The Quantum Structure of Two-Point Algebraic Geometric Codes on Hermitian Curve

Jingqi Huang [a] and Wei Liu [b]

School of Information Engineering, Henan University of Science and Technology, Luoyang 200072, China.

[a]hjq_0521@foxmail.com, [b]liuwei_0613@126.com

Abstract

In order to correct or prevent the quantum error caused by quantum noise in quantum communication and improve the anti-jamming ability of information, a method of constructing quantum code using algebraic geometry code is proposed. Algebraic geometry code has good performance parameters and the ability to detect and correct errors, so the quantum code constructed using algebraic geometry code also has good performance. Using the CSS construction method, a series of quantum two-point codes on a Hermitian curve are constructed, and the parameters such as the dimension and the minimum distance of the quantum code are calculated. Finally, comparing with the quantum Hermitian one-point code, it is shown that the two-point code has better performance parameters than the one-point code.

Keywords

Algebraic-geometry code, Hermitian curve, Quantum error correction code, two-point code.

1. Introduction

Quantam computer is a combination of quantum mechanics and computational problems. It is a research hotspot in recent years and has aroused widespread social attention [1]. Quantum coherence plays a fundamental role in various fields of quantum information theory (quantum computer, quantum cryptography and quantum communication [2], etc.). But under the influence of noise in quantum channels, the information carried by quantum states is destroyed. Quantum coherence inevitably decays exponentially with time, leading to quantum decoherence [3]. Therefore, whether or not the noise can be effectively controlled can be said to play a decisive role in whether the quantum operation process can be effectively realized. The function of quantum error correcting code (hereinafter referred to as quantum code) is to protect quantum information from noise interference, which is very important for quantum computing. Although the basic idea of quantum code and classical code is the same, it is necessary to introduce information redundancy appropriately to improve the anti-interference ability of codeword. However, the physical characteristics of quantum state determine that it is not a simple extension of classical code, and its coding method is more Complex [4]. The first quantum code was discovered by Peter Shor in 1995, which led to efforts to find quantum codes that are more efficient and can correct more errors [5]. In the second year, Shor and Calderbank discovered the first family of quantum error correction codes [6]. In recent years, various types of quantum codes have emerged [7-9].

Algebraic geometry was discovered by Goppa in the 1980s. This discovery made the abstract branch of mathematics, algebraic geometry, applied to communication engineering through coding theory. Starting with the history of algebraic geometry, people have studied the code on the Hermitian curve. The first systematic method of constructing a one-point code on a Hermitian curve was proposed by Tiersma, who found that the dual code of a one-point code on the Hermitian curve is also a one-point code on the curve [10]. Subsequently, Stichtenoth studied the dimension and minimum distance of a one-point code on any q, Hermitian curve [11]. In 2001, Matthews studied the two-point code on the Hermitian curve [12]. Homma and Kim give a complete description of the minimum distances of all two-point Hermitian codes in [13], [14], [15], [16]. [17], further discussion in [18] and [19] has

improved our understanding of these codes. The two-point code has better parameters than the one-point code while maintaining the ease of construction.

This paper studies quantum error correction codes constructed with algebraic geometry codes. In particular, we studied the quantum codes obtained from the two-point code on the Hermitian curve and estimated the relevant parameters of these codes, which show their coding efficiency and error correction capability. In [20], the quantum code from the one-point Hermitian code is studied. We will compare it to prove that the quantum two-point code has better performance parameters than the one-point code.

2. Basic Concepts

2.1 Quantum Code

Definition 1[21] (Quantum code): The negative vector subspace Q of each dimension ≥ 1 of the Hilbert space $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$ is called a quantum error correcting code, where n is the code length of the code Q, and the dimension of Q is $K = \dim_{\mathbb{C}} Q$, $k = \log_2 K$, since $1 \leq K \leq 2^n$, so $0 \leq k \leq n$.

Definition 2 (Error correction capability): A binary quantum error correcting code $[[n,k,d]]_2$ is a 2^k-dimensional subspace of the Hilbert space $\mathbb{C}^{2^n} = (\mathbb{C}^2)^{\otimes n}$, and can correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ quantum errors.

The quantum stable subcode is a subspace of the q^n-dimensional complex Hilbert space $\mathbb{C}^{q^n}$, so that G represents all matrix operators acting on $\mathbb{C}^{q^n}$, and the matrix operator with eigenvalue 1 in the operator set G constitutes a finite Abelian group. The Abel subgroup is called the stable of the quantum code, and the resulting quantum code is called a stable subcode. Quantum-stabilized subcodes can be constructed using classical linear codes, proposed by Canlderbank, Stean, and Shor, called CSS constructors.

Lemma 1 (CSS construction): Let C_1 and C_2 be linear codes whose parameters are $[n,k_1,d_1]_{q^2}$ and $[n,k_2,d_2]_{q^2}$ respectively on the finite field $\mathbb{F}_{q^2}$, and satisfy $C_1 \subset C_2$, let $d = \min\{\mathrm{wt}(C_2 \setminus C_1), \mathrm{wt}(C_1^{\perp} \setminus C_2^{\perp})\}$, then there is a quantum code with parameter $[[n,k_2-k_1,d]]_{q^2}$ .If there are $\mathrm{wt}(C_2 \setminus C_1) = \mathrm{wt}(C_2) = d_2$, $\mathrm{wt}(C_1^{\perp} \setminus C_2^{\perp}) = \mathrm{wt}(C_1^{\perp}) = d_1^{\perp}$, the obtained quantum code is pure quantum code.

The literature [22] gives the CSS construction method of binary quantum code, and the literature [23, 24] gives the CSS construction method of q-ary quantum code.

2.2 Hermitian Code

Let X be a non-singular curve with genus g on the finite field $\mathbb{F}_q$, and $D = P_1 + \cdots + P_n$ be a divisor, where $P_1, \cdots, P_n$ is n different rational points on X. Let G be another divisor whose support set does not intersect with the support set of D, ie $SuppD \cap SuppG = \varnothing$. $\mathrm{L}(G) = \{f \in \mathbb{F}_q(X) | div(f) + G \geq 0\} \cup \{0\}$ is the Riemann-Roch space.

Definition 3: Considering the assignment map $L(G) \to F_q^n, f \mapsto (f(P_1), f(P_2), ..., f(P_n))$, it is obvious that this map can be defined and is a linear map. The image of this map is a linear code on $\mathbb{F}_q$, denoted as $C_L(D,G)$, ie

$$C_L(D,G) = \{(f(P_1), ..., f(P_n)) \mid f \in L(G)\} \tag{1}$$

This code is called the first type of algebraic geometry code.

The following describes another definition of algebraic geometry. Let Ω_x be the set of all differential forms on X and $\Omega(G) = \{\omega \in \Omega_x \mid \omega = 0 \text{ or } (\omega) \geq G\}$ be the linear space.

Definition 4: Consider the assignment map $\Omega(G\text{-}D) \to \mathbb{F}_q^n, \omega \mapsto (res_{P_1}(\omega), ..., res_{P_n}(\omega))$, where $res_{P_i}(\omega)$ is the residue of ω at P_i, which can be defined, the mapped image is a linear code on $\mathbb{F}_q$, denoted as $C_\Omega(D,G)$, ie

$$C_\Omega(D,G) = \{(res_{P_1}(\omega), ..., res_{P_n}(\omega)) \mid \omega \in \Omega(G\text{-}D)\} \tag{2}$$

This code is called the second type of algebraic geometry code.

Lemma 2[25]: $C_{\Omega}(D,G)$ is the dual code of $C_L(D,G)$.

We consider the code on the Hermitian curve X, where curve X is a $q+1$ -order plane curve, which is equivalent to a non-homogeneous equation

$$y^q + y = x^{q+1} \tag{3}$$

mapping of q^2 elements on field $\mathbb{F}_{q^2}$.The genus of curve X is $q(q-1)/2$. The literature [25] proves that the number of finite rational points on the Hermitian curve is $n=q^3$ and the number of infinite points is 1. Obviously X has only points $(0,1,0)$ which are infinity points, denoted by P_∞; $P_{\alpha,\beta}$ represents point $(\alpha,\beta,1)$, and abbreviated P_0 to represent $P_{0,0}$. Therational point set $X(\mathbb{F}_{q^2})$ of curve X on $\mathbf{F}_{q^2}$ is $\{P_{\alpha,\beta} \mid \alpha,\beta \in \mathbb{F}_{q^2}, \beta^q+\beta=\alpha^{q+1}\} \bigcup \{P_\infty\}$, which contains q^3+1 points. So X is a great curve in the sense of Hasse-Weil.

3. Classic Hermitian code

3.1 One-point code

Let us review the construction properties of one-point codes on curve X. Since the automorphism group of the curve X on the finite field $\mathbb{F}_{q^2}$ is removable on the $\mathbb{F}_{q^2}$-rational point set $X(\mathbb{F}_{q^2})$ of X, we can assume that the support set of the division G of the one-point code is P_∞. We use C_s to represent a one-point code $C_L(D,sP_\infty)$ on curve X, where the division is $D=\sum_{P\in X(\mathbb{F}_{q^2})\setminus\{P_\infty\}} P$. Specifically, the assignment of C_s is mapped to

$$f \in L(sP_\infty),\ f \mapsto (...,f(P_{\alpha,\beta}),...)_{P_{\alpha,\beta}\in X(\mathbb{F}_{q^2})\setminus\{P_\infty\}\in(\mathbb{F}_{q^2})^{q^3}} \tag{4}$$

Where $L(sP_\infty)=\{f\in\mathbb{F}_{q^2}(X)^* \mid divf+sP_\infty \succ 0\}\bigcup\{0\}$. $\mathbb{F}_{q^2}(X)$ denotes a rational function of curve X on $\mathbb{F}_{q^2}$, $\mathbb{F}_{q^2}(X)^*$ is its non-zero function group, and $divf=\sum_{P\in X} v_P(f)P$, where v_P is the value at P.

We define the parameter

$$\tilde{s}=max\{l \mid l=iq+j(q+1)\le s,\ \ i\ge 0, 0\le j\le q-1\} \tag{5}$$

The dimension and minimum distance of a one-point Hermitian code are given in [26], as shown in Table 1.

Table 1 Dimension and minimum distance of a ONE-point Hermitian code

s	k	d
$0\le s\le q^2-q-2,$ $\tilde{s}=aq+b,\ 0\le b\le a\le q-1$	$\frac{a(a+1)}{2}+b+1$	$n-\tilde{s}$
$q^2-q-2<s<n-q^2+q$	$s+1-\frac{q(q-1)}{2}$	$n-s$
$n-q^2+q<s\le n,$ $s=n-q^2+aq+b,$ $0\le a,b\le q-1$	$s+1-\frac{q(q-1)}{2}$	$n-s$ if $a<b$, $n-s+b$ if $a\ge b$
$n\le s\le n+q^2-q-2,$ $s^\perp=n+q^2-q-2-s,$ $\tilde{s}^\perp=aq+b,\ 0\le a,b\le q-1$	$n-\frac{a(a+1)}{2}-b-1$	$a+2$ if $b=a$ $a+1$ if $b<a$

3.2 Hermitian Code

The classic two-point code is the code $C_L(D,G)$ and $C_\Omega(D,G)$ with the decimation $G=sP+tQ$.

To construct the required two-point Hermitian code, we first need to determine two rational points P and Q. The typical choice is: P is the infinity point P_∞, and Q is zero point P_0. Then, we let the divisor D be $\sum_{P\in X(\mathbb{F}_{q^2})\setminus\{P_\infty,P_0\}} P$, so that the code length of the two-point code we construct is, which makes the code length of the two-point code shorter than the one-point code. In order to compare the performance of these two codes, we shorten the code length of the one-point code. Since the automorphism group of a one-point code is removable on the coordinate set, the choice of coordinates

is not necessary. This feature makes it easy to compare a two-point code with a code length to an equal-sized shortened one-point code.

Homma and Kim give the relevant parameters of the first type of Hermitian two-point code in [13], [14], [15], [16].

Lemma 3: For two different rational points Q, $Q' \in \mathrm{X}(\mathbb{F}_{q^2})$, there is an automorphism map σ of X in $\mathbb{F}_{q^2}$ so that $\sigma(P_\infty)=Q$, $\sigma(P_0)=Q'$.

Due to the nature of the automorphism mapping σ in the above lemma, $C_L(\sum_{P\in X(\mathbb{F}_{q^2})\setminus\{Q,Q'\}}P, sQ+tQ')$ and $C_L(\sum_{P\in X(\mathbb{F}_{q^2})\setminus\{P_\infty,P_0\}}P, sP_\infty+tP_0)$ are equidistant in the sense of Hamming distance. We use $C(s,t)$ to represent $C_L(D, sP_\infty+tP_0)$, where D is $\sum_{P\in X(\mathbb{F}_{q^2})\setminus\{P_\infty,P_0\}}P$. If $n\ge q+1$, there is isomorphism

$$L(sP_\infty+tP_0)\to L((s+q+1)P_\infty+(t-q-1)P_0) \tag{6}$$

By multiplying by y we get an equidistant

$$C(s,t)\xrightarrow{\sim}C(s+q+1,t-q-1) \tag{7}$$

Since there are $y(P)\neq 0$ for all $P\in X(\mathbb{F}_{q^2})\setminus\{P_\infty,P_0\}$, we can assume $0\le t\le q$.

Lemma 4: Given the integer t, $0\le t\le q$. Let $s=aq+b\in A(\mathbb{Z},q)$ be where s is the integer in set $\{s\in\mathbb{Z}\mid \dim C(s,t)=\dim C(s-1,t)+1\}$, $0\le b<q$.

(1) If $0\le \mathrm{b}\le \mathrm{a}\le$ q-t-1, then $\dim C(s,t)=\frac{1}{2}a(a+1)+b+1$.

(2) If $\max\{q-t,b\}\le \mathrm{a}\le$ q-2, then $\dim C(s,t)=\frac{1}{2}a(a+3)+b+t+2-q$.

(3) If $b=q-1, q-t-1\le \mathrm{a}\le$ q-2, then $\dim C(s,t)=\frac{1}{2}(a+2)(a+3)+t-q$.

(4) If $q-1\le \mathrm{a}\le \min\{q^2-1, q^2+q-(t+3)\}$, then $\dim C(s,t)=s+t+1-\frac{1}{2}q(q-1)$.

(5) If $q^2\le \mathrm{a}\le \min\{q^2+q-(t+3), b+q^2-1\}$, then $\dim C(s,t)=s+t+1-\frac{1}{2}q(q-1)-\frac{1}{2}(a-q^2+1)(a-q^2+2)$.

(6) If $\mathrm{b}\le$ q-2, $q^2+q-(t+2)\le \mathrm{a}\le b+\mathrm{q}^2-1$, then $\dim C(s,t)=s+1-\frac{1}{2}q(q-3)-\frac{1}{2}(a-q^2+2)(a-q^2+3)$.

where we let $A(\mathbb{Z},q)$ be an array of integers of infinite length columns

$$\begin{array}{cccc}
\vdots & \vdots & & \vdots \\
-q & -q+1 & \cdots & -q+(q-1) \\
0 & 1 & \cdots & (q-1) \\
q & q+1 & \cdots & q+(q-1) \\
2q & 2q+1 & \cdots & 2q+(q-1) \\
\vdots & \vdots & & \vdots
\end{array}$$

The minimum distance of code $C(s,t)$ is divided into three cases of $\mathrm{t}=0$, $\mathrm{t}=q$ and $1\le t\le q-1$.

Lemma 5: Let $\mathrm{t}=0$

(1) If $s=aq+b\in A(\mathbb{Z},q)$, where $0\le b<q$, and satisfied $0\le \mathrm{b}\le \mathrm{a}\le b+\mathrm{q}^2$-q-1, then $d(C(\mathrm{s},0))=q^3-1-s$

(2) If $s=(q^2-i)q+j$, and $1\le i\le q$, $0\le j\le q-i$, then $d(C(s,0))=iq-1$

(3) If $s=(q^2+k)q+l$, and $-1\le k\le q-3$, $k+1\le l\le q-1$, then $d(C(s,0))=q-2-k$

Regarding $1\le t\le q-1$, there are the following theorems.

Lemma 6: Determine an integer t, $1\le t\le q-1$, and let $s=aq+b$ be a non-negative integer, of which $0\le b<q$.

(1) If $\mathrm{b}\le a\le q-(t+1)$, then $d(C(s,t))=q^3-1-s$

(2) If s satisfies

i) $0 \le b \le q-2,\ q^2-1 \le a \le b+q^2-1$, or

ii) $b = q-1,\ q^2-1 \le a \le q^2+q-(t+3)$,

then $d(C(s,t)) = q^2+q-a-2$

(3) If s satisfies

i) $b = 0,\ q-t \le a \le q^2-(t+1)$, or

ii) $1 \le b \le q-2$,

$\max\{b, q-n\} \le a \le \min\{b+q^2-(q+1), q^2-(t+2)\}$, or

iii) $b = q-1$, $q-(t+1) \le a \le q^2-(t+2)$

then $d(C(s,t)) = q^3-1-(s+t)$

To describe the minimum distance of other s values, let $s = (q^2-\rho)q+b$.

Lemma 7: Fix an integer t, $1 \le t \le q-1$. Let $s = (q^2-\rho)q+b$ be an integer, where $0 \le b < q$.

(4) If $1 \le b, t+1 \le \rho, \rho+b \le q$, then $d(C(s,t)) = \rho q-(t+1)$.

(5) If $\rho \le t+1, q < \rho+b$, then $d(C(s,t)) = \rho(q-1)-(b-1)$.

(6) Assume $2 \le \rho \le t, \rho+b \le q$

i) If $t \le q-2$ or $t = q-1, \rho+b < q$, then $d(C(s,t)) = \rho(q-1)$;

ii) If $t = q-1, \rho+b = q$, then $d(C(s,t)) = (\rho-1)q$.

Next, we consider code $C(s,q)$.

Lemma 8: Let $s = aq+b \in A(\mathbb{Z},q)$ be the integer in set $\{s \in \mathbb{Z} | \dim C(s,t) = \dim C(s-1,t)+1\}$, $0 \le b < q$.

(1) If s satisfies

i) $0 \le b \le q-2, b \le a \le b+q^2-q-1$, or

ii) $b = q-1, -1 \le a \le q^2-3$,

then $d(C(s,q)) = q^3-q-s-1$

(2) If s satisfies $b+q^2-q \le a \le q^2-2$, then $d(C(s,q)) = (q^2-a-1)q$

(3) If s satisfies $0 \le b \le q-2, q^2-1 \le a \le b+q^2-1$, then $d(C(s,q)) = q^2+q-a-2$

The relevant parameters of the second type of Hermitian two-point code are given in [27].

Lemma 9: Assume that the divisor G is satisfied

(a) $\deg G > \deg K+q$, or

(b) $\deg K \le \deg G \le \deg K+q$, and s, t are not 0.

Let $G = K+s'P_\infty+t'P_0$, where K is the canonical divisor, $s'+t' = s+t-\deg K$

$$s' = s_0(q+1)-s_1, 0 \le s_1 \le q$$

$$t' = t_0(q+1)-t_1, 0 \le t_1 \le q$$

Let $d' = \deg G - \deg K = s'+t'$.

(1) If $0 \le s_1, t_1 \le s_0+t_0$, then $d(C_\Omega(D,G)) = d'$.

(2) If $0 \le t_1 \le s_0+t_0 < s_1$, then $d(C_\Omega(D,G)) = d'+s_1-(s_0+t_0)$

(2') If $0 \le s_1 \le s_0+t_0 < t_1$, then $d(C_\Omega(D,G)) = d'+t_1-(s_0+t_0)$

(3) If $s_0+t_0 < s_1 \le t_1 < q$, then $d(C_\Omega(D,G)) = d'+s_1+t_1-2(s_0+t_0)$

(3') If $s_0+t_0 < t_1 \le s_1 < q$, then $d(C_\Omega(D,G)) = d'+s_1+t_1-2(s_0+t_0)$

(4) If $s_0+t_0 < s_1, t_1$, and $s_1 = q,\ t_1 = q$, then $d(C_\Omega(D,G)) = d'+q-(s_0+t_0)$

3.3 Comparison between two-point code and one-point code

Example1: Let X be the Hermitian curve defined on $\mathbb{F}_{16}$. The curve equation is $y^4+y=x^5$, the genus of the curve is $g=6$, and the number of rational points is 65. We will record these rational points as $P_0,P_1,...P_{63},P_\infty$. Let $P_0=(0,0,1)$ is the origin and $P_\infty=(0,1,0)$ is the infinity point. Let $C_1=C_L(D,G_1)$, $C_2=C_L(D,G_2)$, where $G_1=60P_\infty$, $G_2=56P_\infty+4P_0$, $D=P_1+\cdots+P_{63}$. According to the above lemma, the parameter of C_1 is $[63,55,3]_{16}$, and the parameter of C_2 is $[63,55,4]_{16}$. It can be seen that in the case of equal code length and dimension, the two-point code has a larger minimum distance than the one-point code.

4. Literature References

4.1 Construction method

Recall that the one-point Hermitian code has the form $C_L(D,sP)$, where P is the $\mathbb{F}_{q^2}$-rational point on the Hermitian curve, and the dimension and minimum distance of the one-point Hermitian code are given in [22]. Klappenecker and Sarvepalli studied the specific parameters of quantum Hermitian one-point codes in [16]. In this section we use the classical Hermitian two-point code to construct the quantum code.

We construct quantum code according to Lemma 1.

Theorem 1: Let $C_1=C_L(D,G_1)$, $C_2=C_L(D,G_2)$, where $G_1=s_1P_\infty+t_1P_0$, $G_2=s_2P_\infty+t_2P_0$, $s_1\le s_2,t_1\le t_2$. $D=P_1+\cdots+P_n$, where $n=q^3-1$. Assume $G_1\le G_2$, $(\mathrm{supp}G_1\cup\mathrm{supp}G_2)\cap D=\varnothing$, and $\deg G_2\le n$, there is a quantum code $[[n,k,d]]_{q^2}$, where

$$k=k_2-k_1=\dim(C_L(D,G_2))-\dim(C_L(D,G_1)) \tag{8}$$

$$\begin{aligned} d&=\min\{\mathrm{wt}(C_2\setminus C_1),\mathrm{wt}(C_1^\perp\setminus C_2^\perp)\}\\ &=\min\{d(C_L(D,G_2)\setminus C_L(D,G_1)),d(C_\Omega(D,G_1)\setminus C_\Omega(D,G_2))\}\\ &\ge\min\{d(C_L(D,G_2)),d(C_\Omega(D,G_1))\}\end{aligned} \tag{9}$$

$d(C_L(D,G_2))$ and $d(C_\Omega(D,G_1))$ are identified in Chapter II.

Prove of Theorem 1: According to the Hermitian code construction method, we know when $s_1\le s_2,t_1\le t_2$, $C_L(D,G_1)\subseteq C_L(D,G_2)$, from which we can see $d(C_L(D,G_2)\setminus C_L(D,G_1))\ge d(C_L(D,G_2))$, $d(C_\Omega(D,G_1)\setminus C_\Omega(D,G_2))\ge d(C_\Omega(D,G_2))$, using Lemma 1 we can get the parameters of the quantum code.

We use the following example to illustrate how to construct a quantum code using this theorem.

Example 2: Suppose C_1 and C_2 are both Hermitian two-point codes on $\mathbb{F}_{16}$, ie $q=4$. Let $s_1=18,s_2=44$, and $t_1=t_2=4$, that is $G_1=18P_\infty+4P_0$, $G_2=44P_\infty+4P_0$. $D=P_1+\cdots+P_{63}$ and $(\mathrm{supp}G_1\cup\mathrm{supp}G_2)\cap D=\varnothing$. According to the calculation in Chapter II, we get the parameter of C_1 is $[63,17,41]_{16}$ and the parameter of C_2 is $[63,43,15]_{16}$. The minimum distance of the dual code $C_1^\perp$ of C_1 is 12, so we can get the quantum code with the parameter $[[63,26,\ge12]]_{16}$.

4.2 Code comparison

This section compares the quantum Hermitian two-point code with the shortened quantum Hermitian one-point code.

In order to make the code lengths of the one-point code and the two-point code coincide, let $G=mP_\infty$ in the one-point codes $C_L(D,G)$ and $C_\Omega(D,G)$ and $D=P_1+\cdots+P_n$, where $n=q^3-1$. We use the parameters of the classical Hermitian one-point code shown in the shortened [22] to calculate the parameters of the quantum Hermitian one-point code and compare it with the quantum Hermitian two-point code constructed in this paper.

Example 3: In Example 2, a quantum Hermitian two-point code with the parameter $[[63,26,\ge12]]_{16}$ is obtained. The parameters of the quantum Hermitian one-point code of the same dimension are calculated below. Suppose C_3 and C_4 are both Hermitian one-point codes on $\mathbb{F}_{16}$, ie $q=4$. Let $s_1=22,s_2=48$, that is $G_3=22P_\infty$, $G_4=48P_\infty$. Let $D=P_1+\cdots+P_{63}$, and $(\mathrm{supp}G_3\cup\mathrm{supp}G_4)\cap D=\varnothing$. By calculation, the

parameter of C_3 is $[63,17,41]_{16}$, and the parameter of C_4 is $[63,43,15]_{16}$. The minimum distance of dual code $C_3^{\perp}$ of C_3 is 11, so we can get the quantum code with the parameter $[[63,26,\geq 11]]_{16}$.

Example 4: Suppose C_1 and C_2 are both Hermitian two-point codes on $\mathbb{F}_{16}$, ie $q=4$. Let $s_1=10, s_2=36,\ t_1=t_2=11$, that is $G_1=10P_\infty+11P_0$, $G_2=36P_\infty+11P_0$. $D=P_1+\cdots+P_{63}$ and $(\mathrm{supp}G_1\cup\mathrm{supp}G_2)\cap D=\varnothing$. According to the calculation in Chapter II, we get the parameter of C_1 is $[63,16,42]_{16}$ and the parameter of C_2 is $[63,42,16]_{16}$. The minimum distance of the dual code $C_1^{\perp}$ of C_1 is 12, so we can get the quantum code with the parameter $[[63,26,\geq 12]]_{16}$.The parameters of the quantum Hermitian one-point code of the same dimension are calculated below. Suppose C_3 and C_4 are both Hermitian one-point codes on $\mathbb{F}_{16}$, ie $q=4$. Let $s_3=21, s_4=47$, that is $G_3=21P_\infty, G_4=47P_\infty$. Let $D=P_1+\cdots+P_{63}$, and $(\mathrm{supp}G_3\cup\mathrm{supp}G_4)\cap D=\varnothing$. By calculation, the parameter of C_3 is $[63,16,42]_{16}$, and the parameter of C_4 is $[63,42,16]_{16}$. The minimum distance of dual code $C_3^{\perp}$ of C_3 is 11, so we can get the quantum code with the parameter $[[63,26,\geq 11]]_{16}$.

Example 5: Suppose C_1 and C_2 are both Hermitian two-point codes on $\mathbb{F}_{64}$, ie $q=8$. Let $s_1=82, s_2=442,\ t_1=t_2=7$, that is $G_1=82P_\infty+7P_0$, $G_2=442P_\infty+7P_0$. $D=P_1+\cdots+P_{511}$ and $(\mathrm{supp}G_1\cup\mathrm{supp}G_2)\cap D=\varnothing$. According to the calculation in Chapter II, we get the parameter of C_1 is $[511,62,422]_{64}$ and the parameter of C_2 is $[511,422,62]_{64}$. The minimum distance of the dual code $C_1^{\perp}$ of C_1 is 38, so we can get the quantum code with the parameter $[[511,360,\geq 38]]_{64}$.The parameters of the quantum Hermitian one-point code of the same dimension are calculated below. Suppose C_3 and C_4 are both Hermitian one-point codes on $\mathbb{F}_{64}$, ie $q=8$. Let $s_3=89, s_4=449$, that is $G_3=89P_\infty, G_4=449P_\infty$. Let $D=P_1+\cdots+P_{511}$, and $(\mathrm{supp}G_3\cup\mathrm{supp}G_4)\cap D=\varnothing$. By calculation, the parameter of C_3 is $[511,62,422]_{64}$, and the parameter of C_4 is $[511,422,62]_{64}$. The minimum distance of dual code $C_3^{\perp}$ of C_3 is 34, so we can get the quantum code with the parameter $[[511,360,\geq 34]]_{64}$.

It can be seen from the above example that the quantum Hermitian two-point code has a larger minimum distance and a stronger error correction capability than the quantum Hermitian one-point code when the code length and the dimension are equal.

5. Conclusion

In this paper, the two-point code on the Hermitian curve is quantized using the CSS construction method. Due to the better performance of the classical Hermitian two-point code relative to the one-point code, the quantum code constructed by it has better performance than the quantum Hermitian one-point code. At the end of the paper, the two-point code and the one-point code are compared, and the two-point code can be proved to be superior to the one-point code.

References

[1] Y. C. Han, C. F. Li, G. C. Guo: The Principle and Research Progress of Quantum Computing, Science & Technology Review, vol 35(2017), no. 23, pp. 70-75. (In Chinese)

[2] C. H. Bennett: Quantum Cryptography Using Any Two Nonorthogonal States, Physical Review Letters, vol 68(1992), no. 21, pp. 3121.

[3] B. Schumacher, M.A.Nielsen: Quantum Data Processing and Error Correction, Physical Review A, vol 54(1996), no. 4, pp. 2629.

[4] P. W. Shor: Scheme for Reducing Decoherence in Quantum Computer Memory, Physical review A, vol 52(1995), no. 4, pp. 2493.

[5] P. W. Shor: Scheme for Reducing Decoherence in Quantum Memory, Physical review A, vol 52(1995), no. 4, pp. 2493.

[6] A. R. Calderbank, P. W. Shor: Good Quatum Errorcorrecting Codes Exist, Physical review A, vol 54(1996), pp. 1098-1105.

[7] P. P. Shao, X. L. Tang, W. Zhao: Construction of Quantum Code Based on Polynomial Codes," Journal of Guangzhou University, vol 16, no. 6, pp. 1671- 4229, 2017. (In Chinese)

[8] J. H. Fan, H. W. Chen, R. G. Li: Asymmetric Quantum Product-tensor Product Code, Journal of Southeast University, vol 47(2017), no. 1, pp. 18-22. (In Chinese)
[9] Q. Cheng, H. Yu: Construction of Two Asymmetric Graph Quantum MDS Codes, Computer Engineering and Applications, vol 53(2017), no. 19, pp. 61-64. (In Chinese)
[10] H. J. Tiersma: Remarks on Codes From Hermitian Curves, IEEE Transactions of Information Theory, vol 33(1987), pp. 605-609.
[11] H. Stichtenoth: A Note on Hermitian Codes, IEEE Transactions of Information Theory, vol 34(1988), pp. 1345- 1348.
[12] G. L. Matthews: Weierstrass Pairs and Minimum Distance of Goppa Codes, Designs, Codes and Cryptography, vol 22(2001), pp.107-121.
[13] Masaaki Homma, Seon Jeong Kim: Toward the Determination of the Minimum Distance of Two-point Codes on a Hermitian Curve, Des. Codes Cryptogr, vol 37(2005), no. 1, pp. 111-132.
[14] Masaaki Homma, Seon Jeong Kim: The Two-point Codes on a Hermitian Curve with the Designed Minimum Distance, Des. Codes Cryptogr, vol 38(2006), no. 1, pp. 55-81.
[15] Masaaki Homma, Seon Jeong Kim: The two-point Codes with the Designed Distance on a Hermitian Curve in even Characteristic, Des. Codes Cryptogr, vol 39(2006), no. 3, pp. 375-386.
[16] Masaaki Homma, Seon Jeong Kim: The Complete Determination of the Minimum Distance of Two-point Codes on a Hermitian Curve, Des. Codes Cryptogr, vol. 40(2006), no. 1, pp. 5-24.
[17] P. Beelen: The Order Bound for General Algebraic Geometric Codes, Finite Fields Appl, vol 13(2007), no. 3, pp. 665-680.
[18] S. Park: Minimum Distance of Hermitian Two-point Codes, Designs, Codes and Cryptography, vol 57(2010), no. 2, pp. 195-213.
[19] I. Duursma, R. Kirov: Improved Two-Point Codes on Hermitian Curves, IEEE Transactions on Information Theory, vol 57(2011), no. 7, pp. 4469-4476.
[20] A. Klappenecker, P.K: Sarvepalli. Nonbinary quantum codes from Hermitian curves, International Conference on Applied Algebra, vol 38(2006), no. 57, pp. 136-143.
[21] K. Q. Feng, H. Chen: *Quantum Error Correcting Code*(Beijing: Science Press, 2010) pp. 39-48. (In Chinese)
[22] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane: Quantum Error Correction Via Codes Over GF(4), IEEE International Symposium on Information Theory, vol 44(2002), no. 4, pp. 292.
[23] Markus Grassl, Thomas Beth: On Optimal Quantum Codes, International Journal of Quantum Information, vol 2(2008), no. 1, pp. 55-64.
[24] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli: Nonbinary Stabilizer Codes over Finite Fields, IEEE Transactions on Information Theory, vol 52(2006), no. 11, pp. 4892-4914.
[25] T. Høholdt, J. H. Van Lint, R. Pellikaan: Algebraic Geometry of Codes, Handbook of coding theory, vol. I, II(2011), pp. 871-961.
[26] K. Yang, P. V. Kumar: On the True Minimum Distance of Hermitian Codes, Coding Theory & Algebraic Geometry, vol 15(1992), no. 18, pp. 99-107.
[27] S. Park: Minimum Distance of Hermitian Two-point Codes, Designs Codes & Cryptography, vol 57(2010), no. 2, pp. 195-213.