitive element of $\mathbb{F}_{q^2}$ and write $\bar{\omega} = \omega^q$. Set $D = \omega C_1 + \bar{\omega} C_2^\perp \subseteq \mathbb{F}_{q^2}^n$. Then the dual of D is given by $D^{\perp\circ} := \bar{\omega} C_1^\perp + \omega C_2$, where $D^{\perp\circ}$ is the dual of D with respect to $(\circ)$.*

Theorem 3. *[9] Let $q = p^m$, where p is an odd prime and $m \geq 1$ is an integer. Suppose $C_1 \subseteq C_2 \subseteq \mathbb{F}_q^n$ are $\mathbb{F}_q$-linear codes with dimensions k_1 and k_2, respectively. Then there exists a q-ary $[[n, k_2 - k_1, \min\{d(C_2 \setminus C_1), d(C_1^\perp \setminus C_2^\perp)\}]]$ quantum code.*

Proof. Define $f : \mathbb{F}_{q^2}^n \to \mathbb{F}_q^{2n}$ by $f(x_1, \ldots, x_n) = (x_1^{(1)}, \ldots, x_n^{(1)} \mid x_1^{(2)}, \ldots, x_n^{(2)})$, where $x_i = x_i^{(1)} + \gamma x_i^{(2)}$ for some $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and fixed $\gamma_0 \in \mathbb{F}_q$ satisfying $\gamma^q = \gamma_0 - \gamma$. By letting $D = \omega C_1 + \bar{\omega} C_2^{\perp}$, as in Proposition 2, then $f(D) \subseteq (f(D))^{\perp}$. Then $f(D)$ is an $\mathbb{F}_q$-linear code in $\mathbb{F}_q^{2n}$. By letting $C = f(D)$ as in Proposition 2, the claim follows. □

This q-ary construction of a quantum code is based on Theorem 9 from [2] and Theorem 13 of [12].

3.2 Quantum two-point Hermitian codes

Recall that a one-point Hermitian code is of the form $C_{\mathcal{L}}(D, aP)$ where P is an $\mathbb{F}_{q^2}$-rational point on the Hermitian curve. Quantum codes from one-point Hermitian codes are studied by Klappenecker and Sarvepalli in [10]. Consider the divisor $G = aP_\infty + bP_{00}$ on the Hermitian curve X over $\mathbb{F}_{q^2}$. In this chapter, we study quantum codes associated with $C_{\mathcal{L}}(D, G)$, a two-point code on the Hermitian curve.

To begin, we recall a result on general two-point codes that is a special case of Theorem 1.

Lemma 4. *[11] Let $A = aP_\infty + bP_{00}$, $B = (a+s)P_\infty + (b+t)P_{00}$, and $D = P_1 + \cdots + P_n$ be divisors on a smooth, projective, absolutely irreducible curve X of genus g over $\mathbb{F}_q$ where $s, t \in \mathbb{Z}^+$. Assume that $A \leq B$ and $(\operatorname{supp} A \cup \operatorname{supp} B) \cap D = \emptyset$ and $\deg B < n$. Then there exists a $[[n, \ell(B) - \ell(A), d]]_q$ code C where*

$$\begin{aligned} d &\geq \min\{d(C_{\mathcal{L}}(D, B) \setminus C_{\mathcal{L}}(D, A)), d(C_{\Omega}(D, A) \setminus C_{\Omega}(D, B))\} \\ &\geq \min\{n - \deg B, \deg A - (2g-2)\} \\ &\geq \min\{n - [(a+s) + (b+t)],\ a + b - (2g-2)\}. \end{aligned}$$

We wish to find a better bound on the minimum distance d. To do so, we first

note that any two-point Hermitian code $C_{\mathcal{L}}(D, G)$ can be expressed as $C_{\Omega}(D, G')$ for an appropriate divisor G'. This is detailed in the following lemma.

Lemma 5. *The dual of the two-point Hermitian code $C_{\mathcal{L}}(D, c_1P_\infty + c_2P_{00})$ can be expressed as*

$$C_{\mathcal{L}}(D, c_1P_\infty + c_2P_{00})^\perp \cong C_{\mathcal{L}}(D, (q^3+q^2-q-2-\lambda(q+1)-c_1)P_\infty + (\lambda(q+1)-c_2-1)P_{00}).$$

where $\lambda \in \mathbb{Z}$.

Proof. According to Prop 2.2.10 [20], $C_{\mathcal{L}}(D, c_1P_\infty + c_2P_{00})^\perp = C_{\mathcal{L}}(D, D - c_1P_\infty - c_2P_{00} + K)$ where $K = (q^2-q-2)P_\infty - \sum_{P_{ab}\in X} P_{ab} + q^3P_\infty$. Then,

$$C_{\mathcal{L}}(D, c_1P_\infty + c_2P_{00})^\perp = C_{\mathcal{L}}(D, q^3+q^2-q-2-c_1)P_\infty - (c_2+1)P_{00}.$$

Recall that $(y^\lambda) = \lambda(q+1)P_{00} - \lambda(q+1)P_\infty$. Given any $\lambda \in \mathbb{Z}$ and multiplying by y^λ induces an isomorphism of Riemann Roch Spaces.

$$\begin{array}{rcl} \mathcal{L}((q^3+q^2-q-2-c_1)P_\infty - (c_2+1)P_{00}) & \to & \mathcal{L}((q^3+q^2-q-2-c_1-\lambda(q+1))P_\infty + (\lambda(q+1)-(c_2+1))P_{00}) \\ f & \mapsto & y^\lambda f. \end{array}$$

This sum induces an isometry

$$C_{\mathcal{L}}(D, (q^3+q^2-q-2-c_1)P_\infty - (c_2+1)P_{00}) \cong$$
$$C_{\mathcal{L}}(D, q^3+q^2-q-2-c_1-\lambda(q+1)P_\infty + (\lambda(q+1)-(c_2+1))P_{00}).$$

□

We will let $\lambda = 1$ when convenient. Let

$$G = q^3+q^2-q-2-(q+1)-(a+s))P_\infty + ((q+1)-(b+t)-1)P_{00}$$

and

$$G' = (q^3+q^2-q-2-(q+1)-a)P_\infty + ((q+1)-b-1)P_{00}.$$

Applying Lemma 5, we see that the quantum code C given in Lemma 4 has minimum distance

$$d \geq \min\{d(C_\Omega(D,G) \setminus C_\Omega(D,G'), d(C_\Omega(D,A) \setminus C_\Omega(D,B))\}.$$

Next we study the values of $d(C_\Omega(D,G) \setminus C_\Omega(D,G'))$ for certain divisors G and G', both supported by two points. To do so, one might use the work of Homma and Kim on the minimum distance of two-point Hermitian codes. This is very tedious as it relies on results detailed in a series of papers [5], [6], [7], [8]. In fact, for the exact minimum distance of two-point Hermitian codes, the formulas are described over five pages. Moreover, this does not exclude the weights of words in $C_\Omega(D,G')$ and $C_\Omega(D,B)$. A better bound results if we utilize the recent work of [13]. Hence, we recall the terminology and tools of [13].

Definition 8. [13] Let X denote the Hermitian curve over $\mathbb{F}_{q^2}$. Let $a, b \in \mathbb{Z}$ and $M_{P_\infty}(a,b)$ be the set of pairs $(f,g) \in \mathbb{F}_{q^2}(X)^2$ of rational functions such that

1) $fg \in \mathcal{L}(aP_\infty + bP_{00}) \setminus \mathcal{L}((a-1)P_\infty + bP_{00})$,

2) $f \in \mathcal{L}(aP_\infty + bP_{00})$, and

3) $g \in \mathcal{L}((a+b)P_\infty)$.

The multiplicity $m_{P_\infty}(a,b)$ is defined as

$$m_{P_\infty}(a,b) = \#\{-b \leq i \leq a+1 : \exists (f,g) \in M_{P_\infty}(a+1,b) \text{ with } \nu_{P_\infty}(f) = -i\}.$$

Definition 9. [13] Let X denote the Hermitian curve over $\mathbb{F}_{q^2}$. Let $a, b \in \mathbb{Z}$ and $M_{P_{00}}(a,b)$ be the set of pairs $(f,g) \in \mathbb{F}_{q^2}(X)^2$ of rational functions such that

1) $fg \in \mathcal{L}(aP_\infty + bP_{00}) \setminus \mathcal{L}(aP_\infty + (b-1)P_{00})$,

2) $f \in \mathcal{L}(aP_\infty + bP_{00})$, and

3) $g \in \mathcal{L}((a+b)P_{00})$.

The multiplicity $m_{P_{00}}(a,b)$ is defined as

$$m_{P_{00}}(a,b) = \#\{-a \leq j \leq b+1 : \exists (f,g) \in M_{P_{00}}(a,b+1) \text{ with } \nu_{P_{00}}(f) = -j\}.$$

In [13], multiplicities are used to determine the minimum distances of two-point Hermitian codes. For divisors D and G, let $C_{\mathcal{L}}(D,G) = C_{\mathcal{L}}(G)$ and $C_{\Omega}(D,G)^{\perp} = C_{\Omega}(G)$. Using the previous ideas, we obtain the following result.

Theorem 6. *Let $A = aP_\infty + bP_{00}$ and $B = (a+s)P_\infty + (b+t)P_{00}$ for any $a,b,s,t \in \mathbb{Z}^+$ with $z := (q^3+q^2-q-2-(q+1)-a)$. Then there exists a q-ary quantum code with length $n = q^3-1$, dimension $k = \ell(B) - \ell(A)$, and minimum distance*

$$d \geq \min \left\{ \begin{array}{l} m_{P_{00}}(z,(q+1)-b-1), \ldots, m_{P_{00}}(z,(q+1)-1), \\ m_{P_{00}}(a,0), m_{P_{00}}(a,1), \ldots, m_{P_{00}}(a,b-1) \end{array} \right\}.$$

Proof. Take divisors $M = aP_\infty$ and $B = aP_\infty + bP_{00}$. Then, [11]

$$d \geq \min\{d(C_{\mathcal{L}}(D,B) \setminus C_{\mathcal{L}}(D,M)), d(C_{\Omega}(aP_\infty) \setminus C_{\Omega}(aP_\Omega + bP_{00}).$$

Notice that $C_{\Omega}(aP_\infty) \supseteq C_{\Omega}(aP_\infty + P_{00}) \supseteq \ldots \supseteq C_{\Omega}(aP_\infty + bP_{00})$. We will now utilize Lemma 5:

$$d(C_{\mathcal{L}}(aP_\infty + bP_{00}) \setminus C_{\mathcal{L}}(aP_\infty)) = d(C \setminus C')$$

where $C = C_{\mathcal{L}}((q^3+q^2-q-2-(q+1)-a)P_\infty + ((q+1)-b-1)P_{00})$ and
$C' = C_{\Omega}((q^3+q^2-q-2-(q+1)-a)P_\infty + ((q+1)-1)P_{00})$.

Thus,

$$C_{\Omega}(zP_\infty + ((q+1)-b-1)P_{00}) \supseteq \ldots \supseteq C_{\Omega}(zP_\infty + ((q+1)-1)P_{00}).$$

Finally,

$$\begin{aligned} d &\geq \min\{d(C_{\mathcal{L}}(D,B) \setminus C_{\mathcal{L}}(D,M)), d(C_{\Omega}(D,M) \setminus C_{\Omega}(D,B))\} \\ &= \min \left\{ \begin{array}{l} m_{P_{00}}(z,(q+1)-b-1), \ldots, m_{P_{00}}(z,(q+1)-1), \\ m_{P_{00}}(a,0), m_{P_{00}}(a,1), \ldots, m_{P_{00}}(a,b-1) \end{array} \right\} \end{aligned}$$

□

Hence, to find a better bound for the minimum distance d, we need to further study multiplicities. Using the multiplicity, we present a way to find a lower bound for $d(C_\Omega(a,b))$, and it can also be utilized to find the lower bound on minimum distance on any geometric two-point codes.

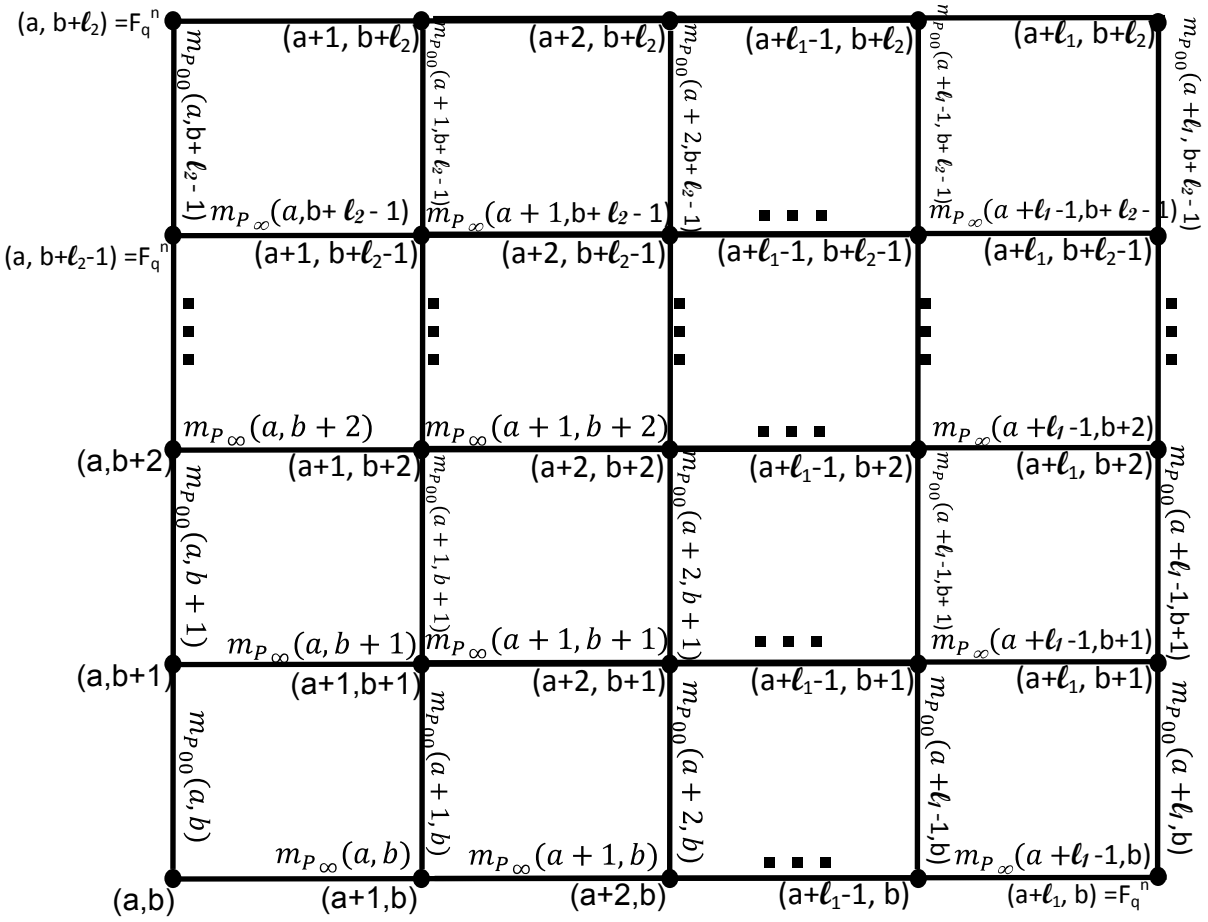
Let $A = aP_\infty + bP_{00}$. We will use the notation $C_\mathcal{L}(a,b)$ to mean $C_\mathcal{L}(D,A)$ and, likewise, $C_\Omega(a,b)$ as the dual code of $C_\mathcal{L}(a,b)$. Consider

$$C_\mathcal{L}(a,b) \subseteq C_\mathcal{L}(a+1,b) \subseteq \cdots \subseteq \mathbb{F}_q^n = C_\mathcal{L}(a+\ell_1,b)$$

for $a,b \in \mathbb{Z}$ and some $\ell_1 \in \mathbb{Z}$. The weight of words c that are orthogonal to $C_\mathcal{L}(a,b)$ but not orthogonal to $C_\mathcal{L}(a+1,b)$ is at least $m_{P_\infty}(a,b)$. Also, the weight of words c that are orthogonal to $C_\mathcal{L}(a+1,b)$ but not orthogonal to $C_\mathcal{L}(a+2,b)$ is at least $m_{P_\infty}(a+1,b)$. This can be continued such that the weight of words c that are orthogonal to $C_\mathcal{L}(a+i,b)$ but not orthogonal to $C_\mathcal{L}(a+i+1,b)$ is at least $m_{P_\infty}(a+i,b)$ for any $i \in \mathbb{Z}$. Also, the weight of words c that are orthogonal to $C_\Omega(a+i+1,b)$ but not orthogonal to $C_\Omega(a+i,b)$ is at least $m_{P_\infty}(a+i,b)$ for any $i \in \mathbb{Z}$. Likewise, since

$$C_\mathcal{L}(a,b) \subseteq C_\mathcal{L}(a,b+1) \subseteq \cdots \subseteq \mathbb{F}_q^n = C_\mathcal{L}(a,b+\ell_2)$$

for $a,b \in \mathbb{Z}$ and some $\ell_2 \in \mathbb{Z}$, the weight of words c that are orthogonal to $C_\mathcal{L}(a,b+j+1)$ (resp. $C_\Omega(a,b+j)$) but not orthogonal to $C_\mathcal{L}(a,b+j)$ (resp. $C_\Omega(a,b+j+1)$) is at least $m_{P_{00}}(a,b+j)$ for any $i \in \mathbb{Z}$. This can be represented by a graph with codes represented by nodes and bounds of the minimum distances as edges.



A path is a sequence of edges that allows one to get to $(a+\ell_1, b+\ell_2)$ from (a,b) without retracing an edge. Using this idea, along with Definition 8, we have the following Theorem.

Theorem 7. *Let $A = aP_\infty + bP_{00}$ and $B = (a+s)P_\infty + (b+t)P_{00}$. Then, there exists a quantum code with length $n = q^3 - 1$, dimension $k = \ell(B) - \ell(A)$, and minimum distance*

$$\begin{aligned} d &\geq \min\{d(C_{\mathcal{L}}(D,B) \setminus C_{\mathcal{L}}(D,A)), d(C_\Omega(D,A) \setminus C_\Omega(D,B))\} \\ &\geq \min\{max\{P_1\}, max\{P_2\}\} \end{aligned}$$

where $P_2 := \{\min(P) : P$ is a path from (a,b) to $(a+s, b+t)\}$,

$P_1 := \{\min(P) : P$ *is a path from* $(q^3+q^2-q-2-(q+1)-(a+s), (q+1)-(b+t)-1)$ *to* $(q^3+q^2-q-2-(q+1)-a, (q+1)-b-1)\}$,

and $\min(P)$ *is the minimum multiplicity along a path* P*.*

Proof. Let $c \in C_\Omega(a, b)$. The words not orthogonal to $C_\mathcal{L}(a + i + 1, b)$ and orthogonal to $C_\mathcal{L}(a + i, b)$ have weight at least $m_{P_\infty}(a + i, b)$ for any given i along the edges in a path P. Similarly, the words not orthogonal to $C_\mathcal{L}(a, b + j + 1)$ and orthogonal to $C_\mathcal{L}(a, b + j)$ have weight at least $m_{P_{00}}(a, b+j)$ for any given j. A lower bound for $\mathrm{wt}(c)$ is the maximum of the set of minimum multiplicites of each individual path. This can easily be found by finding the smallest multiplicity along each path. Then, consider the maximum of this set, which will be a bound for the minimum weight of c. □

This theorem is a better estimate of the minimum distance. We can specify the actual values of the multiplicities given some parameters in [13].

Chapter 4

Conclusion

In this Master's thesis, we considered quantum codes from two-point Hermitian codes. In doing so, we obtained $[[n, k, d]]_q$ quantum codes with a bound on the minimum distance d in terms of multiplicites. In future research, we hope to study multiplicities to better bound the minimum distance d. For a quantum code, the minimum distance is just one of its parameters; other parameters may also be relevant to its strength.

Bibliography

[1] A. Ashikhmin and E. Knill, Nonbinary quantum stabilizer codes. *IEEE Trans. Inform. Theory* 47 (2001), no. 7, 3065-3072.

[2] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Quantum error correction via codes over *GF(4)*, *IEEE Trans. Inform. Theory*, vol. 44, pp. 1369-1387, 1998.

[3] A. R. Calderbank and P. W. Shor, Good quatum error-correcting codes exist, *Phys. Rev. A,* 54, (1996), 1098-1105.

[4] V. D. Goppa, *Geometry and Codes*, Kluwer, 1988.

[5] M. Homma and S. J. Kim, The complete determination of the minimum distance of two-point codes on a Hermitian curve, *Des. Codes Cryptogr.,* 40, (2006), no. 1, 5-24.

[6] M. Homma and S. J. Kim, Toward the determination of the minimum distance of two-point codes on a Hermitian curve, *Des. Codes Cryptogr.,* 37, (2005), no. 1, 111-132.

[7] M. Homma and S. J. Kim, The two-point codes on a Hermitian curve with the designed minimum distance, *Des. Codes Cryptogr.* 38 (2006), no. 1, 55-81.

[8] M. Homma and S. J. Kim, The two-point codes with the designed distance on a Hermitian curve in even characteristic, *Des. Codes Cryptogr.* 39 (2006), no. 3, 375-386.

[9] J.L. Kim and J.L. Walker, Nonbinary quantum error-correcting codes from algebraic curves, *Discrete Math.* (2007), doi:10.016/j.disc.2007.08.038.

[10] A. Klappenecker and P.K. Sarvepalli, Nonbinary quantum codes from Hermitian curves, *Applied algebra, algebraic algorithms, and error-correcting codes*, 136-143, Lecture Notes in Comput. Sci., 3857, Springer, Berlin, 2006.

[11] J. L. Kim and G. L. Matthews, Quantum error-correcting codes from algebraic curves, in *Advances in Algebraic Geometry Codes*, Series on Coding Theory and Cryptology (World Scientific, 2008), vol. 5; E. Martinez-Moro, C. Munuera, and D. Ruano, eds.; 419-444.

[12] R. Matsumoto, and T. Uyematsu, Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes, *IEICE Trans. Fundamentals*, E83-A, (2000), 1878-1883.

[13] S. Park, Applications of algebraic curves to cryptography, Dissertation, University of Illinois, Urbana, 2007.

[14] S. Park, Minimum distance of Hermitian two-point codes, *Des. Codes Cryptogr.* January 2010.

[15] E. M. Rains, Nonbinary quantum codes, *IEEE Trans. Inform. Theory,* 45, (1999), 1827-1832.

[16] P. W. Shor, Scheme for reducing decoherence in quantum memory, *Phys. Rev. A,* 52, (1995), 2493.

[17] A. M. Steane, Multiple particle interference and quantum error correction, *Proc. Roy. Soc. London A* 452, (1996), 2551-2577.

[18] A. M. Steane, Simple quantum error correcting codes, *Phys. Rev. Lett.*, 77, (1996), 793-797.

[19] A. M. Steane, Enlargement of Calderbank-Shor-Steane quantum codes, *IEEE Trans. Inform. Theory,* 45, (1999), no. 7, 2492-2495.

[20] H. Sticktenoth, Algebraic Function Fields and Codes, Springer-Verlag, 1993.

[21] J. L. Walker, *Codes and Curves*, American Mathematical Society, RI, 2000.