# Quantum Error Correcting Codes

Keqin Feng, Tsinghua University, Beijing 100084, China
(kfeng@math.tsinghua.edu.cn)

### Introduction

In the past half century, classical error-correcting codes has been developed, widely and deeply, into a huge body, effectively used in digit and network communication to check and correct errors in transmission channel, and demonstrated remarkable applications of pure mathematical branchs, such as number theory, algebra and algebraic geometry, in practical engineering fields. In the quantum case, error-correcting is also one of important requirements not only for quantum communication but also for quantum computing. There are at least the following reasons to make error-correcting in quantum case more critical than in classical case.

(1). Classsical information can be read, transcribed( into any medium) and duplicated at will. Quantum information, on the other hand, cannot be read or duplicated in general without being disturbed. Thus, for example, we cannot use "repeat" code to correct quantum information.

(2). An interaction of a quantum system with its environment can lead to the so-called decoherence effects and can greatly influence, or even completely destroy, subtle quantum mechanisms.

(3). In classical information processing, measurements usually remain original informations. But in quantum case any measurement likes a kind of noise in some sense since quantum informations would change their state after being measured.

(4). Digital informations have discrete and finite states (finite field $\mathbb{F}_q$), but quantum informations occupy continous states (complex number field $\mathbb{C}$).

These appear to make long reliable quantum computation or communication practically impossible and hopeless. A break-through came in 1995-96 with the pioneering paper of Shor[S95] and Steane[St96(1)] who reduce very complicated entangled errors into simple type of errors (Pauli operations $\sigma_x$, $\sigma_z$ and $\sigma_y$) acting on quantum informations bit-by-bit. Shor made the first quantum error-correcting code in physical way by using 9 quantum bits(qubits) to correct one-bit error. Soon after, Steane was able to reduce encoding message into 7 qubits. An optimal way to correct one qubit, by an entangled state of 5 qubits, was first shown by Laflamme et al.[LMPZ96] and Bennet et al.[BDSW96] in 1996. The first attempts to develop a methodology to design quantum codes in systematic and mathematical way were due to Calderbank and Shor [CS96] [CS97], Steane[St96(2)], Gottesman[G96] and

Calderbank et al. [CRSS97], [CRSS98] in 1996-1998. Particularly in [CRSS98], a neat and rigorous formation on quantum codes was established, and an effective mathematical method to construct nice quantum codes was presented by using character theory of finite abelian groups and symplectic geometry over finite fields which made it possible to construct quantum codes from classical codes over $\mathbb{F}_2$ or $\mathbb{F}_4$. Since then the parameters of constructed quantum codes improved rapidly by using classical Reed-Muller codes[ZF97], [St97], Reed-Solomon codes[CLX01], BCH codes[GB99] and algebraic-geometry codes[CL99], [C01]. At the same time, non-binary quantum codes were formulated[AK00], [K96(1)], [MU99], [SW00], [R99(1)]. It is to a large extent due to these remarkable works that the vision of real quantum computing and communication is much closer.

In this note, we introduce the basic mathematical conceptions on quantum error-correcting codes, main methods to construct quantum codes and some theoretical results in quantum code theory, a theory with six-year history.

§1 Classical error-correcting codes

§2 Quantum error-correcting codes

§3 Basic methods to construct quantum codes

§4 Weight enumerator and Singleton bound

§5 Non-binary case

## §1. Classical error-correcting codes

We start from a quick view of classical error-correcting codes since quantum codes have similar formulation as classical codes in many places and can be effectively constructed from classical codes. We just describe basic facts on classical codes we need in this note. For more detail see books[L82] or [MS77].

### §1.1. Three basic parameters of a code

**Definition1.1.1** *Let $\mathbb{F}_q$ be the finite field with $q$ elements. A code $C$ is defined just a subset of $\mathbb{F}_q^n$. A vector $v$ in $C$ is called a codeword. $n$ is called length, $K = |C|$(the size of $C$), $k = \log_q K$ is called the number of information digits in $C$. $\frac{k}{n}(\leq 1)$ is called transmition ratio which measure the effectivity of the code $C$.*

We have one more important parameter—minimal distance which measure the error-corecting ability of a code $C$.

**Definition1.1.2** *For a vector $v = (v_1, \cdots, v_n)$ in $\mathbb{F}_q^n$ we define the Hamming weight of $v$ by*

$$w_H(v) = \sharp\{1 \leq i \leq n \ |v_i \neq 0\}.$$

*The Hamming distance of two vectors $u = (u_1, \cdots, u_n)$ and $v = (v_1, \cdots, v_n) \in \mathbb{F}_q^n$ is defined by*

$$d_H(u, v) = \sharp\{1 \leq i \leq n \ |u_i \neq v_i\} = w_H(u - v).$$

In this section we simply denote $d_H$ and $w_H$ by $d$ and $w$, but after section 2 we should use $d_H$ and $w_H$ in order to distinguish from quantum weight $w_Q$.

The Hamming distance is really a "mathematical" distance since it satisfies the following basic properties. For $u,\ v,\ w \in \mathbb{F}_q^n$,

(H1) $d(u, v) \geq 0$; and $d(u, v) = 0 \Longleftrightarrow u = v$.

(H2) $d(u, v) = d(v, u)$.

(H3) (The triangle inequality) $d(u, w) \leq d(u, v) + d(v, w)$.

**Definition1.1.3** *Let $C$ be a code over $\mathbb{F}_q$ with length $n$ ($C \subseteq \mathbb{F}_q^n$). The minimal distance of $C$ is defined by*

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

The following result shows that the minimal distance $d(C)$ is the proper parameter to judge the ability of code $C$ to check and correct digital errors.

**Basic theorem1.1.4** *Let $C$ be a code with minimal distance $d = d(C)$. The code $C$ can check $\leq d - 1$ digital errors and correct $\leq [\frac{d-1}{2}]$ digital errors.*

**<u>Proof</u>** Alice send a codeword $c \in C$ to Bob, but has error vector $e \in \mathbb{F}_q^n$ with $1 \leq w(e) \leq d-1$ so that Bob receives vector $y = c + \varepsilon,\ y \neq c$. By definition of $d = d(C)$ we know that $d(c, c') \geq d$ for each codeword $c' \in C,\ c' \neq c$. Now $d(c, y) = w(y - c) = w(\varepsilon) \leq d - 1$. Thus $y$ is not codeword so that Bob find $y$ has errrors.

Moreover, if $w(\varepsilon) \leq [\frac{d-1}{2}]$, then $d(c, y) = w(\varepsilon) \leq [\frac{d-1}{2}]$ and $d(c', y) \geq d(c', c) - d(c, y) \geq d - [\frac{d-1}{2}] > [\frac{d-1}{2}]$ for any $c' \in C,\ c' \neq c$. This means that $c$ is the unique codeword most closer to received $y$. With this way $y$ can be decoded to $c$ correctly.

$\square$

Now we have introduced the basic parameters of a code $C:\ n,\ k(\text{or}K)$ and $d$. We denote this code $C$ over $\mathbb{F}_q$ by $(n,\ K,\ d)_q$ or $[n,\ k,\ d]_q$. A good code should have big values of $\frac{k}{n}$ and $d$. But there are some restrictions, or bounds between parameters.

**<u>Theorem1.1.5</u>** *(Hamming bound) Let $C$ be a code $(n,\ K,\ d)_q$, and $l = [\frac{d-1}{2}]$. Then*

$$q^n \geq K \sum_{i=0}^{l} (q-1)^i \binom{n}{i} \qquad (1.1)$$

**<u>Proof</u>** For $v \in \mathbb{F}_q^n$ and integer $r (0 \leq r \leq n)$, let $S_r(v)$ be the (closed) ball with center $v$ and radius $r$.

$$S_r(v) = \{u \in \mathbb{F}_q^n |\ d(u, v) \leq r\}$$

The size of the ball is $|S_r(v)| = \sum\limits_{i=0}^{r} (q-1)^i \binom{n}{i}$. By the triangle inequality and $2l = 2[\frac{d-1}{2}] < d$ we know that all balls $\{S_l(c) | c \in C\}$ are disjoint to each others. Thus

$$q^n = |\mathbb{F}_q^n| \geq \sum_{c \in C} |S_l(c)| = K \cdot \sum_{i=0}^{l} (q-1)^i \binom{n}{i}. \qquad \square$$

**<u>Definition1.1.6</u>** *A code $(n,\ K,\ d)_q$ is called perfect if (1.1) becomes equality*

$$q^n = K \sum_{i=0}^{l} (q-1)^i \binom{n}{i}.$$

**Example1.1.7** Consider the following binary code $C$ in $\mathbb{F}_2^7$

$$C = \left\{ \begin{array}{c} (0010111),\ (1101000) \\ (1001011),\ (0110100) \\ (1100101),\ (0011010) \\ (1110010),\ (0001101) \\ (0111001),\ (1000110) \\ (1011100),\ (0100011) \\ (0101110),\ (1010001) \\ (0000000),\ (1111111) \end{array} \right\}$$

This is a code $(7,16,3)_2$ or $[7,4,3]_2$. Since $l=1$ and $2^7=2^4(1+\binom{7}{1})$, $C$ is a perfect code.

In order to construct good codes and to have practical decoding algorithm we need to consider codes with more algebraic structures.

## §1.2. Linear codes

**Definition1.2.1** *A code $C$ in $\mathbb{F}_q^n$ is called linear if $C$ is a $\mathbb{F}_q$-subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$.*

Let $k=\dim_{\mathbb{F}_q} C$. Then $K=|C|=q^k$ and $k=\log_q K$ so that $\dim_{\mathbb{F}_q} C$ is the number of information digits of $C$. For the minimal distance of a linear code we have the following result.

**Lemma1.2.2** *For a linear code $C$,*

$$d(C)=\min\{w(c)|c\in C,\ c\neq 0\}$$

**Proof** We denote the right-hand side by $d'$. Then there exist $0\neq c\in C$ such that $w(c)=d'$. Since $C$ is linear so that $0\in C$, $d'=w(c)=d(c,0)\geq d(C)$. On the other hand, we have $c,c'\in C,\ c\neq c'$ such that $d(C)=d(c,c')=w(c-c')$. Since $C$ is linear so that $0\neq c-c'\in C$. Thus $d(C)=w(c-c')\geq d'$. Therefore $d(C)=d'$. $\square$

Let $C$ be a linear code $[n,\ k,\ d]_q$. $C$ is a $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$ with $\dim_{\mathbb{F}_q} C=k$. We may choose a $\mathbb{F}_q$-basis $\{u_1,\cdots,u_k\}$ of $C$

$$u_i=(a_{i_1},\ a_{i_2},\ \cdots,\ a_{i_n})\quad (1\leq i\leq k)\ (a_{i_j}\in\mathbb{F}_q)$$

Each codeword $c\in C$ can be expressed uniquely by

$$\begin{aligned} c &= b_1u_1+b_2u_2+\cdots+b_ku_k \qquad (b_i\in\mathbb{F}_q)\\ &= (b_1,\cdots,b_k)G \end{aligned}$$

where

$$G=\begin{bmatrix} u_1\\ u_2\\ \vdots\\ u_k\end{bmatrix}=\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ a_{k1} & a_{k2} & \cdots & a_{kn}\end{vmatrix}$$

is called a generating matrix of the linear code $C$. $G$ is a $k\times n$ matrix over $\mathbb{F}_q$ with $rank_{\mathbb{F}_q} G=k$. On the other hand, by linear algebra, any subspace $C$ of $\mathbb{F}_q^n$ with dimension $k$ is the intersection of $n-k$ hyperplanes in $\mathbb{F}_q^n$. Namely,there exist $(n-k)\times n$ matrix over $\mathbb{F}_q$ with $rank=n-k$

$$H = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_{n-k} \end{bmatrix} = \begin{vmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n-k,1} & b_{n-k,2} & \cdots & b_{n-k,n} \end{vmatrix} \quad (b_{i_j} \in \mathbb{F}_q)$$

such that for $c = (c_1, c_2, \cdots, c_n) \in \mathbb{F}_q^n$

$$\begin{aligned} c \in C \quad &\Leftrightarrow \quad v_i c^\top = \sum_{\lambda=1}^{n} b_{i\lambda} c_\lambda = 0 \in \mathbb{F}_q \quad (1 \le i \le n-k) \\ &\Leftrightarrow \quad Hc^\top = 0 \in \mathbb{F}_q^{n-k} \end{aligned}$$

$H$ is called a parity-check matrix of the linear code $C$ since for any vector $c$ in $\mathbb{F}_q^n$ one can check if $c$ is a codeword in the linear code $C$ by computing $Hc^T$. Moreover, the parity-check matrix can be used to determine (or design) the minimal distance of a linear code.

**Lemma1.2.3** *Let $C$ be a $[n,\ k,\ d]$ $(d \ge 2)$ linear code over $\mathbb{F}_q$, $H$ be a parity-check $(n-k) \times n$ matrix of $C$. Then*

*(1) Any $d-1$ distinct column vectors are $\mathbb{F}_q$-linear independent.*

*(2) There are $d$ distinct column vectors which are $\mathbb{F}_q$-linear dependent.*

**Proof** Let $H = [w_1, w_2, \cdots, w_n]$ where $w_1, \cdots, w_n$ are column vectors in $\mathbb{F}_q^{n-k}$. For each vector $c = (c_1, c_2, \cdots, c_n) \in \mathbb{F}_q^n$, $w_H(c) = l$, $c_{j_1},\ c_{j_2},\ \cdots,\ c_{j_l} \ne 0$ and $c_j = 0$ for $j \ne j_1,\ \cdots,\ j_l$. Then we have

$$c \in C \Leftrightarrow 0 = Hc^\top = [w_1, w_2, \cdots, w_n] \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = c_{j_1} w_{j_1} + \cdots + c_{j_l} w_{j_l}$$

Therefore a codeword in $C$ with length $l$ corresponds $l$ linear dependent columns in $H$. The conclution of lemma1.2.3 follows from this. $\square$

**Example1.2.4**(Hamming codes) Consider the following matrix over $\mathbb{F}_2$

$$H_3 = \begin{bmatrix} 1001011 \\ 0101110 \\ 0010111 \end{bmatrix}$$

The 7 columns of $H_3$ are just all non-zero vectors in $\mathbb{F}_2^3$. Let $C_3$ be the binary linear code with parity-check matrix $H_3$.

$$C_3 = \{c \in \mathbb{F}_2^7 | Hc^\top = 0\}$$

The code length of $C_3$ is $n = 7$. $k = \dim_{\mathbb{F}_2} C_3 = n - rankH_3 = 7 - 3 = 4$. Since the columns of $H_3$ are distinct, any two columns of $H_3$ are linear independent. There are three columns in $H$ are linear dependent. By lemma1.2.3, $d = d(C_3) = 3$.

Therefore $C_3$ is a binary $[7, 4, 3]$ linear code. In fact, $C_3$ is just the binary code in example1.1.7. Similarly, for each integer $t \geq 3$, let $H_t$ be the $t \times (2^t - 1)$ matrix over $\mathbb{F}_2$ such that the $2^t - 1$ columns of $H_t$ are all non-zero vectors in $\mathbb{F}_2^t$. Let $C_t$ be the binary linear code with parity-check matrix $H_t$. Then $C_t$ is a binary code $[n,\ k,\ d] = [2^t - 1,\ 2^t - 1 - t,\ 3]$. All binary codes $C_t (t \geq 3)$ are perfect, called binary Hamming codes.

For linear codes we have the following bound.

**Theorem1.2.5** *(Singleton bound for linear codes) For a linear code $[n,\ k,\ d]_q$ we have $d \leq n - k + 1$.*

**Proof** Let $H$ be the parity-check matrix of a linear code $[n,\ k,\ d]_q$. The size of $H$ is $(n-k) \times n$ and $rank_{\mathbb{F}_q} H = n-k$. Thus there exist $n-k$ $\mathbb{F}_q$-linear independent columns in $H$. On the other hand, any $n-k+1$ distinct columns of $H$ are $\mathbb{F}_q$-linear dependent. By lemma1.2.3 we know that $d = d(C) \leq n-k+1$. □

A linear code which reaches the Singleton bound ($d = n - k + 1$) is called MDS(maximal distance separable) code. It is easy to see that a linear code $C$ is MDS code if and only if any $n - k$ distinct columns of its parity-check matrix are linear independent.

**Definition1.2.6** *Let $C$ be a linear code $[n,\ k,\ d]$ over $\mathbb{F}_q$. The subset of $\mathbb{F}_q^n$*

$$C^{\perp} = \{v \in \mathbb{F}_q^n | (c, v) = 0 \ for\ all\ c \in C\}$$

*is also a linear code over $\mathbb{F}_q$ where, for $c = (c_1, c_2, \cdots, c_n)$ and $v = (v_1, v_2, \cdots, v_n) \in \mathbb{F}_q^n$, $(c, v)$is the inner product*

$$(c, v) = cv^{\top} = \sum_{i=1}^{n} c_i v_i \in \mathbb{F}_q.$$

*$C^{\perp}$ is called the dual code of $C$. if $C \subseteq C^{\perp}$ then $C$ is called self-orthogonal. Let $v_1,\ \cdots,\ v_k$ be a basis of a linear code $C$. Then $C$ is self-orthogonal if and only if $v_i (1 \leq i \leq k)$ are orthogonal to each other: $v_i v_j^{\top} = 0 \in \mathbb{F}_q (1 \leq i, j \leq k)$.*

**Lemma1.2.7** *Let $C$ be a $[n,\ k]_q$ linear code. Then*
*(1)$C^{\perp}$ is a $[n,\ n-k]_q$ linear code: $\dim_{\mathbb{F}_q} C^{\perp} = n - dim_{\mathbb{F}_q} C$.*
*(2)$(C^{\perp})^{\perp} = C$.*
*(3)A generating (parity-check) matrix of $C$ is a parity-check(generating) matrix of $C^{\perp}$.*

## §1.3. Weight enumerator and MacWilliams identity

**Definition1.3.1** *Let $C$ be a $[n,\ k]_q$ linear code. For each $i (0 \leq i \leq n)$, let $A_i$ be the number of $c \in C$ with $w(c) = i$. The weight enumerator of $C$ is defined by*

$$f_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i \ \in Z[x, y].$$

It is easy to see that $A_0 = 1,\ A_0 + A_1 + \cdots + A_n = |C| = q^k$ and $d(C)$ is the smallest positive integer $d$ such that $A_d \geq 1$.

**Theorem1.3.2** *(MacWilliams Identity) Let $C$ be a $[n,\ k]_q$ linear code and $C^{\perp}$ be the dual code of $C$. Then*

$$f_{C^{\perp}}(x, y) = q^{-k} f_C(x + (q-1)y, x - y).$$

There are many proofs of theorem1.3.2. We choose one proof by using the additive character of $\mathbb{F}_q^n$ since these characters are also used to construct quantum codes in section 3. We list basic definitions and facts on character theory of finite abelian groups. For proofs and more details see [L82] or[LN86].

**Definition1.3.3** *An character of a finite abelian group $G = (G, +)$ is a homomorphism $\chi :\ G \to \mathbb{C}^*$ from $G$ to the multiplicative group $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ of non-zero complex numbers. Namely, for $g_1, g_2 \in G$, we have $\chi(g_1 + g_2) = \chi(g_1)\chi(g_2)$.*

Let $m = |G|$. Then for each $g \in G,\ g^m = 1$ and $\chi(g)^m = \chi(g^m) = \chi(1) = 1$. Thus all $\chi(g)(g \in G)$ are $m$-th root of 1. We denote the trivial character(mapping all $g \in G$ to 1) by 1. Let $\hat{G}$ be the set of all characters of $G$. For $\chi_1, \chi_2 \in \hat{G}$, the mapping $\chi_1\chi_2$ defined by $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$, and $\bar{\chi_1}$ defined by $\bar{\chi_1}(g) = \overline{\chi_1(g)} = \chi_1(g)^{-1}$ are also characters of $G$ and $\bar{\chi_1}\chi_1 = 1$. In this way we make $\hat{G}$ as abelian group, called the character group of $G$.

It is easy to see by the structure theorem of finite abelian groups that two groups $G$ and $\hat{G}$ are isomorphic. Particularly, $|G| = |\hat{G}|$. One more thing we need is the orthogonal relations between characters.

**Lemma1.3.4** *Let $G$ be a finite abelian group. Then*

*(1)For $\chi \in \hat{G}$,*

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & , \quad if\ \chi = 1 \\ 0 & , \quad otherwise \end{cases}$$

*(2)For $g \in G$,*

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} |G| & , \quad if\ g = 1 \\ 0 & , \quad otherwise \end{cases}$$

Now we determine the character group $\widehat{\mathbb{F}_q^n}$ of the additive group $\mathbb{F}_q^n$. Let $q = p^m$ where $p$ is a prime number and $m \geq 1$. We introduce the trace mapping

$$T : \mathbb{F}_q \to \mathbb{F}_p, \quad T(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{m-1}} \quad (\alpha \in \mathbb{F}_q)$$

It is well known that $T$ is a surjective homomorphism from additive group $\mathbb{F}_q$ to additive group $\mathbb{F}_p$.

**Theorem1.3.5** *Let* $\zeta = e^{\frac{2\pi i}{p}}$ *and* $T : \mathbb{F}_q \to F_p$ *be the trace mapping*($q = p^m$)*. For each* $a = (a_1, a_2, \cdots, a_n) \in \mathbb{F}_q^n$ ($a_i \in \mathbb{F}_q$)*, the mapping*

$$\lambda_a : \mathbb{F}_q^n \to \{1, \zeta, \cdots, \zeta^{p-1}\} \subseteq \mathbb{C}^*$$
$$\lambda_a(b) = \lambda_a(b_1, \cdots, b_n) = \zeta^{T(a \cdot b)} = \zeta^{T(a_1 b_1 + \cdots + a_n b_n)} \quad (b = (b_1, \cdots, b_n) \in \mathbb{F}_q^n)$$

*is a character of the additive group* $\mathbb{F}_q^n$*. And* $\widehat{\mathbb{F}_q^n} = \{\lambda_a | a \in \mathbb{F}_q^n\}$*.*

**Lemma1.3.6** *Let* $C$ *be a* $\mathbb{F}_q$*-linear subspace of* $\mathbb{F}_q^n$*. For* $v \in \mathbb{F}_q^n$*,*

$$\sum_{u \in C} \lambda_u(v) = \begin{cases} |C| & , \ if\ v \in C^{\perp} \\ 0 & , \ otherwise \end{cases}$$

Now we can prove theorem1.3.2. For each $u = (u_1, u_2, \cdots, u_n) \in \mathbb{F}_q^n$ ($u_i \in \mathbb{F}_q$), we define a polynomial

$$g_u(z) = \sum_{v \in \mathbb{F}_q^n} \lambda_u(v) z^{w(v)} \quad \in C[z]$$

where $w(v) = w_H(v)$ is the Hamming weight of $v$, and $\lambda_u(v) = \zeta^{T(u \cdot v)}$ is an additive character of $\mathbb{F}_q^n$. Then

$$\begin{aligned} g_u(z) &= \sum_{v_1, \cdots, v_n \in \mathbb{F}_q} \zeta^{T(u_1 v_1 + \cdots + u_n v_n)} z^{w(v_1) + \cdots + w(v_n)} \qquad (w(v_i) = \begin{cases} 0 & , \ if\ \ v_i = 0 \\ 1 & , \ if\ \ v_i \in \mathbb{F}_q^* \end{cases}) \\ &= (\sum_{v_1 \in \mathbb{F}_q} \zeta^{T(u_1 v_1)} z^{w(v_1)}) \cdots (\sum_{v_n \in \mathbb{F}_q} \zeta^{T(u_n v_n)} z^{w(v_n)}) \end{aligned}$$

For $u = 0$ ($w(u) = 0$) we have

$$\sum_{v \in \mathbb{F}_q} \zeta^{T(uv)} z^{w(v)} = \sum_{v \in \mathbb{F}_q} z^{w(v)} = 1 + (q-1)z \tag{1}$$

and for $u \neq 0$ ($w(u) = 1$) we have

$$\begin{aligned} \sum_{v \in \mathbb{F}_q} \zeta^{T(uv)} z^{w(v)} &= 1 + \sum_{v \in \mathbb{F}_q^*} \zeta^{T(uv)} z^{w(v)} = 1 + \sum_{v \in \mathbb{F}_q^*} \zeta^{T(uv)} z \\ &= 1 + (\sum_{v \in \mathbb{F}_q^*} \zeta^{T(v)}) z = 1 + (\sum_{v \in \mathbb{F}_q^*} \lambda_1(v)) z = 1 - z \end{aligned} \tag{2}$$

(1) and (2) can be put together as

$$g_u(z) = (1-z)^{w(u)} (1 + (q-1)z)^{n - w(u)}$$

Thus

$$\begin{aligned}
\sum_{u\in C} g_u(z) &= \sum_{u\in C} (1-z)^{w(u)}(1+(q-1)z)^{n-w(u)} \\
&= \sum_{i=0}^{n} A_i(1+(q-1)z)^{n-i}(1-z)^i \qquad (3)
\end{aligned}$$

On the other hand,

$$\begin{aligned}
\sum_{u\in C} g_u(z) &= \sum_{u\in C}\sum_{v\in\mathbb{F}_q^n} \lambda_u(v) z^{w(v)} = \sum_{v\in\mathbb{F}_q^n} z^{w(v)} \sum_{u\in C} \lambda_u(v) \\
&= q^k \sum_{v\in C^\perp} z^{w(v)} \qquad (by \ \ lemma\ 1.3.6) \\
&= q^k \sum_{i=0}^{n} A_i^\perp z^i
\end{aligned}$$

Therefore

$$\begin{aligned}
f_{C^\perp}(x,y) &= x^n \sum_{i=0}^{n} A_i^\perp (\tfrac{y}{x})^i = x^n q^{-k} \sum_{u\in C} g_u(\tfrac{y}{x}) \\
&= x^n q^{-k} \sum_{i=0}^{n} A_i(1+(q-1)\tfrac{y}{x})^{n-i}(1-\tfrac{y}{x})^i \qquad (by\ (3)) \\
&= q^{-k} \sum_{i=0}^{n} A_i(x+(q-1)y)^{n-i}(x-y)^i \\
&= q^{-k} f_C(x+(q-1)y, x-y).
\end{aligned}$$

This complets the proof of theorem1.3.2. □

## §2 Quantum Error-Correcting Codes

### §2.1. Quantum bits and quantum codes

In digital communication a bit is an element in finite field $\mathbb{F}_q$. A $n$-bit is a vector in $\mathbb{F}_q^n$. In quantum communication a quantum bit (qubit) and $n$-qubit are objects in vector space over complex number field $\mathbb{C}$.

**Definition2.1.1** *A qubit is a non-zero vector in $\mathbb{C}^2$. Physicians usually denote a $\mathbb{C}$-basis of $\mathbb{C}^2$ by $|0>$ and $|1>$. Thus a qubit $|v>$ can be expressed by*

$$|v>= \alpha|0> +\beta|1> \quad (\alpha, \beta \in \mathbb{C},\ (\alpha,\beta) \neq (0,0)).$$

A $n$-qubit is a non-zero vector in the tensor product space $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$. We usually choose the following $\mathbb{C}$-basis of $\mathbb{C}^{2^n}$:

$$\{|a_0a_1\cdots a_{n-1}>=|a_0>\otimes|a_1>\otimes\cdots\otimes|a_{n-1}>:\ (a_0,\cdots,a_{n-1})\in\mathbb{F}_2^n\}$$

Thus a $n$-qubit can be expressed by

$$(0\neq)|v>= \sum_{(a_0,\cdots,a_{n-1})\in\mathbb{F}_2^n} c_{a_0,\cdots,a_{n-1}}|a_0,\cdots,a_{n-1}>=\sum_{a\in\mathbb{F}_2^n} c_a|a>$$

where $c_a \in \mathbb{C}$. We have the Hermitian inner product in $\mathbb{C}^{2^n}$: for

$$|v>=\sum_{a\in\mathbb{F}_2^n} c_a|a> \text{ and } |u>=\sum_{a\in\mathbb{F}_2^n} b_a|a> \quad (c_a, b_a \in \mathbb{C})$$

the Hermitian inner product of $|v>$ and $|u>$ is defined by

$$<u|v>=\sum_{a\in\mathbb{F}_2^n} \overline{b_a}c_a \in \mathbb{C}.$$

If $<u|v>=0$, $|v>$ and $|u>$ are called to be orthogonal.

There is one thing in quantum physics which is different from classical case. In digit communication, two $n$-digits $u=(u_0,\cdots,u_{n-1})$ and $v=(v_0,\cdots,v_{n-1})\in\mathbb{F}_q^n$ are distinct if $u\neq v$(namely, if there is $i, 1\leq i\leq n$ such that $u_i\neq v_i$). In quantum case, for two $n$-qubit $|u>$ and $|v>$,

(I)If $|u>=\alpha|v>$ for some $\alpha\in\mathbb{C}^*=\mathbb{C}\backslash\{0\}$, $|u>$ and $|v>$ are considered as the same quantum state.

(II)$|u>$ and $|v>$ are distinguishable(=totally distinct) if $<u|v>=0$.

**Definition2.1.2** *A quantum code $Q$ is just a subspace of $(\mathbb{C}^2)^{\otimes n}=\mathbb{C}^{2^n}$. $n$ is called the length of the code $Q$. We denote $K=\dim_{\mathbb{C}} Q$ and $k=\log_2 K$ so that $k\leq n$.*

## §2.2. quantum error group

A quantum error on $\mathbb{C}^{2^n}$ is an unitary $\mathbb{C}$-linear operator acting on $\mathbb{C}^{2^n}$ bit by bit. Since each qubit $|v>=\alpha|0>+\beta|1>$ is a vector in $\mathbb{C}^2$, a quantum error can be expressed by unitary matrix with respect to the basis $|0>$ and $|1>$. There are three basic errors (Pauli matrices) acting on qubit:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_x|v>=\beta|0>+\alpha|1>, \quad \sigma_x \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}, \quad (\textit{bit error})$$
$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_z|v>=\alpha|0>-\beta|1>, \quad \sigma_z \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}, \quad (\textit{phase error})$$
$$\sigma_y = i\sigma_x\sigma_z = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_y|v>=-i\beta|0>+i\alpha|1>, \quad \sigma_y \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -i\beta \\ i\alpha \end{pmatrix},$$
$$(I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I|v>=|v>, \quad \textit{no error})$$

Among them there are following relations:

$$\sigma_x^2 = \sigma_z^2 = \sigma_y^2 = I, \quad \sigma_x\sigma_z = -\sigma_z\sigma_x.$$

A quantum error operation acting on $(\mathbb{C}^2)^{\otimes n}$ has following form:

$$e = i^\lambda w_0 \otimes w_1 \otimes \cdots \otimes w_{n-1}$$

where $i = \sqrt{-1}, \ \lambda \in \{0,1,2,3\}, w_i \in \{I, \sigma_x, \sigma_y, \sigma_z\}, \ (0 \le i \le n-1)$ is $\mathbb{C}$-linear unitary operator acting on basis element $|a>=|a_0>\otimes|a_1>\otimes\cdots\otimes|a_{n-1}> \ (a = (a_0, \cdots, a_{n-1}) \in \mathbb{F}_2^n)$ of $\mathbb{C}^{2^n}$ by

$$e|a>=i^\lambda(w_0|a_0>)\otimes(w_1|a_1>)\otimes\cdots\otimes(w_{n-1}|a_{n-1}>).$$

The set of quantum error operators

$$E_n = \{i^\lambda w_0 \otimes w_1 \otimes \cdots \otimes w_{n-1} | 0 \le \lambda \le 3, \ w_i \in \{I, \sigma_x, \sigma_y, \sigma_z\}, \ (0 \le i \le n-1)\}$$

is a finite non-abelian group ($|E_n| = 4^{n+1}$) where for $e = i^\lambda w_0 \otimes w_1 \otimes \cdots \otimes w_{n-1}$ and $e' = i^{\lambda'} w'_0 \otimes w'_1 \otimes \cdots \otimes w'_{n-1}$

$$ee' = i^{\lambda\lambda'}(w_0w'_0)\otimes(w_1w'_1)\otimes\cdots\otimes(w_{n-1}w'_{n-1}).$$

<u>**Example**</u> $(n=2)$. For $e = I_2 \otimes \sigma_x, \ e = \sigma_y \otimes \sigma_z$,

$$ee' = \sigma_y \otimes (\sigma_x\sigma_z) = i^3\sigma_y \otimes \sigma_y, \quad e'e = \sigma_y \otimes (\sigma_z\sigma_x) = i\sigma_y \otimes \sigma_y.$$

It is easy to see that the center of the group $E_n$ is

$$C(E_n) = \{i^\lambda = i^\lambda(I_2 \otimes \cdots \otimes I_2) | 0 \le \lambda \le 3\}.$$

Let $\overline{E_n} = E_n/C(E_n)$. Then $|\overline{E_n}| = 4^n$. Since $ee' = \pm e'e$ for any $e, e' \in E_n$, we know that the quotient group $\overline{E_n}$ is an abelian 2-elementary group ($\bar{e}^2 = 1$ for each $\bar{e} \in \overline{E_n}$). Therefore $\overline{E_n}$ should be isomorphic to the additive group $\mathbb{F}_2^{2n}$.

Now we give $e = i^{\lambda} w_0 \otimes w_1 \otimes \cdots \otimes w_{n-1}$ a new expression

$$e = i^{\lambda+l} X_{(a)} Z_{(b)} \quad (a = (a_0, \cdots, a_{n-1}),\ b = (b_0, \cdots, b_{n-1}) \in \mathbb{F}_2^n)$$

where

$$(a_i, b_i) = \begin{cases} (0,0) & if \quad w_i = I_2 \\ (1,0) & if \quad w_i = \sigma_x \\ (0,1) & if \quad w_i = \sigma_z \\ (1,1) & if \quad w_i = \sigma_y (= i\sigma_x\sigma_z) \end{cases}$$

and $l = \sharp\{0 \leq i \leq n-1 | w_i = \sigma_y\}$. Therefore

$$X_{(a)} = w'_0 \otimes w'_1 \otimes \cdots \otimes w'_{n-1} \quad , \quad w'_i = \begin{cases} I_2, & if \quad a_i = 0 \\ \sigma_x & if \quad a_i = 1 \end{cases}$$
$$Z_{(b)} = w''_0 \otimes w''_1 \otimes \cdots \otimes w''_{n-1} \quad , \quad w''_i = \begin{cases} I_2, & if \quad b_i = 0 \\ \sigma_z & if \quad b_i = 1 \end{cases}$$

From $\sigma_y = i\sigma_x\sigma_z$ we know that $i^{\lambda} w_0 \otimes w_1 \otimes \cdots \otimes w_{n-1} = i^{\lambda+l} X_{(a)} Z_{(b)}$. The following result shows advantage of this new notation.

**Lemma2.2.1** *(1) The action of $X_{(a)}$ and $Z_{(b)}$ $(a, b \in \mathbb{F}_2^n)$ on the basis $|v>= |v_0 v_1 \cdots v_{n-1}>$ $(v \in \mathbb{F}_2^n)$ of $\mathbb{C}^{2^n}$ are*

$$X_{(a)}|v>= |a+v>, \qquad Z_{(b)}|v>= (-1)^{b \cdot v}|v>$$

*(2) For $e = i^{\lambda} X_{(a)} Z_{(b)}$ and $e' = i^{\lambda'} X_{(a')} Z_{(b')}$ in $E_n$,*

$$ee' = (-1)^{a \cdot b' + a' \cdot b} e'e$$

**Proof** (1)By definition $\sigma_x|0>= |1>$ and $\sigma_x|1>= |0>$. Since $X_{(a)} = w_0 \otimes w_1 \otimes \cdots \otimes w_{n-1}$ where

$$w_i = \begin{cases} I_2, & if \quad a_i = 0 \\ \sigma_x & if \quad a_i = 1 \quad (0 \leq i \leq n-1) \end{cases}$$

We know that $w_i|v_i>= |v_i + a_i>$ and $X_{(a)}|v>= |a+v>$.

Similarly, $Z_{(b)} = w_0 \otimes w_1 \otimes \cdots \otimes w_{n-1}$ where

$$w_i = \begin{cases} I_2, & if \quad b_i = 0 \\ \sigma_z & if \quad b_i = 1 \end{cases}$$

From $\sigma_z|0>= |0>$ and $\sigma_z|1>= -|1>$ we know that $w_i|v_i>= (-1)^{b_i v_i}|v_i>$ and $Z_{(b)}|v>= (-1)^{b \cdot v}|v>$.

(2) For each basis element $|v>$ $(v \in \mathbb{F}_2^n)$,

$$\begin{aligned} ee'|v> &= i^{\lambda+\lambda'} X_{(a)} Z_{(b)} X_{(a')} Z_{(b')} |v> \\ &= (-1)^{b' \cdot v} i^{\lambda+\lambda'} X_{(a)} Z_{(b)} X_{(a')} |v> \\ &= (-1)^{b' \cdot v} i^{\lambda+\lambda'} X_{(a)} Z_{(b)} |v+a'> \\ &= (-1)^{b' \cdot v + b \cdot (v+a')} i^{\lambda+\lambda'} X_{(a)} |v+a'> \\ \\ &= (-1)^{b' \cdot v + b \cdot (v+a')} i^{\lambda+\lambda'} |v+a+a'> \end{aligned}$$

Similarly

$$e'e|v> = (-1)^{b \cdot v + b' \cdot (v+a)} i^{\lambda+\lambda'} |v+a+a'>$$

Therefore $ee' = (-1)^{a \cdot b' + a' \cdot b} e'e$. □

For $e = i^{\lambda} X_{(a)} Z_{(b)} \in E_n$, the image of $e$ in $\overline{E_n} = E_n / C(E_n)$ is denoted by

$$\bar{e} = (a|b) \quad (a, b \in \mathbb{F}_2^n)$$

Then for $e' = i^{\lambda'} X_{(a')} Z_{(b')}$, $\bar{e'} = (a'|b')$,

$$\bar{e}\bar{e'} = \overline{ee'} = \overline{i^{\lambda+\lambda'}(-1)^{a \cdot b' + a' \cdot b} X(a+a') Z(b+b')} = (a+a'|b+b') (= \bar{e'}\bar{e})$$

This shows that $\overline{E_n}$ is natually isomorphic to additive group $\mathbb{F}_2^{2n}$. Moreover, by lemma2.2.1(2) we know that

$$ee' = e'e \Leftrightarrow (-1)^{a \cdot b' + a' \cdot b} = 1 \Leftrightarrow a \cdot b' + a' \cdot b = 0 \in \mathbb{F}_2 \qquad (*)$$

We introduce the symplectic inner product $(\ ,\ )_s$ in $\mathbb{F}_2^{2n}$: for $(a|b)$ and $(a'|b') \in \mathbb{F}_2^{2n}$,

$$((a|b), (a'|b'))_s = a \cdot b' + a' \cdot b = (a, b) \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} \begin{pmatrix} a' \\ b' \end{pmatrix} \in \mathbb{F}_2$$

For a subspace $C$ of $\mathbb{F}_2^{2n}$, the symplectic dual of $C$ is defined by the subspace

$$C_s^{\perp} = \{v \in \mathbb{F}_2^{2n} | (v, c)_s = 0 \quad for \quad all \quad c \in C\}$$

We have $\dim_{\mathbb{F}_2} C_s^{\perp} + \dim_{\mathbb{F}_2} C = 2n$ and $(C_s^{\perp})^{\perp} = C$. If $C \subseteq C_s^{\perp}$, this subspace is called symplectic self-orthogonal. From formula(*) we have the following result.

**<u>Lemma2.2.2</u>** *Let $S$ be a subgroup of $E_n$. Then $S$ is abelian if only if $\bar{S}$ is a symplectic self-orthogonal subspace of $\overline{E_n} = \mathbb{F}_2^{2n}$.*

## §2.3. Quantum error-correcting

**<u>Definition2.3.1</u>** *The quantum weight of an error*

$$e = i^{\lambda} w_0 \otimes w_1 \otimes \cdots \otimes w_{n-1} = i^{\lambda'} X_{(a)} Z_{(b)} \quad \bar{e} = (a|b)$$

$$(w_i \in \{I, \sigma_x, \sigma_y, \sigma_z\},\ a = (a_0, \cdots, a_{n-1}),\ b = (b_0, \cdots, b_{n-1}) \in \mathbb{F}_2^n)$$

*is defined by*

$$\begin{aligned} w_Q(e) = w_Q(\bar{e}) &= \sharp\{0 \leq i \leq n-1 | a_i = 1 \ or\ b_i = 1\} \\ &= \sharp\{0 \leq i \leq n-1 | w_i \neq I_2\} \end{aligned}$$

*which is just the number of qubits having errors. For* $0 \leq l \leq n$*, let*

$$E_n(l) = \{e \in E_n | W_Q(e) \leq l\}, \quad \overline{E_n}(l) = \{\bar{e} \in \overline{E_n} | W_Q(\bar{e}) \leq l\}$$

*Then* $|E_n(l)| = 4 \cdot \sum\limits_{i=0}^{l} 3^i \binom{n}{i}, \qquad |\overline{E_n}(l)| = \sum\limits_{i=0}^{l} 3^i \binom{n}{i}.$

Now we are ready to describe the ability to correct quantum errors for a quantum code $Q \subseteq \mathbb{C}^{2^n}$. In classical case, both of error $e = (e_1, \cdots, e_n)$ and codeword $c = (c_1, \cdots, c_n)$ are subjects in $\mathbb{F}_q^n$, an error $e$ acts on a codeword by addition $e + a \in \mathbb{F}_q^n$. For a code $C$ in $\mathbb{F}_q^n$, $C$ can correct $l$ errors means that $C$ satisfies the following condition.

If $c_1, c_2 \in C,\ c_1 \neq c_2$(distinct), and $e_1, e_2 \in \mathbb{F}_q^n,\ w_H(e_1) \leq l,\ w_H(e_2) \leq l$, then $c_1 + e_1 \neq c_2 + e_2$(distinct).

For quantum case, quantum code $Q \subseteq \mathbb{C}^{2^n}$ and quantum error $e \in E_n$ are different subjects. $e$ is an unitary $\mathbb{C}$-linear operator acting on $|v> \in Q$ by $e|v> \in \mathbb{C}^{2^n}$. Remember that the conception "distinct" in classical case corresponds to the conception "distinguishable" in quantum case. We have following definition.

**<u>Definition2.3.2</u>** *A quantum code* $Q \subseteq \mathbb{C}^{2^n}$ *can correct* $\leq l$ *quantum errors* $(0 \leq l \leq n)$ *means that* $Q$ *satisfies the folloing condition.*

*If* $|v_1>, |v_2> \in Q,\ <v_1|v_2> = 0$*(distinguishable), and* $e_1, e_2 \in E_n(l)$*, then* $<v_1|e_1 e_2|v_2> = 0$ *(*$e_1|v_1>$ *and* $e_2|v_2>$ *are distinguishable).*

*A quantum code* $Q$ *is called to have minimal distance* $d$ *means that* $Q$ *satisfies the following condition.*

*If* $|v_1>, |v_2> \in Q,\ <v_1|v_2> = 0$*, and* $e \in E_n(d-1)$*, then* $<v_1|e|v_2> = 0$*.*

Since $w_Q(ee') \leq w_Q(e) + w_Q(e')$ for any $e, e' \in E_n$, it is obvious from the definitions that we have following result.

**<u>Lemma2.3.3</u>** *Let* $d$ *be the minimal distance of a quantum code* $Q$*,* $l = [\frac{d-1}{2}]$*. Then* $Q$ *can correct* $\leq l$ *quantum errors.*

Similar to the classical case, a quantum code $Q$ in $\mathbb{C}^{2^n}$ has three basic parameters: the length $n$, dimension $K = \dim_{\mathbb{C}} Q$ (or $k = \log_2 K$) and the minimal distance $d$.

We denote this quantum code $Q$ by $((n,\ K,\ d))$ or $[[n,\ k,\ d]]$. We also have bounds related to the parameters of a quantum code $Q$ which are analogue to the classical Hamming bound and Singleton bound.

Before introducing the quantum Hamming bound, one difference between classical and quantum cases should be indicated. Let $C$ be a classical code $(n,\ K,\ d)_q$. Namely, $C$ is a subset of $\mathbb{F}_q^n$ with $|C| = K$ and minimal distance $d$. For $l = [\frac{d-1}{2}]$, the sets $e + C$ $(w_H(e) \leq l)$ are disjoint to each others. Therefore we obtain the Hamming bound

$$q^n = |\mathbb{F}_q^n| \geq \sum_{\substack{e \\ w_H(e) \leq l}} |e + C| = |C| \cdot \sum_{\substack{e \\ w_H(e) \leq l}} 1 = K \cdot \sum_{i=0}^{l} (q-1)^i \binom{n}{i}.$$

But in quantum case, for a quantum code $Q$ with parameters $((n,\ K,\ d))$, $eQ$ is a subspace of $\mathbb{C}^{2^n}$ for any quantum error $e \in E_n$ since $Q$ is a subspace and $e$ is a linear operator of $\mathbb{C}^{2^n}$. $Q$ can correct $\leq l$ quantum errors, but this does not imply that the subspaces $\{\bar{e}Q\}(w_H(\bar{e}) \leq l)$ are orthogonal to each other. The reason is that even for $e \neq 1$ $(w_Q(e) \geq 1)$ a codeword $|v> \in Q$ can be fixed by $e:\ e|v> = \alpha|v>$ $(\alpha \in \mathbb{C}^*)$ ($|v>$ is an eigenvector of $e$) so that $eQ \cap Q \neq (0)$.

<u>**Definition2.3.4**</u> *Let $Q$ be a quantum code with minimal distance $d$. $l = [\frac{d-1}{2}]$. If the subspace $\bar{e}Q$ $(w_H(\bar{e}) \leq l)$ of $\mathbb{C}^{2^n}$ are orthogonal to each others, $Q$ is called to be pure.*

<u>**Lemma2.3.5**</u> *(Quantum Hamming bound) For a pure quantum code $((n,\ K,\ d))$, $l = [\frac{d-1}{2}]$, we have*

$$2^n \geq K \sum_{i=0}^{l} 3^i \binom{n}{i}$$

<u>**Proof**</u>

$$2^n = \dim_{\mathbb{C}} \mathbb{C}^{2^n} \geq \sum_{\bar{e} \in \overline{E_n}(l)} \dim(\bar{e}Q) = \dim Q \cdot |\overline{E_n}(l)| = K \cdot \sum_{i=0}^{l} 3^i \binom{n}{i}. \qquad \square$$

We will introduce the quantum Singleton bound in section4.

## §3 Basic Methods to Constructing Quantum Codes

### §3.1. Stabilizer quantum codes

In this section we describe the mathematical method to construct quantum codes introduced in [CRSS98] and its variations. The idea of the method is as follows. Firstly we choose an abelian subgroup $G$ of $E_n$. Such abelian subgroup $G$ comes from a symplectic self-orthogonal code $C$ in $\mathbb{F}_2^{2n}$ ($C \subseteq C_s^{\perp}$) by lemma2.2.2. Then the action of $G$ on $\mathbb{C}^{2^n}$ make $\mathbb{C}^{2^n}$ as a direct sum of $\chi$-eigenspaces $Q(\chi)$ ($\chi \in \hat{G}$). For each subspace $Q = Q(\chi)$, $k = n - \log_2 |G|$ and its minimal distance can be determined by certain properties of $C$ and $C_s^{\perp}$. In this way, nice quantum code $Q$ can be obtained from classical code $C$.

We need a little of representation theory of a finite abelian group. Let $G$ be a finite abelian group acting on a finite-dimensional $\mathbb{C}$-vector space $V$. Each $g \in G$ is a $\mathbb{C}$-linear operator of $V$ and for $g, g' \in G$,

$$(gg')(v) = g(g'v), \quad gg^{-1}(v) = 1(v) \quad (v \in V)$$

where $1 \in G$ is the identity operator on $V$.

Let $\hat{G}$ be the character group of $G$. For each character $\chi \in \hat{G}$, we define a linear operator over $V$

$$e_\chi = \frac{1}{\mid G \mid} \sum_{g \in G} \bar{\chi}(g) g$$

Usually $\{e_\chi \mid \chi \in \hat{G}\}$ is called the system of orthogonal primitive idempotent operators. Their orthogonal and idempotent properties can be justified by following lemma:

**Lemma3.1.1** *(1). $e_\chi^2 = e_\chi$ and $e_\chi e_{\chi'} = 0$ if $\chi \neq \chi'$.*
*(2). $1 = \sum_{\chi \in \hat{G}} e_\chi$;*
*(3). For any $g \in G$, $\quad g e_\chi = \chi(g) e_\chi$.*

**Proof** (1).By the orthogonal property of characters and $\bar{\chi} = \chi^{-1}$,

$$\begin{aligned} e_\chi e_{\chi'} &= \frac{1}{|G|^2} \sum_{g \in G} \bar{\chi}(g) g \cdot \sum_{h \in G} \overline{\chi'}(h) h \ (\text{let } gh = a) \\ &= \frac{1}{|G|^2} \sum_{a, g \in G} \bar{\chi}(g) \overline{\chi'}(a g^{-1}) a \\ &= \frac{1}{|G|^2} \sum_{a \in G} \overline{\chi'}(a) a \cdot \sum_{g \in G} (\bar{\chi}\chi')(g) \\ &= \begin{cases} 0, & \text{if } \ \bar{\chi}\chi' \neq \chi_0 (\Leftrightarrow \chi \neq \chi') \\ \frac{1}{|G|} \sum_{a \in G} \bar{\chi}(a) a = e_\chi & \text{if } \ \chi = \chi' \end{cases} \end{aligned}$$

(2). $\sum_{\chi \in \hat{G}} e_\chi = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \sum_{g \in G} \bar{\chi}(g) g = \frac{1}{|G|} \sum_{g \in G} g \sum_{\chi \in \hat{G}} \bar{\chi}(g) = 1.$

(3). $g e_\chi = \sum_{h \in G} \bar{\chi}(h) gh = \sum_{a \in G} \bar{\chi}(a g^{-1}) a = \chi(g) \sum_{a \in G} \bar{\chi}(a) a = \chi(g) e_\chi.$ $\square$

**Lemma3.1.2** *Suppose that a finite abelian group $G$ act on a finite-dimensional complex vector space $V$ such that each $y \in G$ is a Hermitian linear operator. For each $\chi \in \hat{G}$ we denote*

$$V(\chi) = e_\chi V = \{e_\chi(v) | v \in V\}$$

*(1) For $v \in V(\chi)$ ,$g \in G$ we have*

$$gv = \chi(g)v$$

*Therefore $V(\chi)$ is a common eigenspace for all Hermitian operator $g \in G$.*

*(2) We have the following direct decomposition of $V$.*

$$V = \bigoplus_{\chi \in \hat{G}} V(\chi)$$

*Which means that each $v \in V$ has unique expression $v = \sum_{\chi \in \hat{G}} v(\chi)$, $v(\chi) \in V(\chi)$. Moreover, if all $g \in G$ are unitary linear operators on $V$, then $V(\chi)$ and $V(\chi')$ are hermitian-orthogonal for all $\chi,\ \chi' \in \hat{G},\ \chi \neq \chi'$.*

**Proof** (1).For $v \in V(\chi),\ g \in G$, we have

$$\begin{aligned} gv &= ge_\chi(w) \quad (for\ some\ w \in V) \\ &= \chi(g)e_\chi(w) = \chi(g)v \end{aligned}$$

(2). For each $v \in V$,

$$v = \left(\sum_{\chi \in \hat{G}} e_\chi\right) v = \sum_{\chi \in \hat{G}} v_\chi$$

where $v_\chi = e_\chi v \in V(\chi)$. On the other hand, if we have $v = \sum_{\chi \in \hat{G}} u_\chi$, $u_\chi \in V(\chi)$, Then $u_\chi = e_\chi w_\chi$ for some $w_\chi \in V$. By orthogonal property of $\{e_\chi\}$ we know that for each $\chi \in \hat{G}$,

$$\begin{aligned} v_\chi &= e_\chi v = e_\chi(\sum_{\chi' \in \hat{G}} u_{\chi'}) = e_\chi(\sum_{\chi' \in \hat{G}} e_{\chi'} w_{\chi'}) \\ &= \sum_{\chi' \in \hat{G}} (e_\chi e_{\chi'} w_{\chi'}) = e_\chi w_\chi = u_\chi \end{aligned}$$

Therefore we proved that $V = \bigoplus_{\chi \in \hat{G}} V(\chi)$. The last statement is a well-known fact in linear algebra. □

Let us back to the case that $G$ is an abelian subgroup of $E$ and $G \cong (\mathbb{F}_2^k,\ +)$. $G$ has a basis:

$$\{g_j = i^{\lambda_j} X(a_j)Z(b_j) | 1 \leq j \leq k\} \quad (a_j, b_j \in \mathbb{F}_2^n)$$

where $\lambda_j \in Z_4$ such that $\lambda_j \equiv a_j b_j \pmod 2$ . Since $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are Hermitian, we know that $X(a_j)$ and $Z(b_j)$ are Hermitian, so that

$$\begin{aligned} g_j^\dagger = \bar{g}_j^\top &= (-i)^{\lambda_j} Z(b_j)^T X(a_j)^T = (-i)^{\lambda_j} Z(b_j) X(a_j) \\ &= i^{\lambda_j}(-1)^{a_j b_j} \cdot (-1)^{a_j b_j} X(a_j) Z(b_j) \\ &= i^{\lambda_j} X(a_j) Z(b_j) = g_j \end{aligned}$$

Which means that $g_j$ $(1 \le j \le k)$ are Hermitian. Since $G$ is abelian group generated by $g_j$ $(1 \le j \le k)$, we know that all $g \in G$ are Hermitian linear operators acted on $\mathbb{C}^{2^n}$. By theorem3.1.2, we have direct decomposition

$$\mathbb{C}^{2^n} = \bigoplus_{\chi \in \hat{G}} Q(\chi).$$

where $Q(\chi)$ is the $\chi$-eigenspace of $G$:

$$Q(\chi) = e_\chi \mathbb{C}^{2^n} = \{v \in \mathbb{C}^{2^n} | gv = \chi(g)v \text{ for all } g \in G\}$$

After these preparations, now we can state and prove the most important result in this lecture note.

**<u>Theorem3.1.3</u>** *Suppose that $C$ is a self-orthogonal subspace of $\mathbb{F}_2^{2n}$ with respect to the symplective inner product $< \, , \, >_s$, $\dim C = k$. Let*

$$\begin{aligned} C_s^\perp &= \{u \in \mathbb{F}_2^{2n} | < u, v >= 0 \ for \ all \ v \in C\} \\ d &= w_Q(C_s^\perp \backslash C) = \min\{w_Q(v) | v \in \ C_s^\perp \backslash C\} \end{aligned}$$

*Then there exits $[[n, n-k, d]]$ quantum code.*

**<u>Proof</u>** As we are shown before ,$\bar{G} = C$ can be lifted to an abelian subgroup $G$ of $E$. And $G \cong \mathbb{F}_2^k$ . Then $\mathbb{C}^{2^n} = \bigoplus_{\chi \in \hat{G}} Q(\chi)$ where

$$Q(\chi) = e_\chi \mathbb{C}^{2^n} = \{v \in \mathbb{C}^{2^n} | gv = \chi(g)v \ \text{ for } \ \text{all } g \in G\}.$$

We want to show that each $Q(\chi)$ is a $[[n, n-k, d]]$ quantum code.

First of all, we show $\dim_{\mathbb{C}} Q(\chi) = 2^{n-k}$ for any $\chi \in \hat{G}$. For doing this we consider the actions of $E$ on the set $\{Q(\chi) | \chi \in \hat{G}\}$. For any $|v >\in Q(\chi)$, and $g \in G$, $g|v >= \chi(g)|v >$,$(\chi(g) \in C)$. Thus for any $e \in E$

$$g|e|v >= ge|v >= (-1)^{<\bar{g},\bar{e}>} eg|v >= (-1)^{<\bar{g},\bar{e}>} \chi(g) e|v \quad (\forall g \in G)$$

It is easy to see that:

$$\chi_{\bar{e}} : G \ \rightarrow \ \{\pm 1\} \subseteq \mathbb{C}^*, \ \chi_{\bar{e}}(g) = (-1)^{<\bar{g},\bar{e}>}$$

is a character of $G$. Thus we have:

$$g|e|v>=\chi_{\bar{e}}(g)\chi(g)e|v>=\chi'(g)e|v> \quad (\forall g\in G)$$

which means that $e|v>\in Q(\chi')$ and $e:\ Q(\chi)\to Q(\chi')$, where $\chi'=\chi_{\bar{e}}\cdot\chi$. Since $E$ is a group we know that $e$ is bijective so that $\dim_{\mathbb{C}} Q(\chi)=\dim_{\mathbb{C}} Q(\chi')$. When $e$ runs through $E$, $\chi_{\bar{e}}$ can take all characters of $G$. This implies that all $\dim_{\mathbb{C}} Q(\chi)$,$(\chi\in\hat{G})$ are the same . Let $N$ be this common dimension, then

$$2^n=\dim\mathbb{C}^{2^n}=\sum_{\chi\in\hat{G}}\dim Q(\chi)=\sum_{\chi\in\hat{G}}N=N\cdot|\hat{G}|=N|G|=N\cdot 2^k$$

therefore $\dim Q(\chi)=N=2^{n-k}$ for all $\chi\in\hat{G}$.

Next we show $d(Q(\chi))\geq w_Q(C_s^{\perp}\backslash C)$. For doing this we need to show that for each $e\in E_{d-1}$, $v_1,v_2\in Q(\chi)$, $<v_1|v_2>=0$, then $<v_1|e|v_2>=0$.

(1). If $\bar{e}\in\bar{G}=C$, then $<v_1|e|v_2>=\chi(\bar{e})<v_1|v_2>=0$.

(2). Otherwise, $\bar{e}\notin C$. From $w_Q(\bar{e})=w_Q(e)\leq d-1$, and the assumption $(C_s^{\perp}\backslash C)\cap\overline{E_{d-1}}=\Phi$, we know that $\bar{e}\notin C_s^{\perp}$, which means that there exists $\bar{e'}\in\bar{G}$ such that $ee'=-e'e$. Then for $v_2\in Q(\chi)$,

$$e'e|v_2>=-ee'|v_2>=-\chi(e')e|v_2>,\quad -\chi(e')\neq\chi(e'),$$

Therefore $e|v_2>\in Q(\chi')$, where $\chi'\neq\chi$. Since $v_1\in Q(\chi)$ and $Q(\chi)$ is orthogonal to $Q(\chi')$, we have $<v_1|e|v_2>=0$. This completes the proof of theorem. □

**<u>Definition3.1.4</u>**: *The quantum code constructed by theorem3.1.3 are called stabilizer or additive quantum codes.*

It is easy to see that such quantum code is pure (definition2.3.4) if $C\cap\overline{E_{d-1}}=(0)$.

**<u>Example</u>** For $n=5,k=1,d=3$, we have $2^{n-k}=16=(1+3\cdot 5)=\sum_{i=0}^{1}3^i\binom{5}{i}$. Therefore $[[5,1,3]]$ additive quantum code is perfect if it exists. Such quantum code has been found by Calderbank and Shor[CS96], Gottesman[G96] and Laflamme et.al[LMPZ96] as the first perfect quantum code in the world.

Consider a subspace (= classical binary linear code) $C$ of $\mathbb{F}_2^{10}$ with generating matrix:

$$\left[\begin{array}{ccccc|ccccc} 1&1&0&0&0&0&0&1&0&1\\ 0&1&1&0&0&1&0&0&1&0\\ 0&0&1&1&0&0&1&0&0&1\\ 0&0&0&1&1&1&0&1&0&0 \end{array}\right]=\left[\begin{array}{c} v_1\\ v_2\\ v_3\\ v_4 \end{array}\right] \qquad (1)$$

where, for example, the first row vector $v_1$ means $(a|b)$ with $a=(11000), b=(00101)$. It can be checked that $v_1,v_2,v_3,v_4$ are linear independent over $\mathbb{F}_2$ and orthogonal with respect to the symplectic product $<,>$. Therefore $\dim C=4$ and

$C$ is self-orthogonal. $C_s^\perp \supseteq C$ and $\dim C_s^\perp = 10 - 4 = 6$ , so we need two more vectors in $C_s^\perp$ to make a basis of $C_s^\perp$ with $v_1, v_2, v_3, v_4$. In this way we find

$$C_s^\perp = C \oplus (00000|11111)\mathbb{F}_2 \oplus (11111|00000)\mathbb{F}_2.$$

It can be calculated that $w_Q(C) = 4$ and $w_Q(C_s^\perp) = 3$ (for $(11000|00101)+(11111|00000) = (00111|00101) \in C_s^\perp$ and $w_Q(00111|00101) = 3$ ). Therefore $w_Q(C_s^\perp \backslash C) = 3$ and the quantum code $Q(\chi)$ constructed by $C$ is pure. Since $2n = 10$, $k = n - \dim C = 5 - 4 = 1$, $d = 3$. We know that $Q(\chi)$ is $[[n, k, d]] = [[5, 1, 3]]$ quantum code.

Let us write down the code $Q = Q(\chi_0)$ explicitly where $\chi_0$ is the trivial character of $G$. Recall that $G$ is generated by

$$g_j = i^{\lambda_j} X(a_j) Z(b_j) \quad (1 \leq j \leq 4)$$

While $v_j = (a_j|b_j)$, $\lambda_j \in Z_4$ and $\lambda_j \equiv a_j \cdot b_j \pmod 2$ . It is easy to see from(1) that $a_j \cdot b_j = 0 \in \mathbb{F}_2$ $(1 \leq j \leq 4)$ So we may choose $\lambda_j = 0$ for all $j$ ,$1 \leq j \leq 4$. Therefore

$$\begin{aligned}
G &= < g_1, g_2, g_3, g_4 > \\
&= \{1, g_2, g_3, g_4, g_1g_2, \cdots, g_3g_4, g_1g_2g_3, \cdots, g_2g_3g_4, g_1g_2g_3g_4\} \quad |G| = 16 \\
g_1 &= X(11000)Z(00101) = \sigma_x \otimes \sigma_x \otimes \sigma_z \otimes I_2 \otimes \sigma_z. \\
g_2 &= X(01100)Z(10010) = \sigma_z \otimes \sigma_x \otimes \sigma_x \otimes \sigma_z \otimes I_2. \\
g_3 &= \cdots, \; g_4 = \cdots.
\end{aligned}$$

Since $k = 1$ and $\dim_C Q = 2^k = 2$, we need to find two vector in $\mathbb{C}^{2^n} = C^{32}$ as a basis of $Q$. Since

$$Q = Q(\chi_0) = \{v \in C^{32} | gv = \chi_0(g)v = v \text{ for all } g \in G\}$$

which means that $Q$ consists of the fixed vector by all $g \in G$. It is natural to consider the "average" of a vector $|v> \in C^{32}$ ,

$$|\overline{v>} = \sum_{h \in G} h|v> .$$

Since for each $g \in G$, $g|\overline{v>} = g \sum_{h \in G} h|v> = \sum_{h \in G} (gh)|v> = \sum_{h \in G} h|v> = |\overline{v>}$, thus $|\overline{v>} \in Q$. Then we try $|v> = |00000>$ and $|11111>$ to compute

$$\begin{aligned}
|v_0> &= \sum_{h \in G} h|00000> \\
&= X(00000)Z(00000)|00000> + \sum_{j=1}^{4} g_j|00000> + \sum_{1 \leq i < j \leq 4} g_i g_j |00000> \\
&\quad + \sum_{1 \leq i < j < k \leq 4} g_i g_j g_k |00000> + g_1g_2g_3g_4|00000> \\
&= |00000> \; +(|11000> + |01100> + |00110> + |00011> + |10001>) \\
&\qquad -(|10100> + |01010> + |00101> + |10010> + |01001>) \\
&\qquad +(|11110> + |01111> + |10111> + |11011> + |11101>)
\end{aligned}$$

by using $X(a)|v >= |v+a>$ and $Z(b)|v >= (-1)^{b\cdot v}|v>$. For example:

$$\begin{aligned} g_1g_2 &= X(11000)Z(00101)X(01100)Z(10010) \\ &= X(11000)X(01100)Z(00101)Z(10010)\cdot(-1)^{(00101)\cdot(01100)} \\ &= -X(10100)Z(10111), \end{aligned}$$

Therefore

$$\begin{aligned} g_1g_2|00000> &= -X(10100)Z(10111)|00000 >= -X(10100)|00000> \\ &= -|10100>. \end{aligned}$$

$$\begin{aligned} |v_1> &= \sum_{h\in G} h|11111> \\ &= |11111> \ +(|00111>+|10011>+|11001>+|11100>+|01110>) \\ &\qquad -(|01011>+|10101>+|11010>+|01101>+|10110>) \\ &\qquad -(|00001>+|10000>+|01000>+|00100>+|00010>). \end{aligned}$$

$|v_0>$ and $|v_1>$ is independent, therefore the quantum code $Q$ generated by $|v_0>$ and $|v_1>$ is 2-dimensional and can correct any error ($\sigma_x,\ \sigma_z,\ or\ \sigma_y$) in any one qubit of its five qubits.

### §3.2. From classical codes to quantum codes

The theorem3.1.3 presents a general principle to construct quantum codes from $\chi$-eigenspaces of an abelian subgroup $G$ of $E$ acts on $\mathbb{C}^{2^n}$. Such a group $G$ comes from a binary self-orthogonal linear code $C$ of the symplectic space $\mathbb{F}_2^{2n}$. Therefore theorem3.1.3 establishes a connection between classical binary codes and quantum codes. In this subsection we specify this general connection to give several concrete methods which make it possible to construct quantum codes from known classical binary codes.

**Theorem3.2.1** ([CRSS98]) *Suppose there exists a binary $[n,\ k,\ d]$ linear code and $C \supseteq C^{\perp}$ where $C^{\perp}$ is the dual codes of $C$ with respect to the ordinary inner product in $\mathbb{F}_2^n$. Then we have additive $[[n,\ 2k-n,\ d]]$ quantum code.*

**Proof** from $\dim_{\mathbb{F}_2} C = k$, $\dim_{\mathbb{F}_2} C^{\perp} = n-k$ and $C \supseteq C^{\perp}$ we know that $k \geq \frac{n}{2}$. Consider the subspace $\bar{G}$ of $\mathbb{F}_2^{2n}$ defined by

$$\begin{aligned} \bar{G} &= \{(v_1|v_2) \in \bar{E} = \mathbb{F}_2^{2n} | v_1, v_2 \in C^{\perp}\} \quad \dim_{\mathbb{F}_2} \bar{G} = 2(n-k) \\ &= C^{\perp} \oplus C^{\perp} \end{aligned}$$

Then it is easy to see that:

$$\bar{G}_s^{\perp} = \{(v_1, v_2) \in \bar{E} | v_1, v_2 \in C\}, \quad \dim_{\mathbb{F}_2} \bar{G}_s^{\perp} = 2k$$

and $\bar{G} \subseteq \bar{G}_s^{\perp}$. From theorem 3.1.3 we can construct a $[[n,\ k',\ d']]$ quantum code, where $k' = n-2(n-k) = 2k-n$ and $d' \geq w_Q(\bar{G}_s^{\perp}\backslash\bar{G}) = w_H(C\backslash C^{\perp}) \geq d$. $\square$

**Example** (quantum Hamming codes) Consider the binary Hamming code $C_3$ in section 1,example 1.2.4. The generating matrix of $C_3$ can be rewritten as

$$M = \begin{bmatrix} 1110100 \\ 0111010 \\ 0011101 \end{bmatrix}$$

$C_3$ is a binary $[7, 3, 4]$ linear code. The binary linear code $C_3'$ having generating matrix

$$M' = \begin{bmatrix} 0 & \\ 0 & M \\ 0 & \\ 1 & 1111111 \end{bmatrix}$$

is called extended Hamming code. $C_3'$ is $[8, 4, 4]$ self-dual code ($C_3' = C_3'^{\perp}$). By theorem 3.2.1 we have $[[8, 0, 4]]$ quantun code $Q$. Since $\dim_C Q = 2^k = 1$, the quantum code $Q$ has essentially only one quantum code word in $C^{2^8} = C^{256}$ which can correct one quantum error ($\sigma_x,\ \sigma_z,\ or\ \sigma_y$) in any qubit of its eight qubits. This quantum code $Q$ is not good. If we modify it by choosing linear code $\bar{G}$ in $\mathbb{F}_2^{16}$ with generating matrix

$$\left[\begin{array}{c|c} 01110100 & 00111010 \\ 00111010 & 00011101 \\ 00011101 & 01001110 \\ 11111111 & 00000000 \\ 00000000 & 11111111 \end{array}\right]$$

This time we have $n = 8,\ k = \dim_{\mathbb{F}_2} \bar{G} = 5, \bar{G} \subseteq \bar{G}_s^{\perp}$ and $w_Q(\bar{G}_s^{\perp} \backslash \bar{G}) = w_Q(\bar{G}_s^{\perp}) = 3$. By theorem3.1.3 we have pure $[[8, 3, 3]]$ quantum code $Q'$. $Q'$ is good because we have no $[[7, 3, 3]]$ quantum code by quantum Hamming bound.

**Theorem3.2.2**([CRSS 98]): If we have binary linear codes $C_1 = [n,\ k_1,\ d_1]$, $C_2 = [n,\ k_2,\ d_2]$ and $C_1{}^{\perp} \subseteq C_2$ (so that $n \leq k_1 + k_2$). Then we have additive quantum code $[[n,\ k_1 + k_2 - n,\ \min\{d_1, d_2\}]]$.

**Proof** Let $G_i$ and $H_i$ be generating and parity-check matrices of linear code $C_i$ $(i = 1, 2)$. Consider the linear code $C$ of $\mathbb{F}_2^{2n}$ with generating matrix

$$\begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix} \begin{matrix} n - k_1 \\ n - k_2 \end{matrix}$$

The assumption $C_1{}^{\perp} \subseteq C_2$ implies that $H_1 H_2^{\top} = 0$, and $C_s^{\perp}$ has parity-check matrix $\begin{pmatrix} H_2 & 0 \\ 0 & H_1 \end{pmatrix}$ and generating matrix $\begin{pmatrix} G_2 & 0 \\ 0 & G_1 \end{pmatrix}$. From these we know that $C \subseteq C_s^{\perp}$ and $w_Q(C_s^{\perp} \backslash C) \geq \min\{d_1, d_2\}$. By theorem 3.1.3 we have $[[n,\ k',\ \min\{d_1, d_2\}]]$ quantum code where $k' = n - \dim C = n - (n - k_1 + n - k_2) = k_1 + k_2 - n$. $\square$

Using more technical skill, Steane[St96(2)] improved theorem 3.2.2 which can obtain better quantum codes. Based on theorem3.2.2 and Stean's improvement, several authors ,using classical Reed-muller codes[ZF97],BCH codes [GB99]and algebraic-geometry codes[CL99],constructed a series of quantum codes with better parameters than some quantum codes lited in the table of [CRSS 98].

### §3.3 classical codes over $\mathbb{F}_4$ and quantum codes

In this subsection we introduce how to construct quantum codes from classical codes over $\mathbb{F}_4$.

Finite field $\mathbb{F}_4$ has four elements: $0,\ 1, \omega$, and $\bar{\omega} = \omega^2 = \omega + 1$. Consider the following mapping:

$$\begin{aligned} \Phi: \ & \bar{E} = \mathbb{F}_2^{2n} \to \mathbb{F}_4^n, \\ & v = (a|b) = (a_0, \cdots, a_{n-1}|b_0, \cdots, b_{n-1}) \mapsto \\ & \Phi(v) = \omega a + \bar{\omega} b = (\omega a_0 + \bar{\omega} b_0, \cdots, \omega a_{n-1} + \bar{\omega} b_{n-1}) \end{aligned}$$

Since $\{\omega,\ \bar{\omega}\}$ be a basis of $\mathbb{F}_4$ over $\mathbb{F}_2$, we know that $\Phi$ is isomorphism of $\mathbb{F}_2$-vector spaces.

**Lemma3.3.1** *(1)$\Phi$ keeps weights: $w_Q(v) = w_H(\Phi(v))$ for $v \in \mathbb{F}_2^{2n} = \bar{E}$.*
*(2)$\Phi$ keeps inner products: $< v, v' >_s = < \Phi(v), \Phi(v') >_{th}$ for $v, v' \in \bar{E}$ where for $\alpha = (\alpha_0, \cdots, \alpha_{n-1}),\ \beta = (\beta_0, \cdots, \beta_{n-1}) \in \mathbb{F}_4^n,\ < \alpha, \beta >_{th}$ is the trace-hermitian inner product defined by :*

$$< \alpha, \beta >_{th} = T_r(\sum_{i=0}^{n-1} \alpha_i \bar{\beta}_i) = T_r(\sum_{i=0}^{n-1} \alpha_i \beta_i^2) = \sum_{i=0}^{n-1} (\alpha_i \beta_i^2 + \alpha_i^2 \beta_i)$$

**Proof** (1). Let $v = (a|b),\ v' = (a'|b'),\ a = (a_0, \cdots, a_{n-1}),\ b = (b_0, \cdots, b_{n-1}),\ a' = (a_0', \cdots, a_{n-1}'), b' = (b_0', \cdots, b_{n-1}') \in \mathbb{F}_2^n$. Then $\Phi(v) = (\omega a_0 + \bar{\omega} b_0, \cdots, \omega a_{n-1} + \bar{\omega} b_{n-1})$. Since $\{\omega,\ \bar{\omega}\}$ is a basis of $\mathbb{F}_4$ over $\mathbb{F}_2$, we know that

$$w_Q(a_i|b_i) = 0 \Leftrightarrow (a_i, b_i) = (0, 0) \Leftrightarrow \omega a_i + \bar{\omega} b_i = 0 \Leftrightarrow w_H(\omega a_i + \bar{\omega} b_i) = 0$$

Therefore $w_Q(v) = w_H(\Phi(v))$.

(2).

$$\begin{aligned} < \Phi(v), \Phi(v') >_{th} &= T_r(\sum_{i=0}^{n-1} (\omega a_i + \omega^2 b_i)(\omega^2 a_i' + \omega b_i')) \\ &= \sum_{i=0}^{n-1} T_r(a_i a_i' + \omega^2 a_i b_i' + \omega a_i' b_i + b_i b_i') \\ &= (\sum_{i=0}^{n-1} a_i b_i') T_r(\omega^2) + (\sum_{i=0}^{n-1} a_i' b_i) T_r(\omega) \\ &= \sum_{i=0}^{n-1} a_i b_i' + \sum_{i=0}^{n-1} a_i' b_i \\ &= < v, v' >_s \end{aligned}$$

Since $T_r(1) = 0,\ T_r(\omega) = T_r(\omega^2) = \omega + \omega^2 = 1.$ □

By Lemma 3.3.1 we know that

$$\begin{array}{l} C \text{ is a linear code of } \mathbb{F}_2^{2n} \Leftrightarrow \Phi(C) \text{is an additive code of } \mathbb{F}_4^n \\ C \subseteq C_s^{\perp} \Leftrightarrow \Phi(C) \subseteq \Phi(C)_{th}^{\perp} \end{array}$$

and $d_s(C) = d_H(\Phi(C)),\ |\Phi(C)| = |C| = 2^{\dim_{\mathbb{F}_2} C}$, where

$$\begin{array}{rcl} \Phi(C)_{th}^{\perp} & = & \{\alpha \in \mathbb{F}_4^n | < \alpha, \beta >_{th} = 0 \ for\ all\ \beta \in \Phi(C)\} \\ d_H(\Phi(C)) & = & \min\{w_H(\alpha) | \alpha \in \Phi(C),\ \alpha \neq 0\} \end{array}$$

From these facts, the theorem 3.1.3 can be transformed into the following form.

**Theorem3.3.2** ([CRSS 98]) *Let $C$ be an additive code of $\mathbb{F}_4^n$ (which means that $C$ is an additive subgroup of $\mathbb{F}_4^n$). $C \subseteq C_{th}^{\perp}$, $|C| = 2^{n-k}$. Then we have $[[n,\ k,\ d]]$ quantum code where $d = w_H(C_{th}^{\perp} \backslash C) = \min\{w_H(v) | v \in C_{th}^{\perp} \backslash C\}$.*

The theorem 3.3.2 justifies the name "additive quantum codes" given by Caldbank et al.

Next result shows that if $C$ is a linear code of $\mathbb{F}_4^n$ which means that $C$ is a $\mathbb{F}_4$-linear subspace of $\mathbb{F}_4^n$, then the trace-hermitian product on $\mathbb{F}_4^n$ can be replaced by hermitian product. In this case, the quantum code Q derived from $C$ is called a linear quantum code.

**Theorem3.3.3** *Suppose that $C$ is an linear code of $\mathbb{F}_4^n$. then*

$$C \subseteq C_{th}^{\perp} \Leftrightarrow C \subseteq C_h^{\perp}$$

*where*

$$C_h^{\perp} = \{v \in \mathbb{F}_4^n | < v, u >_h = 0 \ for\ all\ u \in C\},$$

*and for $u = (u_0, \cdots, u_{n-1}),\ v = (v_0, \cdots, v_{n-1}) \in \mathbb{F}_4^n,\ < u, v >_h = \sum_{i=0}^{n-1} u_i v_i^2 \in \mathbb{F}_4$.*

**Proof** ($\Leftarrow$)Let $u,\ v \in C$. If$< u, v >_h = 0$, then $< u, v >_{th} = T_r < u, v >_h = 0$.

($\Rightarrow$)Suppose that $C \subseteq C_{th}^{\perp}$. For any $c \in C$, we have $< c, v >_{th} = 0$ for each $v \in C$. Let $< c, v >_h = a + b\omega$ ($a, b \in \mathbb{F}_2$, since $\{1, \omega\}$ is a basis of $\mathbb{F}_4$ over $\mathbb{F}_2$). Then $0 =< c, v >_{th} = T_r(a + b\omega) = b$ so that $< c, v >_h = a$. Moreover, since $C$ is liner code of $\mathbb{F}_4^n$, $\omega v \in C$ so that

$$0 =< c, \omega v >_{th} = T_r(< c, \omega v >_h) = T_r((\omega^2(a + b\omega)) = T_r(a\omega^2 + b) = a$$

Therefore $< c, v >_h = a + b\omega = 0$ for each $v \in C$ which means that $c \in C_h^{\perp}$ for any $c \in C$. Thus $C \subseteq C_h^{\perp}$. □

**Definition3.3.4** *A subset $C$ of $\mathbb{F}_4^n$ is called even code if for each $c \in C$, $w_H(c)$ is even integer.*

**<u>Lemma3.3.5</u>** *Suppose that* $C \subseteq \mathbb{F}_4^n$.

*(1)If* $C$ *is even and additive code, then* $C$ *is self-orthogonal with respect to* $<\ ,\ >_{th}$ $(C \subseteq C_{th}^{\perp})$.

*(2)If* $C \subseteq C_{th}^{\perp}$ *and* $C$ *is a* $\mathbb{F}_4$*-linear code, then* $C$ *is even code.*

**<u>Proof</u>**(1)Let $u = (u_0, \cdots, u_{n-1}),\ v = (v_0, \cdots, v_{n-1}),\ u_i,\ v_i \in \mathbb{F}_4$. Suppose that $u_i = a + b\omega,\ v_i = c + d\omega$ where $a,\ b,\ c,\ d,\ \in \mathbb{F}_2$. Then

$$T_r(u_i\overline{v_i}) = T_r((a+b\omega)\overline{(c+d\omega)}) = T_r((a+b\omega)(c+d\omega^2)) = ad + bc$$

On the other hand, $w_H(v_i) = 0 \Leftrightarrow a = b = 0$. Thus

$$w_H(u_i) \equiv ab + a + b \pmod 2$$

Similarly we have

$$w_H(v_i) \equiv cd + c + d, \quad w_H(u_i + v_i) \equiv (a+c)(b+d) + a + b + c + d \pmod 2$$

Therefore, for each $i$ $(0 \leq i \leq n-1)$

$$w_H(u_i + v_i) + w_H(u_i) + w_H(v_i) \equiv ad + bc = T_r(u_i\overline{v_i}) \pmod 2$$

which implies that $w_H(u+v) + w_H(u) + w_H(v) \equiv <u, v>_{th} \pmod 2$. From this the condition (1) can be obtained.

(2)For each $u = (u_0, \cdots, u_{n-1}) \in C,\ u_i \in \mathbb{F}_4$, by assumption we have $\omega u \in C$ and

$$0 =< u, \omega u >_{th} = T_r(\sum_{i=0}^{n-1} u_i\omega^2 u_i^2) = T_r(\sum_{i=0}^{n-1} \omega^2 u_i^3) \equiv w_H(u)T_r(\omega^2) \equiv w_H(u) \pmod 2.$$

since for $u_i \in \mathbb{F}_4$,

$$u_i^3 = \begin{cases} 1, & \text{if } \ u_i \neq 0 \\ 0, & \text{if } \ u_i = 0. \end{cases}$$

Therefore $C$ is even code. □

**<u>Example3.3.6</u>**(Quantum Hamming codes via $\mathbb{F}_4$) Let $m \geq 2$ and $\alpha$ be a primitive element of $F_{4^m}$ which means $\alpha \in F_{4^m}^*$ and the multiplicative order of $\alpha$ is $s = 4^m - 1$. By choose a basis $\{v_1,\ \cdots,\ v_m\}$ of $F_{4^m}$ over $\mathbb{F}_4$ (for example, $\{v_1,\ \cdots,\ v_m\} = \{1,\ \alpha,\ \cdots,\ \alpha^{m-1}\}$), each element $c \in F_{4^m}$ can be uniquely expressed by $c = c_1v_1 + \cdots + c_mv_m$ $(c_i \in \mathbb{F}_4)$ or by vector $c = (c_1,\ \cdots,\ c_m) \in \mathbb{F}_4^m$. In this way we view $F_{4^m}$ as a $\mathbb{F}_4$-vector space $\mathbb{F}_4^m$.

Consider the $\mathbb{F}_4$-linear code $C$ in $\mathbb{F}_4^n$ $(n = \frac{s}{3} = \frac{4^m-1}{3})$ with parity-check matrix

$$H = [1^\top, \alpha^\top, (\alpha^2)^\top, \cdots, (\alpha^{n-1})^\top]$$

where $(\alpha^i)^\top$ means the column vector of $\alpha^i$. From the order of $\alpha$ is $s = 4^m - 1$ we know that $\{\alpha^n, \alpha^{2n}\} = \{\omega, \omega^2\}$ so that $\{\alpha^i,\ \alpha^{i+n},\ \alpha^{i+2n}\} = \{\alpha^i,\ \omega\alpha^i,\ \omega^2\alpha^i\}$

for each $i(0 \leq i \leq n-1)$. Therefore the $n$ column vectors in $H$ are just the projective points in the projective space $P^{m-1}(\mathbb{F}_4)$. Therefore $C$ is the Hamming code over $\mathbb{F}_4$ with $[n,\ k,\ d] = [\frac{4^m-1}{3},\ \frac{4^m-1}{3} - m,\ 3]$. It is well know that $C^\perp$ is $[\frac{4^m-1}{3},\ m,\ 4^{m-1}]$ linear code over $\mathbb{F}_4$ and each non-zero codeword in $C^\perp$ has Hamming weight $4^{m-1}$. Therefore $C^\perp$ is even code. By Lemma 3.3.5 we know that $C^\perp$ is self-orthogonal with respect to $<\ ,\ >_{th}$ and it is easy to see that $C^\perp \subseteq (C^\perp)_h^\perp = (C^\perp)^\perp = C$. From theorem3.3.2 and $|C^\perp| = 2^{2m}$ we know that there exist $[[n,\ k,\ d]] = [[\frac{4^m-1}{3},\ \frac{4^m-1}{3} - 2m,\ 3]]$ quantum codes for all $m \geq 2$. All of quantum codes in this series are perfect since they are pure codes and

$$2^{n-k} = 2^{2m} = 1 + 3(\frac{4^m-1}{3}) = 1 + 3n.$$

For $m = 2$ we obtain $[[5,\ 1,\ 3]]$ quantum code again. For more quantum codes constructed from classical codes over $\mathbb{F}_4$ see [CRSS 98]and [TM 00].

## §4 Weight enumerator of quantum codes

Beside constructing good quantum codes, there are other topics on quantum codes being investigated. In this section we show one of such topics: the weight enumerator.

### §4.1. MacWilliams identity for quantum codes

Let $Q$ be a $((n,\ K))$ quantum code which means that $Q$ is a subspace of $\mathbb{C}^{2^n}$ with $\dim_{\mathbb{C}} Q = K$. Let $P:\ \mathbb{C}^{2^n} \to Q$ be the orthogonal projection.

**Definition4.1.1** *Let*

$$B_i = \frac{1}{K^2}\sum_e T_r^2(eP), \quad B_i^{\perp} = \frac{1}{K}\sum_e T_r(ePeP)$$

*where $e = \sigma_0 \otimes \sigma_1 \otimes \cdots \otimes \sigma_{n-1}$ and $w_Q(e) = i$, $\sigma_i \in \{I_2,\ \sigma_x,\ \sigma_y,\ \sigma_z\}$. Since such $e$ is Hermitian operation, so that the Traces of $eP$ and $ePeP$ are real numbers and so are $B_i$ and $B_i^{\perp}$.*

*The weight enumerators of $Q$ are defined by*

$$B(x,y) = \sum_{i=0}^{n} B_i x^{n-i} y^i, \quad B^{\perp}(x,y) = \sum_{i=0}^{n} B_i^{\perp} x^{n-i} y^i,$$

**Theorem4.1.2** *Let $Q$ be a $((n,\ K))$ quantum code and $B(x,y)$, $B^{\perp}(x,y)$ be its weight enumerators. Then*

$$B(x,y) = \frac{1}{K} B^{\perp}\left(\frac{x+3y}{2}, \frac{x-y}{2}\right)$$

**Proof** The first proof is a mixture of physical and mathematical methods given by [SL97]. The following pure mathematical proof is given by[R98]. Suppose that the matrices of $e$ and $P$ with respect to the basis $|j>=|j_0 \cdots j_{n-1}>\quad (0 \le j \le 2^n - 1,\ j = j_0 + j_1 \cdot 2 + \cdots + j_{n-1} \cdot 2^{n-1})$ of $\mathbb{C}^{2^n}$ are

$$e = (e_{ij}), \quad P = (P_{ij}) \quad (0 \le i,\ j \le 2^n - 1)$$

Then $e|i>= \sum\limits_j e_{ij}|j>$ for $e = \sigma_0 \otimes \sigma_1 \otimes \cdots \otimes \sigma_{n-1}$ we have

$$e_{ij} = (\sigma_0)_{i_0 j_0} \bullet \cdots \bullet (\sigma_{n-1})_{i_{n-1} j_{n-1}}, \qquad \sigma_i \in \{I_2,\ \sigma_x,\ \sigma_y,\ \sigma_z\}$$

Therefore,

$$\begin{aligned} B(x,y) &= \tfrac{1}{K^2} \sum_{t=0}^{n} x^{n-t} y^t \sum_{w_Q(e)=t} \sum_{i,j,k,l} P_{ji} e_{ij} P_{lk} e_{kl} \\ &= \tfrac{1}{K^2} \sum_{i,j,k,l} P_{ji} P_{lk} \sum_e e_{ij} e_{kl} x^{n-w_Q(e)} y^{w_Q(e)} \\ &= \tfrac{1}{K^2} \sum_{i,j,k,l} P_{ji} P_{lk} \prod_{t=0}^{n-1} b_{i_t j_t k_t l_t}(x,y) \end{aligned}$$

where

$$b_{i_tj_tk_tl_t}(x,y) = x(I_2)_{i_tj_t}(I_2)_{k_tl_t} + y[(\sigma_x)_{i_tj_t}(\sigma_x)_{k_tl_t} + (\sigma_y)_{i_tj_t}(\sigma_y)_{k_tl_t} + (\sigma_z)_{i_tj_t}(\sigma_z)_{k_tl_t}]$$

Similarly we have

$$B^{\perp}(x,y) = \frac{1}{K}\sum_{i,j,k,l} P_{ji}P_{lk}\prod_{t=0}^{n-1} b^{\perp}_{i_tj_tk_tl_t}(x,y)$$

where

$$b^{\perp}_{i_tj_tk_tl_t}(x,y) = x(I_2)_{i_tl_t}(I_2)_{k_tj_t} + y[(\sigma_x)_{i_tl_t}(\sigma_x)_{k_tj_t} + (\sigma_y)_{i_tl_t}(\sigma_y)_{k_tj_t} + (\sigma_z)_{i_tl_t}(\sigma_z)_{k_tj_t}]$$

We need to prove

$$b_{ijkl}(x,y) = b^{\perp}_{ijkl}(\frac{x+3y}{2}, \frac{x-y}{2})$$

for all 16 cases $i,j,k,l \in \{0,1\}$. For example, $b_{0011}(x,y) = x-y$ and $b^{\perp}_{0011}(x,y) = 2y$. We have the ramain cases to readers. $\square$

The name "weight enumerator" in definition4.1.1 can be justified by following result.

**Lemma4.1.3** *If $Q$ is an additive quantum code derived from an $(n,\ 2^{n-k})$ additive code $C$ over $\mathbb{F}_4$. Then*

$$B_i = \sharp\{c \in C:\ w_H(c) = i\}, \quad B_i^{\perp} = \sharp\{c \in C_{th}^{\perp}:\ w_H(c) = i\}$$

*So that theorem4.1.2 becomes the MacWilliam Identity for additive codes over $\mathbb{F}_4$.*

**Proof** We identify $C$ with $\bar{G}(\subset \bar{E})$ by $\omega a + \bar{\omega} b \mapsto \bar{e} = (a|b) \in \bar{G}$ and $Q = Q(\chi)$ be the $\chi$-eigenspace of $G$ acting on $\mathbb{C}^{2^n}$ for some character $\chi \in \hat{G}$. $K = \dim_C Q = 2^k$. Then the projective operation $P:\ \mathbb{C}^{2^n} \to Q$ is

$$P = 2^{-(n-k)}\sum_{e\in G}\chi(e)e$$

Then we know that for each $e \in E$

$$T_r(eP) = 2^{-(n-k)}\sum_{e'\in G}\chi(e')T_r(ee') = \begin{cases} \chi(e)T_r(P) = \chi(e)2^k, & \text{if } \bar{e} \in \bar{G} = C \\ 0, & \text{otherwise} \end{cases}$$

Therefore

$$B_i = \frac{1}{K^2}\sum_{\substack{e\in G \\ w_Q(e)=i}} 2^{2k} = \sum_{\substack{e\in G \\ w_Q(e)=i}} 1 = \sum_{\substack{c\in C \\ w_H(c)=i}} 1$$

Similarly,

$$\begin{aligned}
T_r(ePeP) &= 2^{-2(n-k)} \sum_{a,b\in G} \chi(ab) T_r(eaeb) \\
&= 2^{-2(n-k)} \sum_{a,b\in G} (-1)^{<\bar{e},\bar{a}>} \chi(ab) T_r(ab) \\
&= 2^{-2(n-k)} \sum_{a\in G} (-1)^{<\bar{e},\bar{a}>} \sum_{b\in G} \chi(b) T_r(b) \\
&= \begin{cases} 2^{-(n-k)} \sum_{b\in G} \chi(b) T_r(b) = T_r(P) = 2^k, & \text{if } \bar{a} \in (\bar{G})_s^{\perp} \\ 0, & \text{otherwise} \end{cases}
\end{aligned}$$

Therefore,

$$B_i^{\perp} = \frac{2^k}{K} \sum_{\substack{\bar{a} \in (\bar{G})_s^{\perp} \\ w_Q(\bar{a}) = i}} 1 = \sum_{\substack{c \in (C)_{th}^{\perp} \\ w_H(c) = i}} 1$$

□

The following result shows that, the weight enumerators of $Q$ can determine $d(Q)$ as in classical case even though $Q$ is not additive.

**Lemma4.1.4** *(1).* $B_0 = B_0^{\perp} = 1, \quad B_i^{\perp} \geq B_i \geq 0 \quad (0 \leq i \leq n)$

*(2). Let $t$ be the maximal integer such that $B_i = B_i^{\perp} (0 \leq i \leq t)$. Then $d(Q) = t + 1$.*

**Proof** (1). $B_0 = \frac{1}{K^2} T_r^2(P) = 1, \quad B_0^{\perp} = \frac{1}{K} T_r(P^2) = 1$

From definition we know that $B_i \geq 0$. Moreover, from the well-known inequality $T_r^2(A^{\dagger}B) \leq T_r(A^{\dagger}A) T_r(B^{\dagger}B)$ and $T_r(AB) = T_r(BA)$ we know that if $e^{\dagger} = e$,

$$T_r^2(eP) = T_r^2(PePP) \leq T_r(PePPeP) \cdot T_r(P^2) = T_r(ePeP) \cdot K \quad (*)$$

from which $B_i^{\perp} \geq B_i$ can be derived.

(2).From the inequality (*) we know that

$$B_i^{\perp} = B_i \Leftrightarrow PeP = \lambda_e P \quad \text{for all } e \in E \text{ such that } w_Q(e) = i.$$

Then the conclusion (2) comes from the following lemma. □

**Lemma4.1.5** *A quantum code $Q$ can correct $\leq l$ errors $\Leftrightarrow$ for each $e \in E_{2l}$, $PeP = \lambda_e P \quad (\lambda_e \in \mathbb{C})$.*

**Proof** ($\Leftarrow$) Suppose that $c,\ c' \in Q$ and $< c|c' >= 0$, we need to prove $< c|ee'|c' >= 0$ for any $e,\ e' \in E_l$. Since $ee' \in E_{2l}$ so that $Pee'P = \lambda_{ee'}P \ (\lambda_{ee'} \in \mathbb{C})$ by assumption. On the other hand, $Pc = c$ and $Pc' = c'$. Therefore

$$\begin{aligned}
< c|ee'|c' > &= < cP|ee'|Pc' >=< c|Pee'P|c' > \\
&= < c|\lambda_{ee'}P|c' >= \lambda_{ee'} < c|c' >= 0.
\end{aligned}$$

($\Rightarrow$) Suppose that $c,\ c' \in Q$ such that $< c|c' >= 0$ and $< c|c >=< c'|c' >= 1$. Then $c \pm c' \in Q$ and $< c + c'|c - c' >=< c|c > - < c'|c' >= 0$. Each $e \in E_{2l}$ can be decomposed as $e = e_1 e_2$ where $e_1,\ e_2 \in E_l$. Since $Q$ can correct $\leq l$ errors, we know that

$$0 =< c + c'|e|c - c' >=< c|e|c > - < c'|e|c' > \qquad (*)$$

Now we choose a basis $c_1,\ \cdots,\ c_K$ of $Q$ such that $< c_i|c_j >= \overline{c_i} \cdot c_j^\top = \delta_{ij}$ $(1 \leq i, j \leq K)$. From(*) we know that for each $e \in E_{2l}$, $< c_i|e|c_i >= \overline{c_i} e c_i^\top = \lambda_e \in \mathbb{C}$ is independent on $i$ $(1 \leq i \leq K)$. Thus the matrix of $P$ with respect to the basis $c_1,\ \cdots,\ c_K$ of $Q$ is $P = \sum\limits_{i=1}^{K} c_i^\top \overline{c_i}$. Then for each $e \in E_{2l}$,

$$\begin{aligned} PeP &= (\sum_i c_i^\top \overline{c_i}) e (\sum_j c_j^\top \overline{c_j}) = \sum_{i,j} c_i^\top (\overline{c_i} e c_j^\top) \overline{c_j} \\ &= \sum_{i,j} c_i^\top \overline{c_j} < c_i|e|c_j >= \lambda_e \sum_{i,j} c_i^\top \overline{c_j} \delta_{ij} = \lambda_e \sum_i c_i^\top \overline{c_i} = \lambda_e P. \end{aligned} \qquad \square$$

**Remark** From theorem4.1.2 we know that $K = \frac{1}{2^n} \sum\limits_{i=0}^{n} B_i^\perp$.

## §4.2 Quantum Singleton Bound

The Mac Williams identity can be used to derive bounds of the parameters of quantum codes by traditional method in classical case. Namely, we use the Krawtchouk polynomials.

**Definition4.2.1** *For fixed positive integer $n$, the Krawtchouk polynomials are defined by*

$$P_i(x) = \sum_{j=0}^{i} (-1)^j 3^{i-j} \binom{x}{j} \binom{n-x}{i-j} \qquad (0 \leq i \leq n)$$

By definition we know that $P_i(x) \in \mathbb{Q}(x)$ and $\deg P_i(x) = i$. The first three polynomials are

$$P_0(x) = 1, \quad P_1(x) = 3n - 4x, \quad P_2(x) = \frac{1}{2}(16x^2 + 8x(1-3n) + 9n(n-1)).$$

We list several properties of Krawtchouk polynomials and relations to weight enumerators of quantum codes in the following lemma.

**Lemma4.2.2** *(1).(Symmetric property)* $3^i \binom{n}{i} P_j(i) = 3^j \binom{n}{j} P_i(j) \quad (0 \leq i,\ j \leq n)$.

*(2). (Orthogonal relations)*

$$\sum_{i=0}^{n} P_r(i) P_i(s) = 4^n \delta_{rs}, \qquad \sum_{i=0}^{n} 3^i \binom{n}{i} P_r(i) P_s(i) = 4^n 3^r \binom{n}{r} \delta_{rs}.$$

*(3).Any polynomial $f(x) \in \mathbb{R}[x]$ have unique expression*

$$f(x) = \sum_{i=0}^{d} f_i P_i(x) \quad (f_i \in \mathbb{R}) \quad d = \deg f.$$

*and*
$$f_i = \frac{1}{4^n}\sum_{j=0}^{n} f(j)P_j(i) = \frac{1}{4^n \cdot 3^i\binom{n}{i}}\sum_{j=0}^{n} 3^j\binom{n}{j} f(j)P_i(j)$$

*(4).Let* $B(x,y) = \sum\limits_{t=0}^{n} B_t x^{n-t}y^t$ *and* $B^{\perp}(x,y) = \sum\limits_{t=0}^{n} B_t^{\perp} x^{n-t}y^t$ *be the weight enumerator of a* $((n,\ k,\ d))$ *quantum code, then*

$$B_i = \frac{1}{2^n K}\sum_{j=0}^{n} P_i(j)B_j^{\perp}.$$

**<u>Proof</u>** (1). By the definition4.2.1,

$$\begin{array}{rcl} \sum\limits_{i=0}^{n} P_i(j)z^j & = & \sum\limits_{i=0}^{n}\sum\limits_{\mu=0}^{i}(-1)^{\mu}3^{i-\mu}\binom{n-j}{i-\mu}\binom{j}{\mu}z^i \\ & = & \sum\limits_{\mu=0}^{n}(-1)^{\mu}\binom{j}{\mu}\sum\limits_{i=\mu}^{n}3^{i-\mu}\binom{n-j}{i-\mu}z^i \\ & = & \sum\limits_{\mu=0}^{n}(-1)^{\mu}\binom{j}{\mu}z^{\mu}\sum\limits_{i=0}^{n-j}3^{i}\binom{n-j}{i}z^i \\ & = & (1-z)^j(1+3z)^{n-j} = (1+3z)^n(\frac{1-z}{1+3z})^j \end{array}$$

and

$$\begin{array}{l} \sum\limits_{i,j=0}^{n} 3^j\binom{n}{j}P_i(j)z^iw^j = \sum\limits_{j=0}^{n}\binom{n}{j}(3w)^j(1+3z)^n(\frac{1-z}{1+3z})^j \\ = (1+3z)^n(1+3w\cdot\frac{1-z}{1+3z})^n = (1+3z+3w-3zw)^n \end{array}$$

The right-hand side of this equality is a symmetric polynomial over $z$ and $w$. Thus

$$\sum_{i,j=0}^{n} 3^j\binom{n}{j}P_i(j)z^iw^j = \sum_{i,j=0}^{n} 3^j\binom{n}{j}P_i(j)z^jw^i = \sum_{i,j=0}^{n} 3^i\binom{n}{i}P_j(i)z^iw^j$$

which implies that

$$3^j\binom{n}{j}P_i(j) = 3^i\binom{n}{i}P_j(i) \quad (0 \le i,j \le n)$$

(2). We have by the equality in (1) that

$$\begin{array}{rl} & \sum\limits_{r,s=0}^{n}\sum\limits_{i=0}^{n}3^i\binom{n}{i}P_r(i)P_s(i)z^rw^s \\ = & \sum\limits_{i=0}^{n}3^i\binom{n}{i}(1-z)^i(1+3z)^{n-i}(1-w)^i(1+3w)^{n-i} \\ = & (1+3z)^n(1+3w)^n\sum\limits_{i=0}^{n}3^i\binom{n}{i}(\frac{(1-z)(1-w)}{(1+3z)(1+3w)})^i \\ = & [(1+3z)(1+3w)+3(1-z)(1-w)]^n \\ = & (4+12zw)^n \\ = & 4^n(1+3zw)^n \end{array}$$

Therefore
$$\sum_{i=0}^{n} 3^i \binom{n}{i} P_r(i)P_s(i) = \delta_{r,s} \cdot 4^n 3^r \binom{n}{r}$$
By(1) we obtain the other orthogonal relation.

(3). Since $\deg P_i(x) = i$ $(i = 0, 1, 2, \cdots)$ we have the unique expression. Then by the orthogonal relations,

$$\sum_{j=0}^{n} f(j)P_j(i) = \sum_{j=0}^{n} P_j(i) \sum_{k=0}^{n} f_k P_k(j) = \sum_{k=0}^{n} f_k \sum_{j=0}^{n} P_j(i)P_k(j) = 4^n f_i$$

(4). From the MacWilliams identity,

$$\begin{aligned}
\sum_{t=0}^{n} B_t x^{n-t} y^t &= \tfrac{1}{K} \sum_{i=0}^{n} B_i^{\perp} (\tfrac{x+3y}{2})^{n-i} (\tfrac{x-y}{2})^i \\
&= \tfrac{1}{2^n K} \sum_{i=0}^{n} B_i^{\perp} \sum_{\lambda,\mu \geq 0} \tbinom{n-i}{\lambda} \tbinom{i}{\mu} x^{n-i-\lambda} (3y)^{\lambda} x^{i-\mu} (-y)^{\mu}
\end{aligned}$$

Thus we have

$$\begin{aligned}
B_t &= \tfrac{1}{2^n K} \sum_{i=0}^{n} B_i^{\perp} \sum_{\substack{\lambda, \mu \geq 0 \\ \lambda + \mu = t}} \tbinom{n-i}{\lambda} \tbinom{i}{\mu} 3^{\lambda} (-1)^{\mu} \\
&= \tfrac{1}{2^n K} \sum_{i=0}^{n} B_i^{\perp} P_t(i)
\end{aligned}$$

The another equality can be derived by inverse transformation in (3). □

Next lemma shows that we can present a bound for $K$ by choosing suitable $f(x)$ in $\mathbb{R}[x]$.

**Lemma4.2.3** Let $Q$ be a $((n,\ K,\ d))$ quantum code. If there exists a *polynomial*

$$f(x) = \sum_{i=0}^{n} f_i P_i(x) \in \mathbb{R}[x] \quad (f_i \in \mathbb{R})$$

*Such that*
*(i)* $f_i \geq 0 \quad (0 \leq i \leq n)$;
*(ii)* $f(j) > 0 \quad (0 \leq j \leq d-1)$ *and* $f(j) \leq 0 \quad (d \leq j \leq n)$
*Then*
$$K \leq \frac{1}{2^n} \max_{0 \leq j \leq d-1} \frac{f(j)}{f_j}$$

**Proof** From the assumptions and lemma 4.2.2 we have the following estimation.

$$\begin{aligned}
2^n K \sum_{i=0}^{d-1} f_i B_i &\leq 2^n K \sum_{i=0}^{n} f_i B_i = \sum_{i=0}^{n} f_i \sum_{j=0}^{n} B_j^{\perp} P_i(j) \\
&= \sum_{j=0}^{n} B_j^{\perp} \sum_{i=0}^{n} f_i P_i(j) = \sum_{j=0}^{n} B_j^{\perp} f(j) \\
&\leq \sum_{j=0}^{d-1} B_j^{\perp} f(j) = \sum_{j=0}^{d-1} B_j f(j) \quad (by\ lemma 4.1.4(2))
\end{aligned}$$

Therefore

$$2^n K \le \frac{\sum_{j=0}^{d-1} B_j f(j)}{\sum_{j=0}^{d-1} f_j B_j} \le \max_{0\le j\le d-1} \frac{f(j)}{f_j}.$$

□

Now we present a bound for any quantum code as an analogue of Singleton bound for classical linear codes.

**Theorem 4.2.4** *(quantum singleton bound) For any $((n,\ K,\ d))$ quantum code such that $d \le \frac{n}{2}+1$, we have $K \le 2^{n-2d+2}$.*

**Proof** Consider

$$f(x) = 4^{n-d+1}\prod_{j=d}^{n}(1-\frac{x}{j}) = 4^{n-d+1}\frac{\binom{n-x}{n-d+1}}{\binom{n}{n-d+1}}$$

The values $f(j)$ $(0 \le j \le n)$ satisfy the condition (ii) of lemma 4.2.3. Next we compute the coefficients $f_i$ in the expression $f(x) = \sum_{i=0}^{n} f_i P_i(x)$. For doing this we consider

$$\begin{aligned}\sum_{\lambda=0}^{n} 3^\lambda\tbinom{n}{\lambda}f(\lambda)z^\lambda &= \tfrac{4^{n-d+1}}{\binom{n}{n-d+1}}\sum_{\lambda=0}^{n} 3^\lambda\tbinom{n}{\lambda}\tbinom{n-\lambda}{n-d+1}z^\lambda \\ &= 4^{n-d+1}\sum_{\lambda=0}^{n}\tbinom{d-1}{\lambda}(3z)^\lambda = 4^{n-d+1}(1+3z)^{d-1}\end{aligned}$$

On the other hand,

$$\begin{aligned}\sum_{\lambda=0}^{n} 3^\lambda\tbinom{n}{\lambda}f(\lambda)z^\lambda &= \sum_{\lambda=0}^{n} 3^\lambda\tbinom{n}{\lambda}z^\lambda\sum_{i=0}^{n} f_iP_i(\lambda) \\ &= \sum_{i,\lambda=0}^{n} 3^i\tbinom{n}{i}z^\lambda\sum_{i=0}^{n} f_iP_\lambda(i) \\ &= \sum_{i=0}^{n} 3^i\tbinom{n}{i}f_i\sum_{\lambda=0}^{n} P_\lambda(i)z^\lambda \\ &= \sum_{i=0}^{n} 3^i\tbinom{n}{i}f_i(1+3z)^n(\tfrac{1-z}{1+3z})^i\end{aligned}$$

Thus

$$\sum_{i=0}^{n} 3^i\binom{n}{i}f_i(\frac{1-z}{1+3z})^i = 4^{n-d+1}/(1+3z)^{n-d+1}$$

Let $w = \frac{1-z}{1+3z}$, then $z = \frac{1-w}{1+3w}$ and

$$\sum_{i=0}^{n} 3^i\binom{n}{i}f_iw^i = \frac{4^{n-d+1}}{(\frac{4}{1+3w})^{n-d+1}} = (1+3w)^{n-d+1} = \sum_{i=0}^{n-d+1}\binom{n-d+1}{i}3^iw^i$$

Therefore we obtain that $f_i = \binom{n-d+1}{i} / \binom{n}{i} = \binom{n-i}{d-1} / \binom{n}{d-1}$ $(0 \le i \le n)$ which satisfy the condition(i) of lemma 4.2.3. Then we have

$$\begin{aligned}
K &\le \frac{1}{2^n} \max_{0 \le j \le d-1} \frac{f(j)}{f_j} \\
&= \frac{1}{2^n} \max_{0 \le j \le d-1} \left\{ 4^{n-d+1} \frac{\binom{n-j}{n-d+1}}{\binom{n}{n-d+1}} \cdot \frac{\binom{n}{d-1}}{\binom{n-j}{d-1}} \right\} \\
&= 2^{n-2d+2} \max_{0 \le j \le d-1} \frac{\binom{n-j}{n-d+1}}{\binom{n-j}{d-1}}
\end{aligned}$$

Let $g(j) = \binom{n-j}{n-d+1} / \binom{n-j}{d-1}$. Then $\frac{g(j)}{g(j+1)} = \frac{n-j-d+1}{d-1-j} \ge 1$ by the assumption $d \le \frac{n}{2}+1$. Therefore $K \le 2^{n-2d+2} g(0) = 2^{n-2d+2}$. $\square$

## §5 Nonbinary case

### §5.1 Stabilizer Nonbinary Quantum Codes

The theory on binary ($p = 2$) quantum codes, described in §2 – §4, has been generalized to nonbinary case ($p \geq 3$)([AK00],[K96(1)],[MU99],[R99(1)]). In this section we introduce the stabilizer nonbinary quantum codes. The conceptions and results are parallel to the binary case without any essential difficulty, so we omit the proof.

We fix an odd prime number $p$.

**<u>Definition 5.1.1</u>** *A qubit is a non-zero vector in $\mathbb{C}^p$,*

$$0 \neq |v>= c_0|0> +c_1|1> + \cdots + c_{p-1}|p-1> \qquad (c_i \in \mathbb{C})$$

*where* $\{|0>, |1>, \cdots, |p-1>\} = \{|a>: \ a \in \mathbb{F}_p\}$ (1)
*is a basis of* $\mathbb{C}^p$.

*A $n$-qubit is a non-zero vector in* $(\mathbb{C}^p)^{\otimes n} = \mathbb{C}^{p^n}$,

$$0 \neq |v>= \sum_{a=(a_1,\cdots,a_n)\in\mathbb{F}_p^n} c_a|a> \qquad (c_a \in \mathbb{C})$$

*where*

$$\{|a>= |a_1 \cdots a_n>= |a_1> \otimes |a_2> \otimes \cdots \otimes |a_n>: \ a = (a_1, \cdots, a_n) \in \mathbb{F}_p^n\} \qquad (2)$$

*ia a basis of* $\mathbb{C}^{p^n}$.

A quantum error $\sigma_l\tau_s$ ($l, s \in \mathbb{F}_p$) on a qubit is a unitary linear operator on $\mathbb{C}^p$, which acts on the basis (1) of $\mathbb{C}^p$ by

$$\sigma_l\tau_s|a>= \zeta_p^{sa}|a+l> \qquad (a \in \mathbb{F}_p)$$

where $\zeta_p = e^{\frac{2\pi i}{p}}$.

A quantum error on a $n-$qubit is a unitary linear operator on $(\mathbb{C}^p)^{\otimes n} = \mathbb{C}^{p^n}$

$$e = \zeta_p^t\omega_1 \otimes \omega_2 \otimes \cdots \otimes \omega_n \qquad (\omega_i = \sigma_{l_i}\tau_{s_i}, \ t, l_i, s_i \in \mathbb{F}_p) \qquad (3)$$

which acts on the basis (2) of $\mathbb{C}^{p^n}$ by

$$\begin{aligned} e|a_1 \cdots a_n> &= \zeta_p^t \cdot (\omega_1|a_1>) \otimes (\omega_2|a_2) \otimes \cdots \otimes (\omega_n|a_n>) \\ &= \zeta_p^{t+s_1a_1+\cdots+s_na_n}(|a_1+l_1> \otimes |a_2+l_2> \otimes \cdots \otimes |a_n+l_n>) \\ &= \zeta_p^{t+(s,a)}|a+l> \qquad (s = (s_1, \cdots, s_n), \ l = (l_1, \cdots, l_n) \in \mathbb{F}_p^n) \end{aligned}$$

All error $e$ of (3) forms a non-abelian error group $E_n$, $|E_n| = p^{2n+1}$. The error $e$ can be expressed by

$$e = \zeta_p^\lambda X(a)Z(b) \quad (a = (a_1, \cdots, a_n), b = (b_1, \cdots, b_n) \in \mathbb{F}_p^n)$$

where

$$X(a) = \sigma_{a_1} \otimes \cdots \otimes \sigma_{a_n}, \quad Z(b) = \tau_{a_1} \otimes \cdots \otimes \tau_{a_n}$$

Then for $e$ and $e' = \zeta_p^{\lambda'} X(a')Z(b')$ we have

$$e'e = \zeta_p^{a' \cdot b - a \cdot b'} ee' \qquad (4)$$

From this we know that the center $C(E_n)$ of $E_n$ is $\{\zeta_p^\lambda | \ \lambda \in \mathbb{F}_p\}$ and the quotient group $\widehat{E_n} = E_n/C(E_n)$ is abelian. The image of $e = \zeta_p^\lambda X(a)Z(b) \in E_n$ in $\overline{E_n}$ is denoted by

$$\overline{e} = (a|b) \quad (a, b \in \mathbb{F}_p^n)$$

Then $\overline{E_n}$ is naturally isomorphic to the additive group of $\mathbb{F}_p^{2n}$. We define the symplectic inner product $(\ ,\ )_s$ in $\mathbb{F}_p^{2n}$ by

$$((a|b), (a'|b'))_s = a \cdot b' - a' \cdot b = \sum_{i=1}^{n} (a_i b_i' - a_i' b_i) \in \mathbb{F}_p$$

Then the formula (4) implies that

**Lemma 5.1.2** *A subgroup $S$ of $E_n$ is abelian if and only if $\overline{S}$ is a symplectic self-orthogonal subspace of $\mathbb{F}_p^{2n}$, namely $\overline{S} \subseteq (\overline{S})_s^\perp$ where*

$$(\overline{S})_s^\perp = \{v \in \mathbb{F}_p^{2n} | \ (v, c)_s = 0 \text{ for all } c \in \overline{S}\}$$

For $e = \zeta_p^\lambda X(a)Z(b)$ $(a, b \in \mathbb{F}_p^n)$ we define the quantum weight of $e$ and $\overline{e} = (a|b)$ by

$$w_Q(e) = w_Q(\overline{e}) = \sharp\{1 \le i \le n | \ (a_i, b_i) \ne (0, 0)\}$$

Let

$$E_n(l) = \{e \in E_n | \ w_Q(e) \le l\} \quad (0 \le l \le n)$$

Then $|E_n(l)| = \sum_{i=0}^{l} (p^2 - 1)^i \begin{pmatrix} n \\ i \end{pmatrix}$.

**Definition 5.1.3** *A subspace $Q$ of $\mathbb{C}^{p^n}$ ia called a quantum code with level $p$ and length $n$. Let $K = dim_{\mathbb{C}} Q$, and $k = log_p K$. Then $0 \le k \le n$.*

*A quantum code $Q$ has minimal distance $d(\ge 1)$ if $|v_1>, |v_2> \in Q$, $<v_1|v_2>= 0$ and $e \in E_n$, $w_Q(e) \le d - 1$ then $<v_1|e|v_2>= 0$ where $<v_1|v_2>$ denotes the hermitian inner product in $\mathbb{C}^{p^n}$.*

*A quantum code $Q$ with parameters $n, K($ or $k)$ and $d$ can be expressed by $((n, K, d))_p$ or $[[n, k, d]]_p$ .*

*A quantum code $Q$ has ability to correct $\leq l$ errors if $|v_1>, |v_2>\in Q,\ <v_1|v_2>= 0$ and $e_1, e_2 \in E_n,\ w_Q(e_1)\leq l,\ w_Q(e_2)\leq l$ imply $<v_1|e_1e_2|v_2>=0$.*

**Lemma 5.1.4** *A $[[n,k,d]]_p$ quantum code can correct $\leq [\frac{d-1}{2}]$ quantum errors.*

**Lemma 5.1.5** *(Quantum Singleton bound) For any $[[n,k,d]]_p$ quantum code, $n \geq k+2(d-1)$.*

A quantum code $Q$ has minimal distance $d$ is called pure if the subspaces $eQ$ ($e \in E_n,\ w_Q(e)\leq [\frac{d-1}{2}]$) is orthogonal to each others.

**Lemma 5.1.6** *(Quantum Hamming bound) For any pure $((n,K,d))_p$ quantum code, $p^n \geq K(\sum\limits_{i=0}^{l}(p^2-1)^i \begin{pmatrix} n \\ i \end{pmatrix})$ where $l=[\frac{d-1}{2}]$.*

The theorem 3.2.1, 3.2.1 and 3.3.2 can be generalized to construct nonbinary quantum codes.

**Theorem 5.1.7** *Suppose that $C$ is a linear code in $\mathbb{F}_p^{2n}, k = dim_{\mathbb{F}_p}C$ and $C$ is symplectic self-orthogonal ($C \subseteq C_s^{\perp}$). Then there exists quantum code $[[n,n-k,d]]_p$ where*

$$d = min\{w_Q(v)|\ v \in C_s^{\perp}\setminus C\}$$

**Theorem 5.1.8** *Suppose that there exists a $[[n,k,d]]_p$ linear code $C$ in $\mathbb{F}_p^n$ and $C \supseteq C^{\perp}$ where $C^{\perp}$ is the dual code of $C$ with respect to the ordinary inner product in $\mathbb{F}_p^n:\ (a,b)=\sum_{i=1}^n a_ib_i \in \mathbb{F}_p$. Then we have quantum code $[[n,2k-n,d]]_p$ .*

**Theorem 5.1.9** *If we have linear codes $C_1=[n,k_1,d_1]_p$ and $C_2=[n,k_2,d_2]_p$ in $\mathbb{F}_p^n$ such that $C_1^{\perp}\subseteq C_2$, then we have quantum code $[[n,k_1+k_2-n, min(d_1,d_2)]]_p$ .*

At last we discuss how to construct quantum codes with level $p$ from classical codes in $\mathbb{F}_{p^2}^n$. We define the trace-hermitian inner product $(\ ,\ )_{th}$ in $\mathbb{F}_{p^2}^n$ as follows. For $a=(a_1,\cdots,a_n), b=(b_1,\cdots,b_n)\in \mathbb{F}_{p^2}^n$,

$$(a,b)_{th} = Tr((a^p,b)) = Tr(\sum_{i=1}^n a_i^p b_i) = \sum_{i=1}^n (a_i^p b_i + a_i b_i^p) \in \mathbb{F}_p$$

For an additive subgroup $C$ of $\mathbb{F}_{p^2}^n$, let

$$C_{th}^{\perp} = \{v \in \mathbb{F}_{p^2}^n|\ (v,c)_{th}=0 \text{ for all } c \in C\}$$

**Theorem 5.1.10** *Let $C$ be an additive subgroup of $\mathbb{F}_{p^2}^n$ and $C \subseteq C_{th}^{\perp},\ |C| = p^{n-k}$. Then we have quantum code $[[n,k,d]]_p$ where*

$$d = min\{w_H(v)|\ v \in C_{th}^{\perp}\setminus C\}.$$

## §5.2 Graphic Method to construct nonbinary Quantum Codes

In this section we introduce a new method to construct nonbinary quantum codes given by A. Schlingemann and R. F. Werner in [SW00]. It seems that many quantum codes can be construct by this graphic (or matrix) method.

Let $V$ be a finite set, $v = |V|$. Each symmetric matrix over $\mathbb{F}_p$

$$A = (a_{ij})_{i,j \in V} \quad (a_{ij} \in \mathbb{F}_p,\ a_{ij} = a_{ji})$$

can be considered as a graph $G = G(A)$. The vertix set of $G$ is $V$ and each edge $\overline{ij}$ $(i, j \in V)$ is weighted by $a_{ij}(= a_{ji}) \in \mathbb{F}_p$.

For two subsets $X$ and $Y$ of $V$, let $A_{XY}$ be the submatrix of $A$

$$A_{XY} = (a_{ij})_{i \in X, j \in Y}$$

We denote $\mathbb{F}_p^X = \mathbb{F}_p^{|X|}$ and $d^X = (d^x)_{x \in X}$ as a column vector in $\mathbb{F}_p^X$. For example, let $V = X \bigcup Y$ and $X \bigcap Y = \emptyset$, then a column vector in $\mathbb{F}_p^V = \mathbb{F}_p^v$ can be written by $d^V = \begin{pmatrix} d^X \\ d^Y \end{pmatrix}$ and

$$Ad^V = \begin{pmatrix} A_{XX} & A_{XY} \\ A_{YX} & A_{YY} \end{pmatrix} \begin{pmatrix} d^X \\ d^Y \end{pmatrix} = \begin{pmatrix} A_{XX}d^X + A_{XY}d^Y \\ A_{YX}d^X + A_{YY}d^Y \end{pmatrix}$$

**Theorem 5.2.1**([SW00]) *Let $p$ be an odd prime number, $X$ and $Y$ be disjoint sets, $|X| = k, |Y| = n \geq k + 2(d-1),\ d \geq 2$. $A = (a_{ij})_{i,j \in X \bigcup Y}$ be a symmetric matrix over $\mathbb{F}_p$ with size $(n+k) \times (n+k)$. For each $E \subseteq Y, |E| = d-1$, let $I = Y \setminus E$. Consider the following two statements for $d^X \in \mathbb{F}_p^X$ and $d^E \in \mathbb{F}_p^E$.*

*(1) $A_{IX}d^X + A_{IE}d^E = O^I$ (zero vector in $\mathbb{F}_p^I$)*

*(2) $d^X = O^X$ and $A_{XE}d^E = O^X$*

*If (1) implies (2) for any subset $E \subseteq Y, |E| = d-1$, then there exists quantum code $[[n, k, d]]_p$ .*

**Proof** Here we present a new proof.

Let $|X| = k,\ |Y| = n \geq k + 2(d-1),\ d \geq 2$ and $X \bigcap Y = \emptyset$. Suppose that there exists a symmetric matrix $A = (a_{ij})_{i,j \in X \bigcup Y}$ over $\mathbb{F}_p$ satisfying the following condition.

For each $E \subseteq Y, |E| = d-1$ and $I = Y \setminus E$, if $d^X \in \mathbb{F}_p^X,\ d^E \in \mathbb{F}_p^E$ and $A_{IX}d^X + A_{IE}d^E = O^I$, then $d^X = O^X$ and $A_{XE}d^E = O^X$ (5)

We define a $\mathbb{C}-$linear mapping

$$\begin{array}{llll} f: & (\mathbb{C}^p)^{\otimes k} & \to & (\mathbb{C}^p)^{\otimes n} \\ & |v> & \mapsto & f(|v>) \end{array}$$

where for an element

$$|v> = \sum_{a=(a_1,\ \cdots,\ a_k) \in \mathbb{F}_p^k} c_a |a> = \sum_{d^X \in \mathbb{F}_p^X} c(d^X)|d^X> \in (\mathbb{C}^p)^{\otimes k}, \quad (c_a, c(d^X) \in C)$$

we define

$$f(|v>) = \sum_{d^Y \in \mathbb{F}_p^Y} f_v(d^Y)|d^Y> \in (\mathbb{C}^p)^{\otimes n}$$

where

$$f_v(d^Y) = \sum_{d^X \in \mathbb{F}_p^X} \zeta_p^{\frac{1}{2}((d^X)^t,\ (d^Y)^t)A\begin{pmatrix} d^X \\ d^Y \end{pmatrix}} c(d^X) \ \in \mathbb{C}$$

Let $Q$ be the image of $f$, $Q = \{f(|v>) : \ |v> \in (\mathbb{C}^p)^{\otimes k}\}$. We show that $Q$ is a quantum code $[[n,k,d]]_p$ .

At first we show that $dim_{\mathbb{C}} Q = 2^k$. Since $dim_{\mathbb{C}}(\mathbb{C}^p)^{\otimes k} = 2^k$ and $f$ is $\mathbb{C}-$linear mapping, we need to show that $f$ is injective. Namely, if $|v> = \sum_{d^X \in \mathbb{F}_p^X} c(d^X)|d^X>$ and $f(|v>) = 0$, we need to prove that $c(d^X) = 0$ for all $d^X \in \mathbb{F}_p^X$.

Assume that $f(|v>) = 0$ which means that

$$\sum_{d^X} \zeta_p^{\frac{1}{2}((d^X)^t,\ (d^Y)^t)A\begin{pmatrix} d^X \\ d^Y \end{pmatrix}} c(d^X) = 0 \quad (\text{for all } d^X \in \mathbb{F}_p^X) \quad (6)$$

Since

$$\frac{1}{2}((d^X)^t,\ (d^Y)^t)A\begin{pmatrix} d^X \\ d^Y \end{pmatrix} = \frac{1}{2}(d^X)^t A_{XX} d^X + \frac{1}{2}(d^Y)^t A_{YY} d^Y + (d^Y)^t A_{YX} d^X$$

the (6) becomes that

$$\sum_{d^X} \alpha(d^X)\zeta_p^{(d^Y)^t A_{YX} d^X} = 0 \quad (\text{for all } d^Y \in \mathbb{F}_p^Y) \quad (7)$$

where

$$\alpha(d^X) = \zeta_p^{\frac{1}{2}(d^X)^t A_{XX} d^X} c(d^X) \qquad (8)$$

$A_{YX}$ is a matrix over $\mathbb{F}_p$ with size $n \times k$ ($n > k$). Now we prove that $rank_{\mathbb{F}_p} A_{YX} = k$. If $rank_{\mathbb{F}_p} A_{YX} < k$, then the $k$ columns of $A_{YX}$ are $\mathbb{F}_p-$linear dependent. Thus the $k$ columns of $A_{IX}$ are also $\mathbb{F}_p-$linear dependent for each $I \subseteq Y, |T| = d-1$. Therefore we have $d^X \neq O^X$ such that $A_{IX}d^X = O^I$. Let $d^E = O^E$. Then $A_{IX}d^X + A_{IE}d^E = O^I$. By the condition (5) we should have $d^X = O^X$ which contradicts to our choosing $d^X \neq O^X$. Therefore $rank_{\mathbb{F}_p} A_{YX} = k$. Then we have invertible matrices $P$ and $R$ over $\mathbb{F}_p$ with size $n \times n$ and $k \times k$ respectively such that $A_{YX} = P\begin{pmatrix} I^k \\ 0 \end{pmatrix}R^{-1}$. The formula (7) becomes

$$\begin{aligned} 0 &= \textstyle\sum_{d^X} \alpha(d^X)\zeta_p^{(d^Y)^t P\begin{pmatrix} I^k \\ 0 \end{pmatrix}R^{-1}d^X} = \textstyle\sum_{g^X \in \mathbb{F}_p^X} \alpha(Rg^X)\zeta_p^{(h^Y)^t\begin{pmatrix} I^k \\ 0 \end{pmatrix}g^X} \\ &= \textstyle\sum_{g^X \in \mathbb{F}_p^X} \alpha(Rg^X)\zeta_p^{h_1g_1+\cdots+h_kg_k} \qquad (h_1,\cdots,h_k \in \mathbb{F}_p) \quad (9) \end{aligned}$$

where

$$g^X = (g_1, \cdots, g_k)^t = R^{-1} d^X, \qquad (h^Y)^t = (h_1, \cdots, h_n) = (d^Y)^t P$$

The formula (9) implies that for each $a^X = (a_1, \cdots, a_k) \in \mathbb{F}_p^X$,

$$\begin{aligned} 0 &= \sum_{(h_1,\cdots,h_k)\in\mathbb{F}_p^k} \zeta_p^{-(h_1a_1+\cdots+h_ka_k)} \sum_{g^X\in\mathbb{F}_p^X} \alpha(Rg^X)\zeta_p^{h_1g_1+\cdots+h_kg_k} \\ &= \sum_{g^X\in\mathbb{F}_p^X} \alpha(Rg^X) \sum_{(h_1,\cdots,h_k)\in\mathbb{F}_p^k} \zeta_p^{h_1(g_1-a_1)+\cdots+h_k(g_k-a_k)} \\ &= p^k \alpha(Ra^X) \end{aligned}$$

Since $R$ is invertible, we know that $\alpha(d^X) = 0$ and $c(d^X) = 0$ (by (8)) for all $d^X \in \mathbb{F}_p^X$ which means that $|v >= 0$. Therefore we proved that $dim_{\mathbb{C}} Q = 2^k$.

Next we prove that $Q$ has minimal distance $d$. Suppose that

$$|w >= f(|v >) = \sum_{d^Y} f_v(d^Y)|d^Y > \in Q, \quad |w' >= f(|v' >) = \sum_{d^Y} f_{v'}(d^Y)|d^Y > \in Q$$

and $< w'|w >= 0$, where

$$f_v(d^Y) = \sum_{d^X} \zeta_p^{\frac{1}{2}((d^X)^t,\ (d^Y)^t)A\begin{pmatrix} d^X \\ d^Y \end{pmatrix}} c(d^X)$$

$$f_{v'}(d^Y) = \sum_{d^X} \zeta_p^{\frac{1}{2}((d^X)^t,\ (d^Y)^t)A\begin{pmatrix} d^X \\ d^Y \end{pmatrix}} c'(d^X)$$

We need to show that $< w'|e|w >= 0$ for each $e \in E_n,\ w_Q(e) \le d-1$. For such $e$ we can find $E \subseteq Y,\ |E| = d-1,\ I = Y \setminus E$ such that

$$e|d^E, d^I >= \zeta_p^{(s^E,\ d^E)}|d^E + l^E,\ d^I > \qquad (s^E,\ l^E \in \mathbb{F}_p^E)$$

Therefore

$$\begin{aligned} e|w > &= \sum_{d^Y} f_v(d^Y) e|d^Y > \\ &= \sum_{d^E,\ d^I} \sum_{d^Y} \zeta_p^{(s^E,\ d^E)+\frac{1}{2}((d^X)^t),(d^E)^t),(d^I)^t)A\begin{pmatrix} d^X \\ d^E \\ d^I \end{pmatrix}} c(d^X)|d^E + l^E, d^I > \\ &= \sum_{d^E,\ d^I} \sum_{d^Y} \zeta_p^{(s^E,\ d^E)+\frac{1}{2}((d^X)^t,(d^E-l^E)^t,(d^I)^t)A\begin{pmatrix} d^X \\ d^E - l^E \\ d^I \end{pmatrix}} c(d^X)|d^E, d^I > \end{aligned}$$

and

$$< w'|e|w >= \sum_{d^E, d^I} \sum_{d^X, (d')^X} \zeta_p^m \overline{c'(d'^X)} c(d^X)$$

where

$$\begin{aligned} m &= (s^E,\ d^E) + \tfrac{1}{2}((d^X)^t, (d^E - l^E)^t, (d^I)^t) A \begin{pmatrix} d^X \\ d^E - l^E \\ d^I \end{pmatrix} \\ & -\tfrac{1}{2}((d'^X)^t, (d^E)^t, (d^I)^t) A \begin{pmatrix} d'^X \\ d^E \\ d^I \end{pmatrix} \\ &= (s^E,\ d^E) + \tfrac{1}{2}(d^X)^t A d^X - \tfrac{1}{2}(d'^X)^t A d'^X + (d^X - d'^X)^t (A_{XE} d^E + A_{XI} d^I) \\ & -(d^X)^t A_{XE} l^E - (l^E)^t A_{EE} d^E + \tfrac{1}{2}(l^E)^t A_{EE} l^E - (l^E)^t A_{EI} d^I \qquad (10) \end{aligned}$$

The terms in $m$ related to $d^I$ is

$$(d^X - d'^X)^t A_{XI} d^I - (l^E)^t A_{EI} d^I = (d^I)^t (A_{IX}(d^X - d'^X) - A_{IE} l^E)$$

Therefore, if $A_{IX}(d^X - d'X) - A_{IE} l^E = a^I \neq O^I$, then

$$< w'|e|w >= \sum_{d^E, d^X, (d')^X} \cdots \sum_{d^I} \zeta_p^{(d^I,\ a^I)} = 0$$

If $A_{IX}(d^X - d'^X) - A_{IE} l^E = O^I$, by condition (5) we have $d^X - d'^X = O^X$ and $A_{XE} l^E = O^X$ so that (10) becomes

$$m = (s^E,\ d^E) - (l^E)^t A_{EE} d^E + \frac{1}{2}(l^E)^t A_{EE} l^E - (l^E)^t A_{EI} d^I$$

which is independent on $d^X (= d'^X)$. Therefore

$$< w'|e|w >= \alpha \cdot \sum_{d^X} \overline{c'(d'^X)} c(d^X) = \alpha < v'|v > \qquad (\alpha \in \mathbb{C}) \qquad (11)$$

On the other hand,

$$0 =< w'|w >= \sum_{d^Y} \sum_{d^X,\ d'^X} c(d^X) \overline{c'(d'^X)} \zeta_p^N \qquad (12)$$

where

$$\begin{aligned} N &= \tfrac{1}{2}((d^X)^t, (d^Y)^t) A \begin{pmatrix} d^X \\ d^Y \end{pmatrix} - \tfrac{1}{2}((d'^X)^t, (d^Y)^t) A \begin{pmatrix} d'^X \\ d^Y \end{pmatrix} \\ &= \tfrac{1}{2}(d^X)^t A_{XX} d^X - \tfrac{1}{2}(d'^X)^t A_{XX} d'^X + (d^Y)^t A_{YX}(d^X - d'^X) \end{aligned}$$

From $rank_{\mathbb{F}_p} A_{YX} = k$ we can show as before that

$$\sum_{d^Y} \zeta_p^{(d^Y)^t A_{YX}(d^X - d'^X)} = \begin{cases} p^n, & \text{if } d^X = d'^X \\ 0, & \text{otherwise} \end{cases}$$

Then the formula (12) becomes

$$0 = p^n \sum_{d^X} c(d^X)\overline{c'(d^X)} = p^n < v'|v >$$

By (11) we have $< w'|e|w >= 0$. This completes the proof of theorem 5.2.1 . $\square$

The condition (1) in theorem can be rewritten as

$$[A_{IX}\ A_{IE}] \begin{pmatrix} d^X \\ d^E \end{pmatrix} = O^I \qquad (*)$$

If $n = k + 2(d-1)$, then $|X \bigcup E| = k + d - 1 = |I|$ so that $[A_{IX}\ A_{IE}]$ is a matrix os size $(k + d - 1) \times (k + d - 1)$. If this matrix is invertible over $\mathbb{F}_p$, then the condition (1) of theorem (5.2.1) (which is the same as $(*)$ ) implies $d^X = O^X$ and $d^E = O^E$ so that the condition (2) of the theorem is satisfied. Thus we have following

**Theorem 5.2.2** *Let $p$ be an odd prime number, $X$ and $Y$ be two disjoint sets, $|X| = k, |Y| = n = k + 2(d-1)$, $d \geq 2$. $A = (a_{ij})_{i,j \in X \bigcup Y}$ be a symmetric matrix over $\mathbb{F}_p$. If the submatrix $[A_{IX}\ A_{IE}]$ is invertible over $\mathbb{F}_p$ for any subset $E$ of $Y$, $|E| = d-1$ and $I = Y \setminus E$, then there exists quantum code $[[n, k, d]]_p$ (which reaches the Singleton bound).*

We may call the quantum codes constructed in theorem 5.2.2 by graphic quantum codes. One advantage of graphic quantum codes is shown in following result.

**Theorem 5.2.3** *If there exists quantum code $[[n, k, d]]_p$ ($d \geq 2, n = k+2(d-1)$), then for each $i, 1 \leq i \leq d-2$, there exists (graphic) quantum code $[[n-i, k+i, d-i]]_p$.*

**Proof** By assumption we know that there exists a symmetric matrix

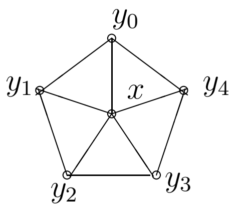
$$A = (a_{ij})_{i,j \in X \bigcup Y} \qquad (|X| = k, |Y| = n, X \bigcap Y = \emptyset)$$

over $\mathbb{F}_p$ such that for each $E \subseteq Y, |E| = d-1, I = Y \setminus E$ the matrix $[A_{IX}\ A_{IE}]$ is invertible. Now we choose $T \subseteq Y, |T| = i$ and let $X' = X \bigcup T, Y' = Y \setminus T$. Then $|X'| = k + i, |Y'| = n - i$. For each $E' \subseteq Y', |E'| = d - i - 1$ and $I' = Y' \setminus E'$, let $E = T \bigcup E' \subseteq Y$ and $I = I'$, then $|E| = d - 1, I = Y \setminus E$ and $X' \bigcup E' = X \bigcup E$ so that $[A_{I'X'}\ A_{I'E'}] = [A_{IX}\ A_{IE}]$ up to a permutation of columns. By assumption this matrix is invertible. Thus there exists graphic quantum code $[[n-i, k+i, d-i]]_p$. $\square$

**Example** Rains[R99(1)] proved that there exists quantum code $[[5, 1, 3]]_p$ for all $p \geq 3$. Schlingemann and Werner [SW00] present another proof by using theorem

5.2.2. Let $X = \{x\}$, $Y = \{y_0, y_1, y_2, y_3, y_4\} = \{y_i | \ i \in \mathbb{Z}/5\mathbb{Z}\}$. Consider the following symmetric matrix

$$A = \begin{array}{c} \\ x \\ y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{array} \begin{array}{c} \begin{array}{cccccc} x & y_0 & y_1 & y_2 & y_3 & y_4 \end{array} \\ \left[\begin{array}{cccccc} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right] \end{array}$$




(graph G)

The graph $G$ corresponded to $A$ is shown in the right-hand side. For $E = \{y_i, y_j\}$ $(0 \le i \ne j \le 4)$ and $I = Y \setminus E$, we denote the determinant $A_{(ij)} = |A_{IX} \ A_{IE}|$. From the cyclic properties of the graph $G$ we know that $A_{(ij)} = A_{(i+1,j+1)}$. Thus we need to compute $A_{(01)}$, and $A_{(02)}$.

$$|A_{(01)}| = \begin{vmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{vmatrix} = 1, \quad |A_{(02)}| = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix} = 1$$

By theorem 5.2.2, there exist (graphic) quantum code $[[5, 1, 3]]_p$ for all $p \ge 3$. In fact, from theorem 5.2.3 we know that there exist $[[4, 2, 2]]_p$ for all $p \ge 3$.

With a little more number theory and combinatorics, we can show that there exist $[[6, 2, 3]]_p$, $[[5, 3, 2]]_p$ and $[[7, 3, 3]]_p$ for all $p \ge 3$ [F01].

**Theorem 5.2.4** *Let $d \ge 2, k \ge 0, n = k + 2(d-1)$. Then there exists graphic quantum code $[[n, k, d]]_p$ for each prime number $p \ge \left(\begin{array}{c} n \\ d-1 \end{array}\right) + 1$.*

**Proof** Let$X \bigcap Y = \emptyset, |X| = k, |Y| = n$. Consider the set $S$ of all zero-diagonal symmetry matrices over $\mathbb{F}_p$.

$$S = \{A = (a_{ij})_{i,j \in X \bigcup Y} | \ a_{ij} \in \mathbb{F}_p, a_{ij} = a_{ji}, a_{ii} = 0\}$$

There are $\frac{1}{2}\left(\begin{array}{c} n \\ 2 \end{array}\right)$ independent entries $a_{ij}$ in $A$, thus $|S| = p^{\frac{1}{2}\left(\begin{array}{c} n \\ 2 \end{array}\right)}$. For each $E \subseteq Y, |E| = d-1$ and $I = Y \setminus E$, the matrix $[A_{IX} \ A_{IE}]$ have $(k+d-1)^2$ independent entries since $I \bigcap (X \bigcup E) = \emptyset$. It is well know that the number of invertible matrices with size $l$ over $\mathbb{F}_p$ is

$$|GL_l(\mathbb{F}_p)| = \prod_{i=0}^{l} (p^l - p^i)$$

Therefore

$$\begin{aligned}
\sharp\{A \in S|\ |A_{IX}A_{IE}| \neq 0\} &= |GL_{k+d-1}(\mathbb{F}_p)| \cdot p^{\frac{1}{2}\binom{n}{2}-(k+d-1)^2} \\
\sharp\{A \in S|\ |A_{IX}A_{IE}| = 0\} &= p^{\frac{1}{2}\binom{n}{2}} - |GL_{k+d-1}(\mathbb{F}_p)| \cdot p^{\frac{1}{2}\binom{n}{2}-(k+d-1)^2} \\
&= p^{\frac{1}{2}\binom{n}{2}}(1 - \prod_{i=1}^{k+d-1}(1 - \tfrac{1}{p^i}))
\end{aligned}$$

There are $\binom{n}{d-1}$ subset $E$ of $Y$ such that $|E| = d-1$. Therefore if

$$p^{\frac{1}{2}\binom{n}{2}} > \binom{n}{d-1} p^{\frac{1}{2}\binom{n}{2}}(1 - \prod_{i=1}^{k+d-1}(1 - \frac{1}{p^i})) \qquad (*)$$

then there exists $A \in S$ such that $|A_{IX}A_{IE}| \neq 0$ for all $E \subseteq Y, |E| = d-1$ and $I = Y \setminus E$ which implies the existence of graphic quantum code $[[n,k,d]]_p$ by lemma 5.2.3. It is easy to see that the condition $(*)$ is equivalent to $\prod_{i=1}^{k+d-1}(1 - \frac{1}{p^i}) > 1 - \binom{n}{d-1}^{-1}$. Moreover, if $p \geq \binom{n}{d-1} + 1$, then

$$\prod_{i=1}^{k+d-1}(1 - \frac{1}{p^i}) \geq 1 - \sum_{i=1}^{k+d-1}\frac{1}{p^i} > 1 - \sum_{i=1}^{\infty}\frac{1}{p^i} = 1 - \frac{1}{p-1} \geq 1 - \binom{n}{d-1}^{-1}.$$

This completes the proof of theorem 5.2.4. $\square$

# References


[AK00] A. Ashikhim and E.Knill, Non-binary quantum stabilizer codes, quant-ph/0005008, 2000.

[AL99] A. Ashikhim and S.Litsyn, Upper bounds on the size of quantum codes, IEEE Trans. IT-45(1999),1206-1215.

[ALT00] A. Ashikhim, S.Litsyn, and M.A. Tsfasman, Asymptotically good quantum codes, quant-ph/0006061,2000.

[BDSW96] C.H.Bennett, D.P.Divincenzo, J.A. Smolin and W.K. Wootters, Mixed state entanglement and quantum error correction. Phys. Rev. A, 54(1996), 3824-3851.

[C01] Hao Chen, Some good quantum error-correcting codes from algebraic-geometry codes, IEEE Trans. IT-47(2001), 2059-2061.

[CEL99] G. Cohen, S.Encheva and S.Litsyn, On binary consructions of quantum codes, IEEE Trans. IT-45(1999), 2495-2498.

[CL99] Hao Chen and J. H. Lai, Construction of quantum error-correcting codes via algebraic-geometry codes, preprint, 1999.

[CLX01] H. Chen, S. Ling and C. Xing, Asympototically good quantum codes exceeding the Ashikhim-Litsyn-Tsfasman bound, IEEE Trans. IT-47(2001), 2055-2058.

[CLX01] H. Chen, S. Ling and C. Xing, Quantum codes from concatenated Reed-Soloman codes, Preprint, 2001.

[CRSS97] A.R.Calderbank, E.M.Rains, P.W.Shor and N.S.Sloane, Quantum error correction and orthogonal geometry, Phys. Rev. Lett, 78(1997), 405-408.

[CRSS98] A.R.Calderbank, E.M.Rains, P.W.Shor and N.S.Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. IT-44(1998), 1369-1387.

[CS96] A.R.Calderbank, P.W.Shor, Good quantum error-correcting codes exist, Phys. Rev. A 54(1996), 1098-1105.

[F01] K.Feng, Quantum codes $[[6,2,3]]_p$ and $[[7,3,3]]_p$ ($p \geq 3$) exist, preprint, 2001.

[GB99] M.Grassl and T. Beth, Quantum BCH codes, quant-ph/9910060, 1999.

[GGB99] M.Grassl, W. Geiselmann and T.Beth, Quantum Reed-Solomon codes, In proceedings AAECC-13, LNCS 1719, Springer-Verlag, 1999, pp. 231-244.

[G96] D. Gottesman, Class of quantum error correcting codes saturating the quantum Hamming bound, Phys. Rev. A, 54(1996), 1862-1868.

[G97] D. Gottesman, Stabilizator codes and quantum error correction, PhD thesis, CIT,1997, quant-ph/9705052.

[G00] D. Gottesman, <An introduction to Quantum Error Correction>. Proceedings of Symposia in Applied Mathematics, 2000.

[Gr99] J.Gruska, < Quantum Computing>, The McGraw-Hill Compainies, London, 1999.

[K96(1)] E. H. Knill, Non-binary unity error bases and quantum codes, quant-ph/9608048, May, 1996.

[K96(2)] E. H. Knill, Group reprensentations, error bases and quantum codes, quant-ph/9608048, Aug, 1996.

[KL97] E. H. Knill, and R.Laflamme, Theory of quantum error-correcting codes, Phys. Rev. A, 55(1997), 900-911.

[LMPZ96] R.Laflamme, C. Miquel, J.Paz and W.H.Zurek, Perfect quantum error correction code, Phys. Rev. Lett.,77(1996), 198-201.

[L82] J.H. Van Lint, <Introduction to Coding Theory>, Springer-Varlag, NY, 1982.

[LN86] R. Lidl and H. Niederreiter, <Introduction to Finite Fields and Their Applications>, Cambridge Univ. Press,1986.

[MS77] F. J. MacWilliams and N.J.A. Sloane, <The Theory of Error-Correcting Codes>, North-Holland, Amsterdam, 1977.

[MU99] R. Matsumoto and T. Uyematsu, Constructing quantum error-correcting codes for $p^m-$state systems from classical error-correcting codes, quant-phy/9911011, 1999.

[P93] A. Peres,<Quantum Theory: Concepts and Methods.> Kluwer Acad. Pub., 1993.

[R98] E. M. Rains, Quantum weight enumerators, IEEE Trans. IT-44(1998), 1388-1394.

[R99(1)] E. M. Rains, Non-binary quantum codes, IEEE Trans. IT-45(1999), 1827-1832.

[R99(2)] E. M. Rains, Quantum codes of minimal distance two, IEEE Trans. IT-45(1999), 266-271.

[R99(3)] E. M. Rains, Quantum shadow enumerators, IEEE Trans. IT-45(1999), 2361-2366.

[R00] E. M. Rains, Polynomial invarians of quantum codes, IEEE Trans. IT-46(2000), 54-59.

[RHSS97] E. M. Rains, R. H. Hardin, P. W. Shor and N. J. A. Sloane, A nonadditive quantum code, Phys. Rev. Lett. 79(1997), 953-954.

[SW00] A. Schlingemann and R. F. Werner, Quantum error-correcting codes associated with graphs, quant-ph/00012111, 2000.

[S95] P. W. Shor, Scheme for reducing decoherence in quantum computer mempry, Phys. Rev. A, 52(1995), 2493-2496.

[SL97] P. W. Shor and R.Laflamme, Quantum analog of the MacWilliams identities in class coding theory, Phy. Rev. Lett. 78(1997), 1600-1602.

[St96(1)] A. M. Steane, Multiple particle interference and quantum error correction, Proc. Roy. Soc. Lond. A, 452(1996), 2551-2577.

[St96(2)] A. M. Steane, Error correcting codes in quantum theory, Phys. Rev. Lett. 77 (1996), 793-797.

[St96(3)] A. M. Steane, Simple quantum error correction codes, Phys. Rev. Lett. 77 (1996), 7.

[St99(1)] A. M. Steane, Quantum Reed-Muller codes, IEEE Trans. IT-45(1999), 1701-1704.

[St99(2)] A. M. Steane, Enlargement of Calderbank-Shor-Steane quantum codes, IEEE Trans. IT-45(1999), 2492-2495.

[TM00] A. Thangaraj and S. W. Mclaughlin, Quantum codes from cyclic codes over $GF(4^m)$, quant-ph/008129, 2000.