Quantum Algebraic-Geometric Codes

Chiu Fan Lee
Clare Hall
Cambridge

Part III essay in the
Department of Applied Mathematics and Theoretical Physics
University of Cambridge

May 2001

Abstract

This is a Part III essay aiming to discuss the contruction of quantum error-correcting codes through the use of the theory of algebraic function fields, which produces codes with asymptotically good parameters. This exposition emphasises constructibility and several applications of the main theorem (theorem 6.2) are given. Prerequisites are the first 12 lectures of the Part III course Quantum Information Theory [16] or chapter 7 of Preskill's Lecture Notes [15], and the first two chapters of Stichtenoth's *Algebraic Function Fields and Codes* [19].

Contents

Chapter 1

Introduction

As of today, scientists widely speculate that quantum computers could offer more computational power than conventional computers are able to. But due to the delicate nature of quantum quantities, the introduction of error during computation seems inevitable. Therefore, protections of information either by encoding or other methods were introduced. This essay aims to discuss the application of algebraic geometry on quantum error-correcting codes. The motivation behind is the potential error-correcting power of this method of construction. For instance, quantum algebraic-geometric codes are the only known quantum error-correcting codes that are asymptotically good, a notion which will be explained later.

The essay is organised in eight chapters. The next chapter offers a brief review on general coding theory in both classical and quantum cases. Chapter three investigates the stabilizer formalism, which corresponds to a very large subset of all known quantum error-correcting codes. Chapter four discusses the Calderbank-Shor-Steane construction of quantum codes, which makes use of the self-duality property of classical codes to produce quantum codes. Chapter five serves as a review and a quick reference guide on the theory of algebraic-geometric codes. Chapter six describes how algebraic geometry is used to construct asymptotically good quantum codes. The machinery developed is then applied to some specific algebraic function fields in chapter seven.

To make the exposition more transparent, all algorithms, definitions, examples and remarks will end with the symbol '$\triangle$', while all proofs will end with the symbol '$\diamondsuit$' throughout the essay.

Chapter 2

Review on coding theory

2.1 Review on classical coding theory

In this section, we will review some important notions in classical coding theory.

Let GF_q denote the finite field with q elements. We consider the n-dimensional vector space GF_q^n.

Definition 2.1 For $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n) \in GF_q^n$, let

$$d(a, b) := \#\{i \mid a_i \neq b_i\}.$$

The *weight* of an element in GF_q^n is defined as

$$wt(a) := d(a, 0) = \#\{i \mid a_i \neq 0\}.$$

△

Definition 2.2 A *code* C is a linear subspace of GF_q^n; the elements of C are called *codewords*. We call n the *length* of C and denote $dim C$ by k. An $[n, k]$ code is a code of length n and dimension k. The *minimum distance* $d(C)$ is defined to be

$$d(C) := \min\{d(a, b) \mid a, b \in C \text{ and } a \neq b\} = \min\{wt(c) \mid 0 \neq c \in C\}.$$

We refer to such a code C as an $[n, k, d]$ code. △

Definition 2.3 Let C be an $[n, k]$ code over GF_q^n. A *generator matrix* G of C is a $k \times n$ matrix whose rows are a basis of C. △

Definition 2.4 If $C \subseteq GF_q^n$ is a code, then

$$C^{\perp} := \{u \in GF_q^n \mid \sum_{i=1}^{n} u_i c_i = 0, \ \forall c \in C\}$$

is called the *dual* of C. △

Definition 2.5 A generator matrix H of $C^{\perp}$ is said to be a *parity-check matrix* for C. $\triangle$

Note that $Hu^t = 0$ for all $u \in C$ where u^t is the transpose of u.

2.2 Review on quantum coding theory

So much for classical coding theory, we will now introduce some important elements in the theory of quantum error-correcting code. See [15] for the physical significance of the statements in this section.

Let $\mathbf{C}^2$ be a 2-dimensional complex Hilbert space. An element of $\mathbf{C}^2$ is called a *qubit*. The space $(\mathbf{C}^2)^{\otimes n}$ is the space of quantum words of length n.

Definition 2.6 A *quantum code* Q is a K-dimensional linear subspace of $(\mathbf{C}^2)^{\otimes n}$. We refer to Q as an $((n, K))$ quantum code. Note the double brackets used to distinguish quantum codes from classical codes. $\triangle$

Definition 2.7 An *error* is a linear operator E acting on $(\mathbf{C}^2)^{\otimes n}$. $\triangle$

Definition 2.8 We define the *support* $SuppE$ in the following way. If E can be written as $I_i \otimes E'$, where I_i is the identity operator acting on the i-th tensor component and E' acts on other tensor components only, then we say $i \notin SuppE$. The *weight* of E is defined to be

$$wt(E) = \#SuppE.$$

$\triangle$

Definition 2.9 A quantum code Q is called *d-error correcting* if for all errors E, F with $wt(E), wt(F) \leq d$ and for all pair of vectors $u, v \in Q$,

$$\langle F(v) \mid E(u) \rangle = c_{E,F} \langle v \mid u \rangle,$$

where $c_{E,F}$ is a complex number depending only on E and F and $\langle \mid \rangle$ is the standard Hermitian inner product. Furthermore, if $c_{E,F}$ is 0 unless $E = F$, then we say the quantum code is *nondegenerate*.

Similar to the classical case, we will refer to Q as an $((n, K, d))$ quantum code. $\triangle$

For long quantum codes to be useful, we need to know their asymptotic behaviour. Letting $k_Q = \log_2 K_Q$, we set

$$R_Q = \frac{k_Q}{n}, \tag{2.1}$$

$$\delta_Q = \frac{d_Q}{n}, \tag{2.2}$$

$$R(\delta) = \limsup_{n \to \infty} R_Q, \tag{2.3}$$

where the limit is taken over all quantum codes with $\delta_Q \geq \delta$. The best known nonconstructive lower bound (see lecture 9 of [16]) on $R(\delta)$ is

$$R(\delta) \geq 1 - \delta \log_2 3 - H(\delta), \tag{2.4}$$

where $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function.

2.3 From non-binary to binary codes

In order to utilize the potential of algebraic construction, one needs to consider algebraic functions over finite fields other then GF_2. This section is thus aimed to estimate the parameters of the code obtained by binary expanding a code over GF_{2^m}.

Definition 2.10 The *trace* of $a \in GF_{2^m}$ is defined by

$$Tr(a) = \sum_{i=0}^{m-1} a^{2^i}.$$

△

Theorem 2.11 *For all natural number m, there exists a self-dual basis $\{u_1, \ldots, u_m\}$ of GF_{2^m} over GF_2, i.e.,*

$$Tr(u_i u_j) = \delta_{ij}.$$

Proof. See [12]. ♢

The following theorem is due to T. Kasami and S. Lin [11].

Theorem 2.12 *Let C be a code over GF_{2^m}, $C \supset C^\perp$ and $u_i, i = \{1, \ldots, m\}$ be a self-dual basis of GF_{2^m} over GF_2. Let D and E be codes obtained by the symbolwise binary expansion of codes C and $C^\perp$ in the basis u_i. Then* (1) *$D \supset E$ and* (2) *$E = D^\perp$.*

Proof. (1) The statement is obvious since D, E are obtained from $C, C^\perp$ by binary expansion.

(2) Let $a = (a_1, \ldots, a_n) \in C$ and $b = (b_1, \ldots, b_n) \in C^\perp$. Let

$$a_j = \sum_{i=1}^{m} a_i^{(j)} u_i \text{ and } b_j = \sum_{i=1}^{m} b_i^{(j)} u_i.$$

Then

$$0 \;=\; \sum_{j=1}^{n} a_j b_j = Tr(\sum_{j=1}^{n} a_j b_j) \tag{2.5}$$

$$= Tr(\sum_{j=1}^{n} \sum_{i,k=1}^{m} a_i^{(j)} b_k^{(j)} u_i u_k) \quad (2.6)$$

$$= \sum_{j=1}^{n} \sum_{i,k=1}^{m} a_i^{(j)} b_k^{(j)} Tr(u_i u_k) \quad (2.7)$$

$$= \sum_{j=1}^{n} \sum_{i=1}^{m} a_i^{(j)} b_i^{(j)} \quad (2.8)$$

So $D^{\perp} \supseteq E$. Now as the dimensions of D and E are complementary, we have $E = D^{\perp}$. $\diamondsuit$

Remark 2.13 It is obvious that if we start with a triple $C' \supset C \supseteq C^{\perp}$ of codes over GF_{2^m}, the binary expansion again gives us a triple $D' \supset D \supseteq D^{\perp}$ of binary codes. $\triangle$

Chapter 3

Stabilizer formalism and encoding procedure

3.1 Stabilizer formalism

Definition 3.1 For $(a \mid b), (u \mid v) \in \{0,1\}^{2n}$ we define a *symplectic scalar product* $\odot$ on $\{0,1\}^{2n}$ by

$$(a \mid b) \odot (u \mid v) = a \cdot v \oplus u \cdot b,$$

where $\oplus$ denotes mod-2 addition. △

Definition 3.2 A *stabilizer matrix*

$$\mathcal{H} = (H_X \mid H_Z)$$

is a $(n-k) \times 2n$ matrix of rank $(n-k)$ such that for any rows $(a \mid b), (u \mid v)$ in $\mathcal{H}$,

$$(a \mid b) \odot (u \mid v) = 0$$

and

$$a \cdot b := \sum_{i=1}^{n} a_i b_i = 0.$$

△

Definition 3.3 Let S be the vector space generated by the rows of $\mathcal{H}$, we define the *weight* of an element $(a \mid b) \in S$ as

$$wt(a \mid b) = \sum_i (a_i \vee b_i),$$

where $a_i \vee b_i = \max\{a_i, b_i\}$. △

Theorem 3.4 *For any stabilizer matrix $\mathcal{H}$, and S the vector space generated by the rows of $\mathcal{H}$. If d is an integer such that for all $(a \mid b) \in \{0,1\}^{2n}$ with weight $= \sum_i (a_i \vee b_i) < d$, either $(a \mid b)$ lies in S or lies outside of the $\odot$-orthogonal space $S_{\odot}^{\perp}$. Then there is a quantum code Q associated to $\mathcal{H}$ with length n and dimension 2^k which is d-error correcting.*

Furthermore, if for all vectors $(a \mid b)$ with $wt(a \mid b) < d$, they all lie outside of $S_{\odot}^{\perp}$, then the quantum code is nondegenerate.

PROOF. See lecture 11 of [16] or chapter 7 of [15]. ♢

Definition 3.5 Given a stabilitzer matrix $\mathcal{H} = (H_X \mid H_Z)$ with $(n-k)$ rows, we refer to the corresponding quantum code Q as an $[[n,k,d]]$ if Q is d-error correcting. △

3.2 Converting stabilizer matrix into standard form

In this following two sections, we will investigate the procedure for encoding. For more detailed treatment, we refer the readers to [4, 7, 14].

Given a stabilizer matrix $\mathcal{H}$, by Gaussian elimination (which correspond to multiplying two generators and switching qubits enumerations and hence do not change the corresponding quantum code), we can transform $\mathcal{H}$ into the following form:

$$\begin{array}{r} \\ r\{ \\ n-k-r\{ \end{array} \begin{array}{c} \overbrace{}^{r}\overbrace{}^{n-r}\,\overbrace{}^{r}\overbrace{}^{n-r} \\ \left(\begin{array}{cc|cc} I & A & B & C \\ 0 & 0 & D & E \end{array} \right) \end{array}$$

where I denotes the $r \times r$ identity matrix and r is the rank of H_X.

Then, by doing Gaussian elimination on E, we can have $\mathcal{H}$ transformed to:

$$\begin{array}{r} \\ r\{ \\ n-k-r-s\{ \\ s\{ \end{array} \begin{array}{c} \overbrace{}^{r}\overbrace{}^{n-k-r-s}\overbrace{}^{k+s}\,\overbrace{}^{r}\overbrace{}^{n-k-r-s}\overbrace{}^{k+s} \\ \left(\begin{array}{ccc|ccc} I & A_1 & A_2 & B & C_1 & C_2 \\ 0 & 0 & 0 & D_1 & I & E_2 \\ 0 & 0 & 0 & D_2 & 0 & 0 \end{array} \right). \end{array}$$

In order for the first r rows of H_X to be $\odot$-orthogonal to the last s rows of H_Z, we must have $D_2 = 0$, which implies $s = 0$. Also, by using the last $n-k-r$ rows, C_1 can be eliminated all together. Therefore, we can always put $\mathcal{H}$ into the following form which we call the *standard form*:

$$\begin{array}{r} \\ r\{ \\ n-k-r\{ \end{array} \begin{array}{c} \overbrace{}^{r}\overbrace{}^{n-k-r}\overbrace{}^{k}\,\overbrace{}^{r}\overbrace{}^{n-k-r}\overbrace{}^{k} \\ \left(\begin{array}{ccc|ccc} I & A_1 & A_2 & B & 0 & C \\ 0 & 0 & 0 & D & I & E \end{array} \right). \end{array} \tag{3.1}$$

We now define two matrices, $\bar{X}$ and $\bar{Z}$, which will enable us to find a basis for Q with easy encoding procedure.

Definition 3.6 Given a stabilizer matrix $\mathcal{H}$ in standard form as above, the $\bar{X}^{\mathcal{H}}$-matrix and $\bar{Z}^{\mathcal{H}}$-matrix are defined to be

$$\bar{X}^{\mathcal{H}} = (\overbrace{0}^{r} \quad \overbrace{E^t}^{n-k-r} \quad \overbrace{I}^{k} \mid \overbrace{C^t}^{r} \quad \overbrace{0}^{n-k-r} \quad \overbrace{0}^{k})$$

$$\bar{Z}^{\mathcal{H}} = (\overbrace{0}^{r} \quad \overbrace{0}^{n-k-r} \quad \overbrace{0}^{k} \mid \overbrace{A_2^t}^{r} \quad \overbrace{0}^{n-k-r} \quad \overbrace{I}^{k}).$$

We denote the i-th row of $\bar{X}^{\mathcal{H}}$ and $\bar{Z}^{\mathcal{H}}$ by $\bar{X}_i^{\mathcal{H}}$ and $\bar{Z}_i^{\mathcal{H}}$ respectively. △

Proposition 3.7 *Given a stabilizer matrix $\mathcal{H}$.*
(a) *The rows in $\bar{Z}^{\mathcal{H}}$ are linearly independent and $\odot$-orthogonal with the rows in $\mathcal{H}$.*
(b) *The rows of $\bar{X}^{\mathcal{H}}$ are linearly independent and $\odot$-orthogonal with the rows in $\mathcal{H}$. Moreover, $\bar{X}_j^{\mathcal{H}}$ is $\odot$-orthogonal with all the $\bar{Z}_i^{\mathcal{H}}$ except $\bar{Z}_j^{\mathcal{H}}$.*

Proof. Straight forward verification. ♢

Because of the previous result, we can define a basis for the quantum code Q associated to $\mathcal{H}$ to be the states with stabilizer

$$\langle \mathcal{H}_1, \ldots, \mathcal{H}_{n-k}, (-1)^{x_1} \bar{Z}_1^{\mathcal{H}}, \ldots, (-1)^{x_k} \bar{Z}_k^{\mathcal{H}} \rangle$$

where $(x_1, \ldots, x_k) \in \{0,1\}^k$.

3.3 Quantum circuit for encoding

In order to encode any quantum message, we first need the following proposition.

Proposition 3.8 *Given a stabilizer matrix $\mathcal{H} = (H_X \mid H_Z)$ in standard form (3.1). For any i-th row of $\mathcal{H}$, there is a vector $U^i = (u_x^i \mid u_z^i)$ such that U^i is $\odot$-orthogonal to all $\bar{Z}^{\mathcal{H}}$ and is $\odot$-orthogonal to all the rows in $\mathcal{H}$ except the i-th row.*

Proof. We take

$$U = \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & I & 0 & 0 \\ 0 & I & 0 & 0 & 0 & 0 \end{array} \right)$$

and let U^i be the i-th row of U. The claim will then be easily verified. ♢

To encode the $|0\rangle^{\otimes k}$ state, we start with the state $|0\rangle^{\otimes n}$ and measure each of the observables $\mathcal{H}_1, \ldots, \mathcal{H}_{n-k}, \bar{Z}_1^{\mathcal{H}}, \ldots, \bar{Z}_k^{\mathcal{H}}$ in turn. We then will have a state stabilized by $\langle \pm\mathcal{H}_1, \ldots, \pm\mathcal{H}_{n-k}, \pm\bar{Z}_1^{\mathcal{H}}, \ldots, \pm\bar{Z}_k^{\mathcal{H}} \rangle$ where the plus or minus signs depend on the measurement outcomes. Then by applying the set of operators $\{\bar{X}_1^{\mathcal{H}}, \ldots, \bar{X}_k^{\mathcal{H}}\}$ and those found by proposition 3.8, we can change the state to an arbitrary encodes basis state $|x_1, \ldots, x_k\rangle_{encoded}$.

Figure 3.1: Quantum circuit for measuring a single qubit operator M with eigenvalues ± 1.

We now consider the network that performs the measurement. We first note that to do a measurement on a operator M with eigenvalues ± 1, the quantum circuit in figure 3.1 may be used:

Then, the following example should suffice to demonstrate how encoding procedure is done in general.

Example 3.9 We consider the five-qubit code which has stabilizer matrix

$$\mathcal{H} = \left(\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{array}\right).$$

Hence, we have

$$\bar{X} = (00001 \mid 10010) \ , \ \bar{Z} = (00000 \mid 11111).$$

Therefore, to measure the observables $\mathcal{H}_1, \ldots, \mathcal{H}_{n-k}, \bar{Z}_1^{\mathcal{H}}, \ldots, \bar{Z}_k^{\mathcal{H}}$, the circuit in figure 3.2 may be used.

After the measurement, we may then apply $\bar{X}$ and those operators found in proposition 3.8 to convert the quantum state into any encoded state as desired.

△

Figure 3.2: Quantum circuit for measuring the generators and $\bar{Z}$ of the 5-qubit code.

Chapter 4

Calderbank-Shor-Steane construction

4.1 CSS construction

Definition 4.1 Let C be a classical $[n, k, d]$ code containing its dual $C^{\perp}$ and let H be the parity-check matrix of C. Then the CSS code corresponding to C is the quantum code associated to the stabilizer matrix

$$\mathcal{H} = \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix}.$$

△

By construction, it is trivial that $\mathcal{H}$ is indeed a stabilizer matrix.

Theorem 4.2 *Let C be a classical $[n, k, d]$ code containing its dual $C^{\perp}$. Then the corresponding CSS code is a $[[n, 2k - n, d]]$ quantum code.*

Proof. The theorem follows easily from theorem 3.4 and the construction of $\mathcal{H}$. ♢

4.2 Enlargement of CSS quantum codes

Definition 4.3 The *i-th generalized distance d_i* of a linear code C is the minimum size of the support of a i-th dimensional subcode of C. △

Note that d_1 is the minimum distance of the code and d_2 is the minimum weight of the bitwise OR of two different nonzero codewords, i.e., $d_2 = \min\{\sum_i (a_i \vee b_i) \mid a, b \in C\}$. We also have the following inequality for d_1 and d_2.

Proposition 4.4 *For any linear code C with parameters $[n, k, d]$,*

$$\left\lceil \frac{3d_1}{2} \right\rceil \leq d_2.$$

PROOF. Take any two distinct element $u, v \in C$ such that the corresponding d_2 is achieved. Assume $wt(u) = d_1 = d$ and the general case can then be proved by induction. By rearranging terms, we can assume the first d entries of u are 1's. If $d_2 < \lceil \frac{3d}{2} \rceil$, either $wt(v) < d$ or $wt(u+v) < d$, a contradiction as $v, u+v \in C$. $\diamondsuit$

To construct better quantum codes, we need the enlarged CSS construction which was first invented by Steane [17]. He proved that the quantum code constructed has parameter $[[n, k+k'-n, \min\{d, \lceil \frac{3d'}{2} \rceil\}]]$. Cohen, Encheva and Litsyn later improved the minimal distance to $\min\{d, d_2'\}$ [5]. We will give an alternative proof to the theorem based on the symplectic geometry formalism introduced earlier.

Theorem 4.5 *Given a classical binary error correcting code $C = [n, k, d]$ which contains its dual, $C^\perp \subseteq C$, and which can be enlarged to $C' = [n, k' > k+1, d']$, a nondegenerate quantum code of parameters $[[n, k+k'-n, \min\{d, d_2'\}]]$ can be constructed.*

PROOF. Let H' be the parity-check matrix of C' and H' and B together check C. Consider

$$\mathcal{H} = \begin{pmatrix} AB & B \\ H' & 0 \\ 0 & H' \end{pmatrix},$$

where A is a $(k'-k) \times (k'-k)$ matrix such that AB, $(A+I)B$ and B generate the same set. One possible choice is

$$A = \begin{pmatrix} 0100\ldots0 \\ 0010\ldots0 \\ 0001\ldots0 \\ \ldots \\ 0000\ldots1 \\ 1100\ldots0 \end{pmatrix}.$$

By construction, u, v rows in H' implies

$$u, v \in C'^\perp \Rightarrow u \in C^\perp \subset C' \Rightarrow u \cdot v = 0.$$

Similar calculations can show $\mathcal{H}$ is indeed a stabilizer matrix.

We now let S be the vector space generated by the rows of $\mathcal{H}$. If $(\alpha \mid \beta) \in \{0,1\}^{2N}$ is such that

$$(\alpha \mid \beta) \odot (u \mid v) = \alpha \cdot v \oplus u \cdot \beta = 0, \forall (u \mid v) \in S.$$

Then we consider two cases: (1) either α or β is $\mathbf{0}$; (2) they are both nonzero.

(1) W.l.o.g., take β to be zero, then $\alpha \in C$, so $wt(\alpha) \geq d$.

(2) If they are both nonzero, we have $\alpha, \beta \in C'$. If $\alpha = \beta$, then by the requirement of A, $\alpha = \beta$ is in C and so $wt(\alpha \mid \beta) \geq d$. If $\alpha \neq \beta$, $wt(\alpha \mid \beta) \geq d_2'$ by definition.

Now, as all the vectors with weights under $\min\{d, d_2'\}$ are outside of $S_\odot^\perp$, the corresponding quantum code is nondegenerate. $\diamondsuit$

Chapter 5

Algebraic function fields and codes

This chapters serves as a reference on definitions and theorems needed for later development. All proofs of statements can be found in [19].

5.1 Review on algebraic function fields

Definition 5.1 An *algebraic function field* F/K of one variable over K is an extension field $F \supseteq K$ such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over K. $\triangle$

Definition 5.2 A *valuation ring* of the function field F/K is a ring $O \supseteq F$ such that: (1) $K \subset O \subset F$, and (2) for any $z \in F$, $z \in O$ or $z^{-1} \in O$. $\triangle$

Proposition 5.3 *Let O be a valuation ring of the function field F/K. Then (a) O is a local ring, i.e., O has a unique maximal ideal P.*
(b) P is a principal ideal.
(c) If $P = tO$ then any $0 \neq z \in F$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbf{Z}$, $u \in O^*$.

Proof. See proposition I.1.5 and theorem I.1.6 in [19]. $\diamondsuit$

Definition 5.4 (a) A *place* P of the function field F/K is the maximal ideal of some valuation ring O of F/K. Any element $t \in P$ such that $P = tO$ is called a prime element of P.

(b) $\mathbf{P}_F := \{P \mid P \text{ is a place of } F/K\}$.

(c) To any place $P \in \mathbf{P}_F$ we associate a function $v_P : F \to \mathbf{Z} \cup \{\infty\}$ by defining $v_P(0) := \infty$ and $v_P(z) := n$ when $z = t^n u$ with t a prime element of P. $\triangle$

Definition 5.5 Let P be a place of F/K and O_P be its valuation ring. For $x \in O_P$ we define $x(P) \in O_P$ to be the residue class of x modulo P, for $x \in F \backslash O_P$ we define $x(P) := \infty$. We note that this symbol ∞ is different from that used in the previous definition but confusion should not arise. $\triangle$

Proposition 5.6 *In a function field F/K, for any element $0 \neq x \in F$, the set $\{P \in \mathbf{P}_F \mid v_P(x) \neq 0\}$ is finite.*

PROOF. See corollary I.3.4 in [19]. ♢

Definition 5.7 The free abelian group which is generated by the places of F/K is denoted by $\mathcal{D}_F$, the *divisor group* of F/K. The element of $\mathcal{D}_F$ are called divisors of F/K. In other words, a divisor is a formal sum

$$D = \sum_{P \in \mathcal{P}_F} n_P P \text{ with } n_P \in \mathbf{Z}, \text{ almost all } n_P = 0.$$

△

Definition 5.8 $(x) = \sum_{P \in \mathbf{P}_F} v_P(x)P$. △

Remark 5.9 (x) is in $\mathcal{D}_F$ by proposition 5.6. △

Definition 5.10 For a divisor $A \in \mathcal{D}_F$ we set

$$\mathcal{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{0\}.$$

The dimension of the vector space $\mathcal{L}(A)$ over K is denoted by $dim(A)$. △

Definition 5.11 An *adele* of F/K is a mapping

$$\alpha : \begin{cases} \mathbf{P}_F & \to & F \\ P & \mapsto & \alpha_P, \end{cases}$$

such that $\alpha \in O_P$ for almost all $P \in \mathbf{P}_F$.

$$\mathcal{A}_F := \{\alpha \mid \alpha \text{ is an adele of } F/K\}$$

is called the *adele space* of F/K. It is also a vector space over K. △

Definition 5.12 A *Weil differential* of F/K is a K-linear map $\omega : \mathcal{A}_F \to K$ vanishing on $\mathcal{A}_F(A) + F$ for some divisor $A \in \mathcal{D}_F$. We call

$$\Omega := \{\omega \mid \omega \text{ is a Weil differential of } F/K\}$$

the *module of Weil differentials* of F/K. For $A \in \mathcal{D}_F$ let

$$\Omega(A) := \{\omega \mid \omega \text{ vanishes on } \mathcal{A}_F(A) + F\}.$$

Also, for $\omega \neq 0$, let

$$M(\omega) := \{A \in \mathcal{D}_F \mid \omega \text{ vanishes on } \mathcal{A}_F(A) + F\}.$$

△

Theorem 5.13 *Let $0 \neq \omega \in \Omega$. Then there is a uniquely determined divisor $W \in M(\omega)$ such that $A \leq W$ for any $A \in M(\omega)$.*

PROOF. Theorem I.5.10 in [19]. ♢

Definition 5.14 The divisor (ω) of a Weil differential $\omega \neq 0$ is the uniquely determined divisor of F/K satisfying
(1) ω vanishes on $\mathcal{A}_F((\omega)) + F$.
(2) If ω vanishes on $\mathcal{A}_F(A) + F$, then $A \leq (\omega)$.
A divisor W is called a *canonical divisor* of F/K if $W = (\omega)$ for some $\omega \in \Omega$. △

Theorem 5.15 *Let $A \in \mathcal{D}_F$ and $W = (\omega)$ a canonical divisor of F/K. Then $\mathcal{L}(W - A)$ and $\Omega(A)$ are isomorphic as K-vector space. In particular,*

$$dim(W - A) = dimA - degA + g - 1.$$

PROOF. See theorem I.5.14 in [19]. ♢

Definition 5.16 The *genus* g of F/K is defined by

$$g := \max\{degA - dimA + 1 \mid A \in \mathcal{D}_F\}.$$

△

Theorem 5.17 *The genus g of F/K is a non-negative integer.*

PROOF. See remark I.4.16 in [19]. ♢

Theorem 5.18 (Riemann-Roch Theorem) *Let W be a canonical divisor of F/K. Then, for any $A \in \mathcal{D}_F$,*

$$dimA = degA + 1 - g + dim(W - A).$$

PROOF. See theorem I.5.15 in [19]. ♢

Corollary 5.19 *For a canonical divisor W, we have*

$$degW = 2g - 2 \text{ and } dimW = g.$$

PROOF. To show $dimW = g$, take $A = 0$. To show $degW = 2g - 2$, take $A = W$. ♢

Theorem 5.20 *If A is a divisor of F/K of degree $\geq 2g - 1$, then*

$$dimA = degA + 1 - g.$$

PROOF. See theorem I.5.17 in [19]. ♢

Definition 5.21 Let $P \in \mathbf{P}_F$.

(a) For $x \in F$, let $\iota_P(x) \in \mathcal{A}_F$ be the adele whose P-component is x, and all other components are 0.

(b) For a Weil differential $\omega \in \Omega$, define its *local component* $\omega_P : F \to K$ by

$$\omega_P(x) := \omega(\iota_P(x)).$$

△

Proposition 5.22 *Let $P \in \mathbf{P}_F$ be a place of degree one and $\omega \in \Omega$. Let $(\omega) = \sum_{i=1}^{n} a_{P_i} P_i$ be such that $a_{P_i} \geq -1$ for $P_i = P$.*

(a) $\omega_P(1) = 0 \Leftrightarrow a_P \geq 0$.

(b) For $x \in F$ with $v_P(x) \geq 0$,

$$\omega_P(x) = x(P)\omega_P(1).$$

PROOF. See proofs of theorems II.2.7 and II.2.8 in [19]. ♢

Theorem 5.23 *Let $\omega \in \Omega$ and $\alpha = (\alpha_P) \in \mathcal{A}_F$. Then $\omega_P(\alpha_P) \neq 0$ for at most finitely many places P, and*

$$\omega(\alpha) = \sum_{P \in \mathbf{P}_F} \omega_P(\alpha_P).$$

PROOF. See proposition I.7.2 in [19]. ♢

5.2 Algebraic geometric codes

For this section, we will always have the following notations:

F/GF_q is an algebraic function fields of genus g;
$P_1, \ldots, P_n$ are pairwise distinct places of F/GF_q of degree 1;
$D = P_1 + \ldots + P_n$;
G is a divisor of F/GF_q such that $suppG \cap suppD = \emptyset$.

Definition 5.24 The *algebraic geometric codes* $C_{\mathcal{L}}(D, G)$ and $C_{\Omega}(D, G)$ associated with the divisors D and G are defined by

$$C_{\mathcal{L}}(D, G) := \{(x(P_1), \ldots, x(P_n)) \mid x \in \mathcal{L}(G)\} \subseteq GF_q^n \quad (5.1)$$

$$C_{\Omega}(D, G) := \{(\omega_{P_1}(1), \ldots, \omega_{P_n}(1)) \mid \omega \in \Omega_F(G - D)\} \subseteq GF_q^n. \quad (5.2)$$

△

Theorem 5.25 $C_{\Omega}(D, G) = C_{\mathcal{L}}(D, G)^{\perp}$.

PROOF. See theorem II.2.8 in [19]. ♢

Theorem 5.26 *Let $2g - 2 < degG < n$. Then $C_{\Omega}(D, G)$ is an $[n, k, d]$ code with parameters*

$$k = n + g - 1 - degG \ , \ d \geq degG - (2g - 2).$$

PROOF. See theorem II.2.7 in [19]. ♢

Chapter 6

Quantum algebraic geometric codes

The following presentation is based on the paper *Asymptotically Good Quantum Codes* by A. Ashiknmin, S. Litsyn and M. A. Tsfasman [2].

Definition 6.1 Let $\theta \in (GF_q^*)^n$. For a code $C \subseteq GF_q^n$, we define

$$C_\theta^\perp = \{x \in GF(q)^n \mid \sum_{i=1}^{n} \theta_i x_i y_i = 0, \forall y \in C\}.$$

$\triangle$

Theorem 6.2 *If F is an algebraic function field over GF_q of genus g with at least $n' \geq 3g$ places of degree 1. Then for any $n \leq n'-g$, and for any $a = 2g-1, \ldots, \min\{n, n'/2+g/2-1\}$, there exists an $[n, k = n+g-1-a, d \geq a-2g+2]$-code C such that $C \supseteq C_\theta^\perp$ for some $\theta \in (GF_q^*)^n$.*

Moreover, if $q = 2^m, m \in \mathbf{N}$, there exists such a code with $C \supseteq C^\perp$.

PROOF. Let G be a positive divisor of degree a, i.e., $G \geq (0)$, and $\mathcal{P}' = \{P_1, \ldots, P_{n'}\}$ is the set of places in F of degree 1 such that $SuppG \cap \mathcal{P}' = \emptyset$. Set

$$D' = P_1 + \ldots, +P_{n'} \in \mathcal{D}_F.$$

Now let E be an effective divisor of degree $n' + g - 2 - 2a$, which implies that $a \leq n'/2 + g/2 - 1$. Define A to be $D' - 2G - E$, then for a canonical divisor W, we have $deg(W + A) = g$ be corollary 5.19. By theorem 5.15,

$$dim\Omega(-A) = dim(W + A).$$

By Riemann-Roch Theorem (theorem 5.18),

$$dim(W + A) = g + 1 - g + dim(W - A) \geq 1.$$

Therefore, $\exists$ nonzero $\omega_0 \in \Omega(-A)$.

Consider the map

$$\begin{aligned} \Omega(-A) &\rightarrow C_\Omega(D', D' - A) && (6.1)\\ \omega &\mapsto (\omega_{P_1}(1), \ldots, \omega_{P_{n'}}(1)). && (6.2) \end{aligned}$$

The kernel is $\Omega(2G + E)$. Let $\omega_{0P_{i_j}}(1) = 0$ for $\{P_{i_1}, \ldots, P_{i_m}\} \equiv \mathcal{P}_0$. Then

$$\omega_0 \in \Omega(2G + E - (D' - \sum_{j=1}^{m} P_{i_j})) = \Omega(-A + \sum_{j=1}^{m} P_{i_j}).$$

As $\omega_0 \neq 0$, by theorem 5.20, we must have

$$deg(-A + \sum_{j=1}^{m} P_{i_j}) \leq 2g - 2,$$

i.e.,

$$-(2 - g) + m \leq 2g - 2$$

which implies $m \leq g$.

Let $\mathcal{P} = \{P_1, \ldots, P_n\} \equiv \mathcal{P}' \backslash \mathcal{P}_0$. Then $n \geq n' - g$. Put $D = P_1 +, \ldots, +P_n \in \mathcal{D}_F$, we have $\omega_0 \in \Omega(2G + E - D)$. Define $\theta = (\omega_{0P_1}(1), \ldots, \omega_{0P_n}(1))$.

We consider

$$C = C_{\mathcal{L}}(D, G)^{\perp}_{\theta} = \{x \in GF_q^n \mid \sum_i \theta_i x_i y_i = 0, \forall y \in C_{\mathcal{L}}(D, G)\}.$$

For $x, y \in \mathcal{L}(G)$, we have

$$\begin{aligned} 0 &= \omega_0(xy) && (6.3)\\ &= \sum_{P \in \mathbf{P}_F} \omega_{0P}(xy) && (6.4)\\ &= \sum_{i=1}^{n} \omega_{0P_i}(xy) && (6.5)\\ &= \sum_{i=1}^{n} x(P_i) y(P_i) \omega_{0P_i}(1) && (6.6)\\ &= \sum_{i=1}^{n} x(P_i) y(P_i) \theta_i, && (6.7) \end{aligned}$$

where (6.3) and (6.5) follow from the fact that $\omega_o \in \Omega(2G + E - D)$ and $x, y \in \mathcal{L}(G)$; (6.4) follows from theorem 5.23; (6.6) follows from proposition 5.22.

Therefore, $C \supseteq C_{\mathcal{L}}(D, G)$. Also, $x \in C_\theta^\perp \Rightarrow x \in C_{\mathcal{L}}(D, G)^\perp \Rightarrow x \in C$. Hence, $C \supseteq C_\theta^\perp$.

If $q = 2^m$, any element in GF_q is a square. Let $\theta_i = \eta_i^2$. Consider the multiplication map

$$\begin{aligned} m_\eta : GF_q^n &\rightarrow GF_q^n & (6.8)\\ x &\mapsto (\eta_1 x_1, \ldots, \eta_n x_n). & (6.9) \end{aligned}$$

Define $C' = m_\eta(C)$ which will then contain its dual, i.e., $C' \supseteq C'^{\perp}$.

Now for $n \geq a \geq 2g-1$, by theorem 5.25 and 5.26, $C_{\mathcal{L}}(D,G)^{\perp} = C_\Omega(D,G)$ is a $[n, k = n+g-1-a, d \geq a-2g+2]$ linear code. The multiplication map $m_{\theta^{-1}}$ from $C_\Omega(D,G)$ to C is a isomorphism of vector spaces. Hence, C is a linear code with the same parameters.

Recalling the restrictions on a, i.e., $2g-1 \leq a \leq n'/2 + g/2 - 1$, we have $n' \geq 3g$. The theorem is then just a restatement of the previous discussion. ♢

Now, let us define $R = k/n$ and $\delta = d/n$ and do some analysis on them. First of all, by the previous theorem, we have for $n \leq n' - g$ and $2g-1 \leq a \leq \min\{n, n'/2 + g/2 - 1\}$,

$$\begin{aligned} R &= 1 - \frac{a+1+g}{n}, & (6.10)\\ \delta &= \frac{a-2g+2}{n}. & (6.11) \end{aligned}$$

From the equations, we see that R rises with the incease of n and with the decrease of a, while δ rises with the increase of a and with the decrease of n. Also, it is easily seen that $R + \delta = 1 - g/n$. Hence, for fixed δ, we should choose the maximum n available to maximize R. Therefore, we will always choose $n = n' - g$ from now on.

Applying theorem 6.2 to a families of algebraic function fields F's over GF_q, q a square, such that

$$\limsup_{g \to \infty} \frac{N(F)}{g(F)} = \sqrt{q} - 1,$$

where $N(F)$ is the number of places of degree one in F and $g(F)$ is the genus of F (for existence of such families, see [21, 6]), we get the following corollary:

Corollary 6.3 *Let q be an even power of a prime. Then for any*

$$\alpha \in \left(\frac{2}{\sqrt{q}-2} \ , \ \frac{1}{2} + \frac{1}{\sqrt{q}-2} \right)$$

there exists families of codes with asymptotic parameters

$$\begin{aligned} R &= 1 - \alpha + \frac{1}{\sqrt{q}-2}, & (6.12)\\ \delta &\geq \alpha - \frac{2}{\sqrt{q}-2}, & (6.13) \end{aligned}$$

with the property $C \supseteq C_\theta^{\perp}$ for some $\theta \in (GF_q^*)^n$.

It q is an even power of 2, there exists such codes with the property $C \supseteq C^{\perp}$.

PROOF. We have taken $n = n' - g$, so

$$R = \frac{n - a + g - 1}{n} \tag{6.14}$$

$$= 1 - \alpha + \frac{g}{n' - g} \tag{6.15}$$

$$= 1 - \alpha + \frac{1}{\sqrt{q} - 2}, \tag{6.16}$$

where α will lie in the prescribed range. The rest of the proof can be done by similar calculations. ♢

To use the generalized CSS construction, we need a triple $C' \supset C \supseteq C^{\perp}$. Therefore, we take two divisors $G' < G$, then $C_{\mathcal{L}}(D, G') \subset C_{\mathcal{L}}(D, G)$ and we have the opposite inclusion for duals. Taking $SuppG' \cup \mathcal{P} = \emptyset$, ω_0 can then remain the same. Therefore, we have proved the following:

Corollary 6.4 *Let $q = 2^{2m}$. Then for any pair of real numbers (α, α') such that*

$$\frac{2}{2^m - 2} \leq \alpha' < \alpha \leq \frac{1}{2} + \frac{1}{2^m - 2}$$

there exists families of triples of 2^2m-ary codes $C' \supset C \supseteq C^{\perp}$ with asymptotic parameters

$$R' = 1 - \alpha' + \frac{1}{2^m - 2} \ , \ \delta' \geq \alpha' - \frac{2}{2^m - 2}$$

$$R = 1 - \alpha + \frac{1}{2^m - 2} \ , \ \delta \geq \alpha - \frac{2}{2^m - 2}.$$

♢

By using all the machineries developed, we can now construct an asymptotically good quantum code Q and we will state how it can be done in a step by step manner.

Algorithm 6.5

1. Start with a family of algebraic function fields over $GF_{2^{2m}}$ with the property that
$$\lim_{g \to \infty} \frac{N(F)}{g(F)} = 2^m - 1.$$
Each algebraic function field will then give us a triple of 2^{2m}-ary codes $C' \supset C \supseteq C^{\perp}$.

2. Let C' and C be an $[n', k', d']$ code and an $[n, k, d]$ codes respectively. Binary expand C and $C^{\perp}$ with respect to a self-orthogonal basis to get a triple of binary codes $D' \supset D \supseteq D^{\perp}$ with parameters
$$n_{D'} = n_D = 2mn,$$
$$k_{D'} = 2mk' \ , \ k_D = 2mk,$$
$$d_{D'} \geq d' \ , \ d_D = d.$$

3. By the generalized CSS construction, each triple give us a quantum stabilizer code $[[2mn, 2m(k+k'-n), \geq \min\{d, d_2'\}]]$. The corresponding asymptotic parameters are

$$R_Q = R + R' - 1 \tag{6.17}$$

$$\delta_Q \geq \frac{1}{2m}\min\{\delta, \frac{3\delta'}{2}\} \tag{6.18}$$

where R, R', δ, δ' are the parameters of algebraic geometric $GF_{2^{2m}}$-ary codes.

△

Let us now try to find a dependence between R_Q and δ_Q. Letting $\gamma = \frac{1}{2^m-2}$. From the previous section, we see that for $q = 2^{2m}$ and for any pair of real numbers (α, α') such that $2\gamma \leq \alpha' < \alpha \leq \frac{1}{2} + \gamma$,

$$R_Q = 1 - (\alpha + \alpha') + 2\gamma \tag{6.19}$$

$$\delta_Q \geq \frac{1}{2m}\min\{\alpha - 2\gamma\ ,\ \frac{3}{2}(\alpha' - 2\gamma)\}. \tag{6.20}$$

For any fixed δ_Q, in order to maximize R_Q, we want $\alpha - 2\gamma = \frac{3}{2}(\alpha' - 2\gamma)$, i.e., $\alpha' = \frac{2}{3}(\alpha + \gamma)$. Hence,

$$R_Q = 1 - \frac{5}{3}\alpha + \frac{4}{3}\gamma \tag{6.21}$$

$$\delta_Q \geq \frac{1}{2m}(\alpha - 2\gamma). \tag{6.22}$$

Therefore, for any $m \geq 3$ and $\delta \leq \frac{1}{2m}(\frac{1}{2} - \frac{1}{2^m-2})$, we get

$$R_Q = 1 - \frac{2}{2^m - 2} - \frac{10}{3}m\delta_Q. \tag{6.23}$$

Immediately, we see that the asymptotic parameters of QAG codes are separated from zero and so they are asymptotically good as claimed.

Figure 6.1: Nonconstructive bound of equation 2.4 and the bound of equation 6.23.

Chapter 7

Examples

7.1 Rational function field

Definition 7.1 $F = K(x)$ where x is transcendental over K is called the *rational function field over* K. $\triangle$

Remark 7.2 $F = GF_q(x)$ has genus $g = 0$ and $q + 1$ places of degree one which are $\{P_\alpha \mid \alpha \in K\} \cup \{P_\infty\}$. Moreover, for $0 \leq degG \leq n-2$, $k = 1 + degG$ and $d = n - degG$. $\triangle$

Let $K = GF_q$ and $F = K(x)$. Following the previous chapter, we let $G = a \cdot P_\infty, a \in \mathbf{N}$ and $D = \sum_{\alpha \in K, \alpha \neq 0} P_\alpha$ with $degD = n = q-1$. Define $E = (n-2-2a) \cdot P_\infty$ and impose the condition that $a \leq n/2 - 1$ so that E is positive. We now set $A = D - 2G - E = \sum_{\alpha \in K, \alpha \neq 0} P_\alpha - (n-2) \cdot P_\infty$. If we choose as a basis for $\mathcal{L}(G)$ the functions $1, x, \ldots, x^a$ then the geometric Goppa code $C_\mathcal{L}(D, G)$ is given by matrix ζ^{ij} with ζ a primitive element of K. Classically, this code is called *Reed-Solomon code*. In the quantum case, we found an element $\theta \in C_\Omega(D, 2G + E) = C_\mathcal{L}(D, 2G + E)^\perp$. By theorem 6.2, $wt(\theta) = n$. We now consider the image of the multiplication map $m_\theta(C_\mathcal{L}(D, G))$ and its dual is equal to $C' := C_\mathcal{L}(D, G)^\perp_\theta$. We note that the dual code of a code can be easily found by Gaussian elimination on the generator matrix of the code. Again, by theorem 6.2, we get the following parameters for C':

$$n = q - 1 \ , \ k = q - 2 - a \ , \ d \geq a + 2$$

where $1 \leq a \leq \frac{q-1}{2} - 1$.

Now, we set $q = 2^m, m \in \mathbf{N}$ and we find η such that $\eta_i^2 = \theta_i$. Then we set $C = m_\eta(C')$ and we get $C \supseteq C^\perp$. We formulate the above discussion into the following proposition.

Proposition 7.3 *Let $F = GF_q(x)$ where x is transcendental over GF_q and $q = 2^m$, we have for any $1 \leq a' < a \leq \lfloor (2^m - 1)/2 - 1 \rfloor$, there exists an $[[m(2^m - 1), m(2^m - 3 - (a + a')), d \geq \min\{a + 2, \frac{3}{2}(a' + 2)\}]]$ quantum code Q.* $\diamondsuit$

We note that since the construction is similar to that of the classical Reed-Solomon codes, we may identify the codes found in proposition 7.3 as the *Quantum Reed-Solomon Codes*. We also remark that proposition 7.3 is an improvement of theorem 6 in [10].

We now want to consider another class of QAG codes which is the quantum analog of the classical *BCH codes*. Firstly, let $n|q-1$ and let $\zeta \in GF_q$ be a primitive n-th root of unity. We consider the rational function field $F = GF_q(x)$ and let $P_i := x - \zeta^{i-1}$ and $D := P_1 + \cdots + P_n$. We also define $G := a \cdot P_0 + b \cdot P_\infty$ with $0 \leq a, b \leq n-2$, and $E := (n-2-2(a+b)) \cdot P_\infty$ with $(a+b) \leq n/2-1$. We note that the generator matrix of $C_{\mathcal{L}}(D, a \cdot P_0 + b \cdot P_\infty)$ is given by

$$\begin{pmatrix} 1 & \zeta^{-a} & \zeta^{-2a} & \cdots & (\zeta^{n-1})^{-a} \\ 1 & \zeta^{-a+1} & \zeta^{-2a+2} & \cdots & (\zeta^{n-1})^{-a+1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \zeta^{-a+(a+b)} & \zeta^{-2a+2(a+b)} & \cdots & (\zeta^{n-1})^{-a+(a+b)} \end{pmatrix}. \tag{7.1}$$

Following previous exposition, we find η such that $\eta_i^2 = \theta_i$ where $\theta \in C_\Omega(D, 2G+E)$ and consider $C := m_\eta((m_\theta(C_{\mathcal{L}}(D,G))^\perp)$ which is a $[n, n-(a+b)-1, d \geq (a+b)+2]$-code containing its dual.

Then by binary expanding and using the Steane's construction, we get the following proposition.

Proposition 7.4 *Let $F = GF_q(x)$ where x is transcendental over GF_q, $q = 2^m$ and $n|q-1$, we have for any $0 \leq c' < c \leq n/2-1$, there exists an $[[mn, m(n-(c+c')-2), d \geq \min\{c+2, \frac{3}{2}(c'+2)\}]]$ quantum code Q.* ♢

We note that weakly self-dual BCH codes can also be used to construct quantum codes through Steane's construction, but their parameters are no better than those found in the previous proposition. Some more specific discussion on Quantum codes based on BCH codes can be found in [17, 9, 20].

7.2 Elliptic function field

Definition 7.5 An algebraic function field F/K (where K is the full constant field of F) is said to be an elliptic function field if the following conditions hold:
(1) the genus of F/K is 1;
(2) there exists a divisor $A \in \mathcal{D}_F$ with $degA = 1$. △

We consider an elliptic curve $\mathcal{E}$ defined by the equation:

$$y^2 + y = u(x)$$

where $u(x) \in GF_2[x]$ is a polynomial of degree 3.

We now consider the points on $\mathcal{E}$ over GF_q with $q = 2^m$. We follow [18] in this section and define a subset S of $\mathcal{E}(GF_q)$ to be

$$S := \{\alpha \in GF_q \mid (\alpha, \beta, 1) \in \mathcal{E}(GF_q), \alpha \neq 0\}.$$

Let $s = \#S$ and $d \in \mathbf{N}$ be such that $2s - d \geq 1$.

We now define $G := a \cdot P_\infty$ and $D := \sum_{\alpha \in S}(P_\alpha + \bar{P}_\alpha)$ where $P_\alpha := (\alpha, \beta, 1)$ and $\bar{P}_\alpha := (\alpha, \beta + 1, 1)$.

Set $l := \lfloor a/2 \rfloor$ and $l^* := \lfloor (a-3)/2 \rfloor$ and define a function f on E by

$$f(x, z) := \prod_{\alpha \in S}(x + \alpha z).$$

Defining

$$\omega_i := x^i z^{s-1-i} y \frac{dx}{f} \ , \ 0 \leq i \leq s - l - 2$$

$$\omega_j^* := x^j z^{s-j} \frac{dx}{f} \ , \ 0 \leq j \leq a - l^* - 2.$$

They then serve as a basis for $\Omega(D - G)$ and their residue can be calculated to be

$$Res_{P_\alpha}(x^l \frac{dx}{f}) = \frac{\alpha^l}{f'(\alpha)} \ , \ Res_{P_\alpha}(x^l y \frac{dx}{f}) = \frac{\alpha^l y(\alpha)}{f'(\alpha)}$$

where

$$f'(\alpha) = \prod_{\alpha' \in S, \alpha' \neq \alpha}(\alpha + \alpha').$$

The image of the following map is then a $[n, n - d, \geq d]_{2^m}$-code with $n = 2s$.

$$Res : \Omega(D - G) \to C_\Omega(D, G) \subset GF_q^n \tag{7.2}$$

$$\omega \mapsto (Res_{P_1}(\omega), \ldots, Res_{P_s}(\omega), Res_{\bar{P}_1}(\omega), \ldots, Res_{\bar{P}_s}(\omega)). \tag{7.3}$$

To find quantum codes, following the previous definition, we define

$$D' := \sum_{\alpha \in S}(P_\alpha + \bar{P}_\alpha) \tag{7.4}$$

$$G := a \cdot P_\infty \tag{7.5}$$

$$E := (2s - 1 - 2a) \cdot P_\infty. \tag{7.6}$$

We then find an element $\theta \in C_\Omega(D', 2G + E)$, it can have at most one component $= 0$. W.l.o.g., let the first component be zero, we then re-define $D := \sum_{\alpha \in S}(P_\alpha + \bar{P}_\alpha) - P_1$ and find $\eta \in GF_q^{n-1}$ such that $\eta_{i-1}^2 = \theta_i, 2 \leq i \leq n$. We now consider $m_\eta((m_\theta(C_\Omega(D, G))^\perp)$ which contains its dual by theorem 6.2. The parameters of the quantum code will then be

$$[[n = m(2s - 1) \ , \ k = m(2s - (a + a') - 1) \ , \ d \geq \min\{a, \frac{3a'}{2}\}]]$$

where $1 \leq a' \leq a \leq 2s - 1$.

7.3 Hermitian function field

Definition 7.6 The *Hermitian function field* H over GF_{q^2} is defined by the curve

$$x^{q+1} + y^{q+1} + z^{q+1} = 0.$$

$$H := GF_{q^2}(x, y) \text{ with } y^q + y = x^{q+1}.$$

△

Remark 7.7 The genus of H is $g = q(q-1)/2$. △

We shall show that H has $1 + q^3$ points in $\mathbf{P}^2(GF_{q^2})$. In fact, if x, y or $z = 0$, then w.l.o.g., assume $z = 0$ and $y = 1$ and we need to solve the equation $x^{q+1} = 1$ over GF_{q^2} which has $q + 1$ solutions. Therefore, H has $3(q + 1)$ points with $xyz = 0$. Otherwise, take $z = 1$ and $y \in GF_{q^2}^*$ such that $y^{q+1} \neq 1$. For each y, there are $r + 1$ solutions for x. Hence, H has $3(q + 1) + (q - 2)(q + 1)^2 = 1 + q^3$ points.

Choose $\alpha, \beta \in GF_q$ such that $\alpha^q + \alpha = \beta^{q+1} = -1$, and setting

$$u = \frac{\beta}{y - \beta x}\ ,\ v = xu - \alpha$$

we can transform

$$x^{q+1} + y^{q+1} + z^{q+1} = 0$$

to the equation

$$v^q + v = u^{q+1}.$$

We now take $G = a \cdot Q$ where $Q = (0, 1, 0)$ with $q^2 - q < a < q^3$, and $D = \sum_{P \in H, P \neq Q} P$. The classical Hermitian code $C_{\mathcal{L}}(D, G)$ is thus a $[q^3, a - g + 1, \geq q^3 - a]_{q^2}$-code. Also, we note that elements $v^i u^j$ with $i \geq 0, 0 \leq j \leq q - 1$ and $iq + j(q + 1) \leq a$ form a basis of the space $\mathcal{L}(a \cdot Q)$ and so the generator matrix can be found readily. Again by theorem 6.2, we have the following proposition.

Proposition 7.8 *Let H be a Hermitian function field over GF_{q^2} and $q = 2^m$, we have for any $q^2 - q \leq a' < a \leq q^3$, there exists an $[[2mq^3, 2m(q^3 + q^2 - q - 2 - (a + a')), d \geq \min\{a - q^2 + q + 2, \frac{3}{2}(a' - q^2 + q + 2)\}]]$ quantum code Q.* ♢

Similar to the case of BCH code, we may consider Hermitian code that is naturally self-dual. This situation is described by the next theorem.

Theorem 7.9 (a) *For $r \leq s$, we have $C_r \subseteq C_s$ where $C_r := C_{\mathcal{L}}(D, r \cdot Q)$.*

(b) $C_r^{\perp} = C_{q^3+q^2-q-2-r}$

(c) *If $q^2 - q - 2 \leq r \leq q^3 + q^2 - q - 2$. Then $k = r + 1 - q(q-1)/2$ and $d \geq q^3 - r$ where $k = dim C_r$ and d is the minimum distance of C_r.*

PROOF. See Propositions VII.4.2 and VII.4.3 in [19]. ♢

To construct quantum codes throught the Steane's method, we want classical codes C' and C such that $C' \supset C \supseteq C^{\perp}$. By theorem 7.9, we thus have the following corollary.

Corollary 7.10 *For $r, s \in \mathbf{Z}$ such that $\frac{1}{2}(q^3+q^2-q-2) \leq r < s \leq q^3+q^2-q-2$, we have $C_s \supset C_r \supset C_r^{\perp}$ where*

$$dimC_r = r + 1 - \frac{q(q-1)}{2} \ , \ d \geq q^3 - r$$

$$dimC_s = s + 1 - \frac{q(q-1)}{2} \ , \ d \geq q^3 - s.$$

♢

We now let $q = 2^m, m \in \mathbf{Z}$. By binary expanding the finite field GF_{q^2}, we have binary codes D' and D such that

$$n_{D'} = n_D = 2mq$$

$$k_{D'} = 2m(s+1-\frac{q(q-1)}{2}) \ , \ k_D = m(r+1-\frac{q(q-1)}{2})$$

$$d_{D'} = q^3 - s \ , \ d_D = q^3 - r,$$

for $\frac{1}{2}(q^3+q^2-q-2) \leq r < s \leq q^3+q^2-q-2$. Hence, by theorem 4.5, we have the following corollary.

Corollary 7.11 *Associated to the Hermitian function field H over GF_{q^2}, we have a family of quantum codes Q^H with parameters*

$$n = 2mq^3 \tag{7.7}$$

$$k = 2m(s+r+2-q^2+q)) - q^3 \tag{7.8}$$

$$d \geq \min\{q^3 - r, \frac{3}{2}(q^3 - s)\} \tag{7.9}$$

where $\frac{1}{2}(q^3+q^2-q-2) \leq r < s \leq q^3$. ♢

We now set $a := q^3+q^2-q-2-r$ and $a' := q^3+q^2-q-2-s$, we get the following family of codes:

$$[[2mq^3 \ , \ 2m(q^3+q^2-q-2-(a+a') \ , \ \geq \min\{a-q^2+q+2, \frac{3}{2}(a'-q^2+q+2\}]]$$

where $q^2-q-2 \leq a' < a \leq \frac{1}{2}(q^3+q^2-q-2)$.

Comparing thre result with proposition 7.8, we see that construction by Ashikhmin, Litsyn and Tsfasman is more general, but the weakly self-duality of Hermitian code does manage to improve the lower bound by 2.

Chapter 8

Conclusion

So we have succeed in finding some asymptotically good codes, but it seems that we should be able to do much better than what we have done. For instance, the parameters of QAG codes are still far from attaining the quantum lower bound in equation 2.4

$$R(\delta) \geq 1 - \delta \log_2 3 - H(\delta).$$

So as it is guaranteed that there are good codes that are even better than our QAG codes, why are we wasting time on QAG codes? The answer lies on the fact that the lower bound is nonconstructive. In other words, those imaginary codes appearing in the lower bound cannot be constructed in polynomial time in n while the QAG codes can be. In fact, recalling our three steps in algorithm 6.5, step (1) is polynomially constructible, see [21], step (2) is polynomially constructible because binary expansion is, step (3) is also polynomially constructible (c.f. section 3.3). Therefore, our QAG codes are polynomially constructible.

On the other hand, if we know improvement is possible, what should we go about in achieving that? First of all, if manipulation of spins (or other quantum quantities) in higher dimension is possible, we should try to generalise our QAG codes to higher dimension and it may improve their parameters. For instance, the Gilbert-Varshamov bound is achieved when $q \geq 49$ in the classical case. Secondly, in constructing QAG codes, we were basically converting classical algebraic-geometric codes to quantum ones through the Steane's construction. One may wonder if the theory of algebraic function fields could be applied directly to the quantum case without recuring to our classical counter part.

Some research has been done in the first direction [1, 3, 13], but it is still unclear about how to combine the techniques devised on higher dimensional quantum codes with the algebraic-geometric constructions. For the second direction, it may require another quantum leap in ideas of QECC constructions similar to the invention of CSS construction and the Steane's improvement on it.

Bibliography

[1] A. Ashikhmin and E. Knill, "Nonbinary Quantum Stabilizer Codes", quant-ph/0005008.

[2] A. Ashikhmin, S. Litsyn and M.A. Tsfasman, "Asymptotically Good Quantum Codes", Physical Review A **63**, 032311 (2001).

[3] J. Bierbrauer and Y. Edel, "Quantum twisted codes", available at http://www.math.mtu.edu/ jbierbra/.

[4] R. Cleve and D. Gottesman, "Efficient computations of encodings for quantum error correction", quant-ph/9607030.

[5] G. Cohen, S. Encheva and S. Litsyn, "On binary constructions of quantum codes", IEEE Transaction on Information Theory **45**, p.2495-2498 (1999).

[6] A. Garcia and H. Stichtenoth, "On the asymptotic behaviour of some towers of function fields over finite fields," Journal of Number Theory **61**, p.248-273 (1996).

[7] D. Gottesman, "Stabilizer Codes and Quantum Error Correction", quant-ph/9705052.

[8] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound", Physical Review A **54**, 1862 (1996).

[9] M. Grassl and T. Beth, "Quantum BCH Codes", quant-ph/9910060.

[10] M. Grassl, W. Geiselmann, T. Beth, "Quantum Reed-Solomon Codes", Lecture Notes in Computer Science **1719** (1999).

[11] T. Kasami and S. Lin, "The binary weight distribution of the extended $(2^m, 2^m - 4)$ code of the Reed-Solomon code over GF_{2^m} with generator polynomial $(x - \alpha)(x - \alpha^2)(x - \alpha^3)$", Linear Algebra and its Applications **98**, p.291 (1988).

[12] A. Lempel, "Matrix factorization over GF_2 and trace-orthogonal bases of GF_{2^n}", SIAM Journal on Computing **4**, p.175 (1975).

[13] R. Matsumoto and T. Uyematsu, "Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes", quant-ph/9911011.

[14] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[15] J. Preskill's Lecture notes is available at http://www.theory.caltech.edu/people/preskill/ph229/#lecture.

[16] Part III Quantum Information Theory lecture notes by Y. Suhov and O. Johnson is available at http://www.statslab.cam.ac.uk/ yms/.

[17] A.M. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes", IEEE Transaction on Information Theory **45**, p.2492 (1999).

[18] S.A. Stephanov, *Codes on Algebraic Curves*, (Kluwer Academic / Plenum Publishers, 1999).

[19] H. Stichtenoth, *Algebraic Function Fields and Codes*, (Springer-Verlag, 1993).

[20] A. Thangaraj, S. McLaughlin, "Quantum codes from cyclic codes over GF(4^m)", IEEE Transaction on Information Theory **47**, p.1176 (2000).

[21] M.A. Tsfasman and S.G. Vlăduţ, *Algebraic-Geometric Codes* (Kluwer Academic Publishers, 1991).