第45卷第3期 中国科学技术大学学报 Vol. 45, No. 3
2015年3月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Mar. 2015

Article ID:0253-2778(2015)03-0199-06

Quantum codes from cyclic codes over ring $F_q + uF_q$

LI Jin

(*School of Mathematics, Hefei University of Technology, Hefei* 230009, *China*)

Abstract: A method for constructing quantum codes from cyclic codes over the ring F_q+uF_q was given, where q is a prime power and $u^2=0$. First, symplectic self-orthogonal codes over F_q were obtained as images of cyclic codes over F_q+uF_q. Then, these codes were used to construct quantum codes. Examples including quantum MDS codes were given.

Key words: quantum codes; cyclic codes; self-orthogonal codes

CLC number: TN911 **Document code**: A doi:10.3969/j.issn.0253-2778.2015.03.004

2010 Mathematics Subject Classification: 94A55

Citation: Li Jin. Quantum codes from cyclic codes over ring F_q+uF_q[J]. Journal of University of Science and Technology of China, 2015,45(3):199-204.

环 F_q+uF_q 上循环码构造的量子码

李 锦

(合肥工业大学数学学院,安徽合肥 230009)

摘要:给出了利用环 F_q+uF_q 上循环码构造的量子码的一种方法,其中 q 是素数幂次方,$u^2=0$.先由环 F_q+uF_q 上循环码的像得到了 F_q 辛自正交的码,再用这些自正交码构造量子码,并给出了一些包括量子MDS码的例子.

关键词:量子码;循环码;自正交码

0 Introduction

Since the discovery that quantum error correcting codes protect quantum information as classical error correcting codes protect classical information[1], quantum error correcting codes have made great progress. In Ref. [2], the construction of binary quantum error correcting codes was taken from a classical binary self-orthogonal code with respect to a certain inner product. Since then, many good binary quantum error correcting codes have been constructed by using various techniques in Refs. [3-6]. With the development of the theory of binary quantum error correcting codes, nonbinary quantum error correcting codes have received much attention. Works on nonbinary quantum error correcting codes are likely to become extremely useful, shown, for example, by the proof of concept implementation in certain ion trap models. Many

Received: 2013-09-27; **Revised**: 2014-01-05

Foundation item: Supported by the National Natural Science Foundation of China (61370089), the Fundamental Research Funds for the Central Universities (JZ2014HGBZ0349).

Biography: LI Jin, female, born in 1987, PhD. Research field: algebraic coding theory. E-mail: lijin_0102@126.com

nonbinary quantum error-correcting codes have been constructed by using classical linear codes over finite field F_q[7-8]. Recently, in Refs. [9-10], nonbinary quantum codes were constructed from cyclic codes over finite ring F_2+uF_2 and F_4+uF_4. This motivates us to consider linear codes over F_q+uF_q to obtain good nonbinary quantum codes.

In this paper, we find self-orthogonal codes with respect to symplectic inner product over F_q as images of cyclic codes over F_q+uF_q. These codes are used to construct quantum codes. This paper is organized as follows. In Section 1, we give a construct for quantum codes from linear codes over F_q+uF_q. We introduce a map from F_q+uF_q to F_q^2. Using this map, we derive symplectic self-orthogonal codes over F_q. In Section 2, we study cyclic codes over F_q+uF_q, and give a sufficient and necessary condition for the existence of Hermitian self-orthogonal cyclic codes over F_q+uF_q. Then we construct quantum codes from the symplectic self-orthogonal codes. Finally, a summary of this result is given in Section 3.

1 A construction of quantum codes

Let q be a prime power and F_q the finite field with q elements. Consider the polynomial residue ring $R=F_q[u]/\langle u^2\rangle$, where u denotes an indeterminate. The ring R is a finite chain ring with maximal ideal $\langle u\rangle$. Structurally, R can be expressed as F_q+uF_q, where $u^2=0$. Given n-tuples

$\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})$, $\boldsymbol{b}=(b_0,b_1,\cdots,b_{n-1})\in R^n$,

their Euclidean inner product is defined as

$$\boldsymbol{a}\cdot\boldsymbol{b}=a_0b_0+a_1b_1+\cdots+a_{n-1}b_{n-1}\in R.$$

Two n-tuples $\boldsymbol{a}$, $\boldsymbol{b}$ are called orthogonal with respect to the Euclidean inner product if $\boldsymbol{a}\cdot\boldsymbol{b}=0$. A code over R of length n is a nonempty subset of R^n, and a code is linear over R of length n if it is an R-submodule of R^n. For a linear code C of length n over R, the Euclidean dual code $C^\perp$ is defined as

$$C^\perp=\{\boldsymbol{a}\in F_q^n\mid \boldsymbol{a}\cdot\boldsymbol{b}=0 \text{ for all } \boldsymbol{b}\in C\}.$$

A linear code C of length n over R is called self-orthogonal with respect to the Euclidean inner product if $C\subseteq C^\perp$. For $\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})\in R^n$, the Hamming weight of $\boldsymbol{a}$ is the number of nonzero components of $\boldsymbol{a}$, we denote the Hamming weight of $\boldsymbol{a}$ by $\mathrm{wt}_H(\boldsymbol{a})$. The minimum Hamming weight of a linear code is the smallest nonzero Hamming weight among all its codewords. Let $\mathscr{A}=(\boldsymbol{a}\mid\boldsymbol{b})$ be any element in F_q^{2n}, where $\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})$, $\boldsymbol{b}=(b_0,b_1,\cdots,b_{n-1})\in F_q^n$. Then we define the symplectic weight of $\mathscr{A}$ as

$$\mathrm{wt}_S(\mathscr{A})=\#\{i\mid a_i\neq 0 \text{ or } b_i\neq 0,\ 0\leqslant i\leqslant n-1\}.$$

For $\mathscr{A}=(\boldsymbol{a}\mid\boldsymbol{b})$, $\mathscr{B}=(\boldsymbol{a}'\mid\boldsymbol{b}')\in F_q^{2n}$, define the symplectic inner product as

$$(\mathscr{A},\mathscr{B})_S=\boldsymbol{a}\cdot\boldsymbol{b}'-\boldsymbol{a}'\cdot\boldsymbol{b}\in F_q.$$

For a q-ary linear code $\mathscr{C}$ of length $2n$, the symplectic dual code $\mathscr{C}^{\perp_S}$ is defined as

$$\mathscr{C}^{\perp_S}=\{\mathscr{A}\in F_q^{2n}\mid(\mathscr{A},\mathscr{B})_S=0 \text{ for all } \mathscr{B}\in\mathscr{C}\}.$$

A q-ary linear code $\mathscr{C}$ of length $2n$ is said to be self-orthogonal with respect to the symplectic inner product if $\mathscr{C}\subseteq\mathscr{C}^{\perp_S}$. We use the notation $[[n,k,d]]$ to denote a quantum error-correcting code for n qubits having q^k codewords and minimum distance d. Any $[[n,k,d]]$ quantum code must meet the quantum singleton bound, i.e., $k\leqslant n-2d+2$. If a quantum code attains this bound, i.e., $k=n-2d+2$, it is called a quantum maximum-distance-separable (MDS) code. The following important construction of quantum codes was proposed in Ref. [11].

Theorem 1 Let $\mathscr{C}$ be a q-ary self-orthogonal $[2n,k]$ code with respect to the symplectic inner product. Then there exists a q-ary $[[n,n-k,d]]$ quantum code with

$$d=\mathrm{wt}_S(\mathscr{C}^{\perp_S}\backslash\mathscr{C})=\min\{\mathrm{wt}_S(\boldsymbol{a})\in\mathscr{C}^{\perp_S}\backslash\mathscr{C}\}.$$

Our goal is to construct q-ary self-orthogonal codes with respect to the symplectic inner product by employing linear codes over R. Observe that each element $c\in R$ can be written in the form $c=a+ub$, where $a,b\in F_q$. We first introduce a map from R to F_q^2 given by $\phi(c)=(a\mid b)$. This map can be naturally extended to R^n as follows:

$$\phi:\ R^n\to F_q^{2n}$$
$$\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})\to$$
$$(a_0,a_1,\cdots,a_{n-1}\mid b_0,b_1,\cdots,b_{n-1}),$$

where $c_i=a_i+ub_i$ with $a_i,b_i\in F_q$ for $0\leqslant i\leqslant n-1$.

For a linear code C over R of length n, it is easy to verify that $\phi(C)$ is a q-ary linear code of length $2n$. Note that $a+ub=0$ if and only if $a=b=0$, so the map ϕ is a weight-preserving map from R^n (Hamming weight) to F_q^{2n} (symplectic weight). For $c=a+ub$ with $a,b\in F_q$, define the conjugation of c to be $\bar{c}=a-ub$. Given n-tuples $\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})$, $\boldsymbol{b}=(b_0,b_1,\cdots,b_{n-1})\in R^n$, their Hermitian inner product is defined as

$$(\boldsymbol{a},\boldsymbol{b})_H=a_0\bar{b}_0+a_1\bar{b}_1+\cdots+a_{n-1}\bar{b}_{n-1}.$$

Two n-tuples $\boldsymbol{a}$, $\boldsymbol{b}$ are called orthogonal with respect to the Hermitian inner product if $(\boldsymbol{a},\boldsymbol{b})_H=0$. For a linear code C of length n over R, its Hermitian dual code $C^{\perp_H}$ is defined as

$$C^{\perp_H}=\{\boldsymbol{a}\in R^n\mid(\boldsymbol{a},\boldsymbol{b})_H=0\text{ for all }\boldsymbol{b}\in C\}.$$

The Hermitian dual of a code over R was introduced in Ref. [12] to build unimodular lattices, and a mass formula for self-dual codes over R with respect to the Hermitian inner product was given in Ref. [13].

Lemma 1　If C is a self-orthogonal code of length n over R with respect to the Hermitian inner product, then $\phi(C)$ is a q-ary self-orthogonal code of length $2n$ with respect to the symplectic inner product.

Proof　Let $\mathscr{A}=(\boldsymbol{a}\mid\boldsymbol{b})$ and $\mathscr{B}=(\boldsymbol{a}'\mid\boldsymbol{b}')$ be two codewords in $\phi(C)$. Then $\boldsymbol{c}=\boldsymbol{a}+u\boldsymbol{b}$, $\boldsymbol{c}'=\boldsymbol{a}'+u\boldsymbol{b}'\in R^n$. Since C is self-orthogonal with respect to the Hermitian inner product, it follows that

$$(\boldsymbol{c},\boldsymbol{c}')_H=(\boldsymbol{a}+u\boldsymbol{b})\cdot(\boldsymbol{a}'-u\boldsymbol{b}')=\boldsymbol{a}\cdot\boldsymbol{a}'-u(\boldsymbol{a}\cdot\boldsymbol{b}'-\boldsymbol{a}'\cdot\boldsymbol{b})=0.$$

This gives that $\boldsymbol{a}\cdot\boldsymbol{b}'-\boldsymbol{a}'\cdot\boldsymbol{b}=0$. So we have $(\mathscr{A},\mathscr{B})_S=0$, and $\mathscr{A}\in\phi(C)^{\perp_S}$. Therefore,

$$\phi(C)\subseteq\phi(C)^{\perp_S}.\qquad\square$$

Observe that the map ϕ is a bijection. Combining the above lemma with Theorem 1 we get the following construction of quantum codes.

Theorem 2　If C is a self-orthogonal code over R of length n with respect to the Hermitian inner product and contains q^k codewords, then there exists a q-ary $[[n,n-k,d]]$ quantum code with

$$d=\mathrm{wt}_H(C^{\perp_H}\backslash C)=\min\{\mathrm{wt}_H(\boldsymbol{a})\in C^{\perp_H}\backslash C\}.$$

From the above theorem we see that quantum codes can be directly constructed by using Hermitian self-orthogonal codes over R. In the following, we will obtain Hermitian self-orthogonal codes over R by employing cyclic codes over R.

2　Cyclic codes over F_q+uF_q

Cyclic shift on R^n is defined as

$$\tau(c_0,c_1,\cdots,c_{n-1})=(c_{n-1},c_0,\cdots,c_{n-2}),$$

and a linear code C of length n over R is cyclic if the code is invariant under the cyclic shift τ. We identify a codeword $c=(c_0,c_1,\cdots,c_{n-1})$ and its polynomial representation

$$c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}.$$

Then $xc(x)$ corresponds to a cyclic shift of $c(x)$ in the ring $R[x]/\langle x^n-1\rangle$. As usual, a cyclic code of length n over R is precisely an ideal of $R[x]/\langle x^n-1\rangle$. Throughout this paper n is coprime to p. The following lemma gives the structure of cyclic codes.

Lemma 2[12]　Suppose C is a cyclic code of length n over R, then there are unique and monic polynomials $G_0(x)$, $G_1(x)$, $G_2(x)\in F_q[x]$ such that

$$C=\langle G_1(x)G_2(x),uG_0(x)G_2(x)\rangle,$$

where $G_0(x)G_1(x)G_2(x)=x^n-1$, and $|C|=q^{2\deg(G_0)+\deg(G_1)}$.

It was shown that $R[x]/\langle x^n-1\rangle$ is a principal ideal ring in Refs. [12-13]. We will give an alternative generator for a cyclic code of length n over R as follows.

Theorem 3　Let $G_0(x)$, $G_1(x)$ and $G_2(x)$ be defined as in Lemma 1. If C is a cyclic code of length n over R, then

$$C=\langle F_1(x)F_2^2(x)\rangle=\langle G_1(x)G_2(x),uG_0(x)G_2(x)\rangle,$$

where $F_i(x)\in R[x]$ such that

$$F_0(x)F_1(x)F_2(x)=x^n-(1+u),$$
$$F_i(x)\equiv G_i(x)(\mathrm{mod}\ u)$$

for $i=0,1,2$. Moreover, $|C|=q^t$, where

$$t=2n-(\deg(F_1(x))+\deg(F_2(x))).$$

Proof　Let $F_i(x)=G_i(x)+uH_i(x)$ for some

$H_i(x)\in F_q[x]$, $i=0,1,2$. Since $G_0(x)$ and $G_1(x)$ are coprime in $R[x]$, there exist $a(x), b(x)\in R[x]$ such that $a(x)G_0(x)+b(x)G_1(x)=1$. Then

$$F_1(x)F_2^2(x)=[G_1(x)+uH_1(x)][G_2(x)+uH_2(x)]^2=[G_2(x)+2uH_2(x)+ub(x)G_2(x)H_1(x)]\cdot G_1(x)G_2(x)+ua(x)H_1(x)G_0(x)G_2^2(x).$$

It follows that

$$\langle F_1(x)F_2^2(x)\rangle\subseteq\langle G_1(x)G_2(x), uG_0(x)G_2(x)\rangle.$$

On the other hand,

$$uG_0(x)G_2(x)=[F_0(x)-uH_0(x)]^2[F_2(x)-uH_2(x)]=uF_0(x)F_2(x)=-F_0^2(x)F_1(x)F_2^2(x).$$

This shows $uG_0(x)G_2(x)\in\langle F_1(x)F_2^2(x)\rangle$. Since $G_0(x)G_2(x)$ and $G_1(x)$ are coprime in $R[x]$, there exist $s(x), t(x)\in R[x]$ such that

$$s(x)G_0(x)G_2(x)+t(x)G_1(x)=1.$$

Multiplying both sides by $G_1(x)$, we get $G_1(x)=t(x)G_1^2(x)$ in $R[x]/\langle x^n-1\rangle$. Similarly, $G_2(x)=t(x)G_2^2(x)$ in $R[x]/\langle x^n-1\rangle$, for some $v(x)\in R[x]$. Computing in $R[x]/\langle x^n-1\rangle$, we have

$$G_1(x)G_2(x)=t(x)G_1^2(x)v(x)G_2^2(x)=[F_1(x)-uH_1(x)]^2[F_2(x)-uH_2(x)]^2=t(x)v(x)[F_1(x)-2uH_1(x)+2F_0(x)F_1^2(x)H_2(x)]F_1(x)F_2^2(x).$$

This gives $G_1(x)G_2(x)\in\langle F_1(x)F_2^2(x)\rangle$.

Hence,

$$\langle F_1(x)F_2^2(x)\rangle\supseteq\langle G_1(x)G_2(x), uG_0(x)G_2(x)\rangle.$$

The desired result follows. □

By Hensel's lemma[14], each monic polynomial $F_i(x)$ has a unique decomposition as product of monic basic irreducible pairwise coprime polynomials. Thus, a cyclic code of length n over R can be written in the form $C=\langle\prod_{i=1}^{r}f_i(x)^{k_i}\rangle$, where $f_i(x)$ $(1\leqslant i\leqslant r)$ are monic basic irreducible divisors of $x^n-(1+u)$ in $R[x]$ and $0\leqslant k_i\leqslant 2$. To study the dual of a cyclic code, we need the following result. Its proof is similar to that of Proposition 2.12 in Ref. [15] and is thus omitted.

Lemma 3 Let

$$a(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1},$$

$$b(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}\in R[x].$$

Then $a(x)b(x)=0$ in $R[x]/\langle x^n-1\rangle$ if and only if $(a_0, a_1, \cdots, a_{n-1})$ is Hermitian orthogonal to $(\bar{b}_{n-1}, \bar{b}_{n-2}, \cdots, \bar{b}_0)$ and all its cyclic shifts.

For a polynomial $f(x)$ whose degree is t, the reciprocal polynomial of $f(x)$ is

$$f^*(x)=x^tf(x^{-1}).$$

So that the roots of $f^*(x)$ are the reciprocals of the corresponding root of $f(x)$. We denote by $f^\dagger(x)$ the conjugation of the reciprocal polynomial of $f(x)$, i.e. $f^\dagger(x)=\overline{f^*(x)}$. Let ζ be a primitive nth root of unity. Then it is easy to check that if ζ^z is a root of $f(x)$ for some integer z, then $f^\dagger(x)$ has ζ^{-z} as a root.

Theorem 4 Let $C=\langle\prod_{i=1}^{r}f_i^{k_i}(x)\rangle$ be a cyclic code of length n over R, where $f_i(x)$ are monic basic irreducible divisors of $x^n-(1+u)$ in $R[x]$, and $0\leqslant k_i\leqslant 2$, $1\leqslant i\leqslant r$. Then

$$C^{\perp_H}=\langle\prod_{i=1}^{r}(f_i^\dagger(x))^{2-k_i}\rangle,$$

and $|C^{\perp_H}|=q^t$, where $t=\sum_{i=1}^{r}k_i\deg f_i(x)$.

Proof Let

$$D=\langle\prod_{i=1}^{r}(f_i^\dagger(x))^{2-k_i}\rangle\subseteq R[x]/\langle x^n-1\rangle,$$

a direct computation shows that

$$\prod_{i=1}^{r}f_i^{k_i}(x)(\prod_{i=1}^{r}(f_i^\dagger(x))^{2-k_i})^\dagger=\prod_{i=1}^{r}f_i^{k_i}(x)f_i^{2-k_i}(x)=\prod_{i=1}^{r}f_i^2(x)=(x^n-(1+u))^2=0.$$

Hence, $D\subseteq C^{\perp_H}$. For each i, let a_i denote the constant of $f_i(x)$. Since $x^n-(1+u)=\prod_{i=1}^{r}f_i(x)$, we have $\prod_{i=1}^{r}a_i=-(1+u)$. It follows that each a_i is an invertible element of R and $\bar{a}_i$ is a leading coefficient of $f_i^\dagger(x)$. For each i, let $b_i=\bar{a}_i^{-1}$, then $\prod_{i=1}^{r}b_i=\prod_{i=1}^{r}\bar{a}_i^{-1}=-(1+u)$, and $b_if_i^\dagger(x)$ is a monic polynomial. Thus,

$$\prod_{i=1}^{r}b_if_i^\dagger(x)=\prod_{i=1}^{r}b_i\prod_{i=1}^{r}f_i^\dagger(x)=x^n-(1+u).$$

We know $b_i f_i^{\dagger}(x)$ also are monic basic irreducible divisors of $x^n-(1+u)$ in $R[x]$, so $|D|=q^{\sum_{i=1}^{r}k_i\deg f_i(x)}$. On the other hand, from $|C||C^{\perp_H}|=q^{2n}$, we find that $|D|=|C^{\perp_H}|$. Therefore, $C^{\perp_H}=\langle\prod_{i=1}^{r}(f_i^{\dagger}(x))^{2-k_i}\rangle$. □

Let i be an integer such that $0\leqslant i\leqslant n-1$, and let m_i be the smallest positive integer such that $iq^{m_i}\equiv i(\mathrm{mod}\ n)$. Then $C_i=\{i, iq, \cdots, iq^{m_i-1}\}$ is the q-cyclotomic coset modulo n containing i. Let ζ be a primitive nth root of unity in F_{q^m}, where $m=m_1$. The minimal polynomial of ζ^i over F_q is $m_i(x)=\Pi_{j\in C_i}(x-\zeta^j)$. Let I be a complete set of q-cyclotomic coset representatives modulo n. For each $i\in I$, let $M_i(x)$ be a basic irreducible divisor of $x^n-(1+u)$ in $R[x]$ such that $M_i(x)\equiv m_i(x)(\mathrm{mod}\ u)$. We note that if $M_i(x)$ is a basic irreducible polynomial over R, then $M_i^{\dagger}(x)$ is also a basic irreducible polynomial over R, and if C_i is the set of zeros of $m_i(x)$, then $C_{-i}=C_{n-i}=\{-i \bmod n\mid i\in C_i\}$ is the set of zeros of $m^{\dagger}(x)$. It is easy to verify that $M_i^{\dagger}(x)\equiv m_i^{\dagger}(x)(\mathrm{mod}\ u)$.

Let $I_1=\{i\in I\mid -i\in C_i\}$, $I_2=\{i\in I\mid -i\notin C_i\}$. From Theorem 3, we obtain that the generator polynomial of C has the form

$$\langle\prod_{i\in I_1}M_i^{j_i}(x)\prod_{i\in I_2}M_i^{k_i}(x)M_{-i}^{l_i}(x)\rangle$$

where $0\leqslant j_i, k_i, l_i\leqslant 2$. In the following, we will give a sufficient and necessary condition for the existence of Hermitian self-orthogonal cyclic codes over R.

Theorem 5　Let

$$C=\langle\prod_{i\in I_1}M_i^{j_i}(x)\prod_{i\in I_2}M_i^{k_i}(x)M_{-i}^{l_i}(x)\rangle$$

be a cyclic code over R of length n, where $0\leqslant j_i, k_i, l_i\leqslant 2$. Then $C\subseteq C^{\perp_H}$ if and only if $j_i\geqslant 1$, $k_i+l_i\geqslant 2$.

Proof　Let

$$F(x)=\prod_{i\in I_1}M_i^{j_i}(x)\prod_{i\in I_2}M_i^{k_i}(x)M_{-i}^{l_i}(x),$$

then

$$C^{\perp_H}=\langle G(x)\rangle=\langle\prod_{i\in I_1}M_i^{2-j_i}(x)\prod_{i\in I_2}M_i^{2-l_i}(x)M_{-i}^{2-k_i}(x)\rangle.$$

For the code C, $C\subseteq C^{\perp_H}$ if and only if $G(x)\mid F(x)$, comparing the indexes of $G(x)$ with those $F(x)$, we can get the result. □

To determine the Hamming distance of a cyclic code C of length n over R, we associate the code C with the torsion code of C: $Tor(C)=\{x\in F_q^n\mid ux\in C\}$. The following theorem determines the torsion code of a cyclic code over R, which is a generalization of Theorem 8 in Ref. [9]. Its proof is similar.

Lemma 4　Let $C=\langle\prod_{i=1}^{r}f_i^{k_i}(x)\rangle$ be a cyclic code of length n over R, where $f_i(x)$ $(1\leqslant i\leqslant r)$ are monic baisc irreducible divisors of $x^n-(1+u)$ in $R[x]$ and $0\leqslant k_i\leqslant 2$. Then

① $Tor(C)=\langle\prod_{i=1}^{r}g_i(x)^{\tau_i}\rangle$, where $g_i\equiv f_i(\mathrm{mod}\ u)$, $\tau_i=0$ if $k_i=0$ or 1, and $\tau_i=1$ if $k_i=2$.

② $d_H(C)=d_H(Tor(C))$.

Combining Theorem 5 with Theorem 2, we can produce the following construction of quantum codes.

Theorem 6　Let

$$C=\langle\prod_{i\in I_1}M_i^{j_i}(x)\prod_{i\in I_2}M_i^{k_i}(x)M_{-i}^{l_i}(x)\rangle$$

be a cyclic code over R of length n with size q^k, where $0\leqslant j_i, k_i, l_i\leqslant 2$. If $j_i\geqslant 1, k_i+l_i\geqslant 2$, and the Hamming distance of $C^{\perp_H}$ is d, then a quantum code with parameters $[[n, n-k, d]]$ can be obtained from C.

Example 1　Suppose that q is an odd prime power. Let $m=q-1$ and α be a primitive element of F_q. Then $x^m-1=\prod_{i=0}^{q-2}(x-\alpha^i)$ in $R[x]$. Hence, $x^m-(1+u)=\prod_{i=1}^{q-1}(x-(1-u)\alpha^i)$ in $R[x]$. Let C be a cyclic code over R of length $m=q-1$ with generator polynomial

$$[x-(1-u)]^2[x-(1-u)\alpha^{\frac{q-1}{2}}]^2\cdot\prod_{i=1}^{d-1}[x-(1-u)\alpha^i]^2\cdot\prod_{i=d}^{\frac{q-3}{2}}[x-(1-u)\alpha^i]^2[x-(1-u)\alpha^{q-1-i}]^2,$$

where $1 \leqslant d \leqslant (q+1)/2$.

By Theorem 5, C is a Hermitian self-orthogonal cyclic code over R with size $q^{2(d-1)}$ and

$$C^{\perp_H} = \langle \prod_{i=1}^{d-1} [x-(1-u)\alpha^i]^2 \rangle.$$

By Lemma 4, $Tor(C^{\perp_H})$ is a $[q-1, q-d, d]$ RS code over F_q and $d(C^{\perp_H}) = d$. Applying Theorem 6 yields a $[[q-1, q-2d+1, d]]_q$ quantum MDS code.

Example 2 Consider cyclic codes over $F_3 + uF_3$ of length 13. In $(F_3+uF_3)[x]$,

$$x^{13} - (1+u) = f_0(x) f_1(x) f_2(x) f_3(x) f_4(x),$$

where

$$f_0(x) = (x-(1+u)),$$
$$f_1(x) = x^3 - (1-u)x - 1,$$
$$f_2(x) = x^3 + (1+u)x^2 - 1,$$
$$f_3(x) = x^3 - (1+u)x^2 - (1-u)x - 1,$$
$$f_4(x) = x^3 + (1+u)x^2 + (1-u)x - 1.$$

Let $C = \langle g(x) \rangle = \langle f_0(x)^2 f_1(x)^2 f_2(x)^2 f_3(x)^2 \rangle$. By Theorem 5, $C \subseteq C^{\perp_H}$ and $C^{\perp_H} = \langle f_3(x)^2 \rangle$. We find that the Hamming distance of $C^{\perp_H}$ is equal to 3. From Theorem 6, a $[[13,7,3]]_3$ quantum code can be obtained.

Example 3 Consider cyclic codes over $F_5 + uF_5$ of length 11. In $(F_3+uF_3)[x]$,

$$x^{11} - (1+u) = f_0(x) f_1(x) f_2(x),$$

where

$$f_0(x) = x - (1-u),$$
$$f_1(x) = x^5 - (1+u)x^3 + x^2 - (1-u)x - (1+u),$$
$$f_2(x) = x^5 + (1-u)x^4 + (1+u)x^3 + x^2 - (1+u).$$

Let $C = \langle g(x) \rangle = \langle f_0(x)^2 f_1(x)^2 \rangle$. By Theorem 5, $C \subseteq C^{\perp_H}$ and $C^{\perp_H} = \langle f_1(x)^2 \rangle$. We find that the Hamming distance of $C^{\perp_H}$ is equal to 5. From Theorem 6, a $[[11,1,5]]_5$ quantum code can be obtained.

3 Conclusion

We have obtained symplectic self-orthogonal codes over F_q by virtue of cyclic codes over $F_q + uF_q$. This enabled us to come up with a method for constructing quantum codes. Some good quantum codes have been constructed from cyclic codes over $F_q + uF_q$. In future work, we will use the computer algebra system MAGMA to find more good nonbinary quantum codes.

References

[1] Shor P W. Scheme for reducing decoherence in quantum computer memory[J]. Phys Rev A, 1995, 52: 2 493-2 496.

[2] Calderbank A R, Rains E M, Shor P M, et al. Quantum error correction via codes over $GF(4)$ [J]. IEEE Trans Inform Theory, 1998, 44: 1 369-1 387.

[3] Cohen G, Encheva S, Litsyn S. On binary constructions of quantum codes [J]. IEEE Trans Inform Theory, 1999, 45: 2 495-2 498.

[4] Li R, Li X. Binary construction of quantum codes of minimum distance three and four [J]. IEEE Trans Inform Theory, 2004, 50: 1 331-1 336.

[5] Li R, Li X. Quantum codes constructed from binary cyclic codes [J]. Int J Quant Inform, 2004, 2: 265-272.

[6] Steane A M. Quantum Reed-Muller codes[J]. IEEE Trans Inform Theory, 1999, 45: 1 701-1 703.

[7] Lin X. Quantum cyclic and constacyclic codes [J]. IEEE Trans Inform Theory, 2004, 50: 547-549.

[8] Thangaraj A, McLaughlin S W. Quantum codes from cyclic codes over $GF(4^m)$ [J]. IEEE Trans Inform Theory, 2001, 47: 1 176-1 178.

[9] Kai X, Zhu S. Quaternary construction of quantum codes from cyclic codes over $F_4 + uF_4$ [J]. Int J Quant Inform, 2011, 9: 689-700.

[10] Qian J, Ma W, Guo W. Quantum codes from cyclic codes over finite ring[J]. Int J Quant Inform, 2009, 7: 1 277-1 283.

[11] Ashikhmin A, Knill E. Nonbinary quantum stabilizer codes[J]. IEEE Trans Inform Theory, 2001, 47(7): 3 065-3 072.

[12] Bachoc C. Applications of coding theory to the construction of modular lattices[J]. J Combin, Theory Ser A, 1997, 78(1): 92-119.

[13] Gaborit P. Mass formulas for self-dual codes over Z_4 and $F_q + uF_q$ rings[J]. IEEE Trans Inform Theory, 1996, 42: 1 222-1 228.

[14] McDonald B R. Finite Rings With Identity[M]. New York: Dekker, 1974.

[15] Dinh H Q, Lpez-Permouth S R. Cyclic and negacyclic codes over finite chain rings[J]. IEEE Trans Inform Theory, 2004, 50: 1 728-1 744.