SKEW CYCLIC AND LCD CODES OVER $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$

LI Hui, HU Peng, LIU Xiu-sheng

(School of Mathematics and Physics, Hubei Polytechnic University, Huangshi 435003, China)

Abstract: In this paper, we investigate skew cyclic and LCD codes over the ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$ ($u^2 = u, v^2 = v, uv = vu = 0$), where $q$ is a prime power. Using some decompositions of linear codes and their duals over ring $R$, we obtain the generator polynomials of skew cyclic and their dual codes over $R$. Finally, we address the relationship of LCD codes between $R$ and $\mathbb{F}_q$. By means of the Gray map from $R$ to $\mathbb{F}_q^3$, we obtain that Gray images of LCD codes over $R$ are LCD codes over $\mathbb{F}_q$.

Keywords: skew cyclic codes; LCD codes; dual codes

2010 MR Subject Classification: 94B15; 11A15


1 Introduction

Cyclic codes over finite rings are important class from a theoretical and practical viewpoint. It was shown that certain good nonlinear binary codes could be found as images of linear codes over $\mathbb{Z}_4$ under the Gray map (see [1]). In [2], Zhu et al. studied constacyclic codes over ring $\mathbb{F}_2 + v\mathbb{F}_2$, where $v^2 = v$. We in [3] generated ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$, where $v^2 = v, u^2 = 0, uv = vu = 0$, and studied the structure of cyclic of an arbitrary length $n$ over this ring.

Boucher et al. in [4] initiated the study of skew cyclic codes over a noncommutative ring $\mathbb{F}_q[x, \Theta]$, called skew polynomial ring, where $\mathbb{F}_q$ is a finite field and $\Theta$ is a field automorphism of $\mathbb{F}_q$. Later, in [5], Abualrub and Seneviratne investigated skew cyclic codes over ring $\mathbb{F}_2 + v\mathbb{F}_2$, where $v^2 = v$. Moreover, Gao [6] and Gursoy et al. [7] presented skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and $\mathbb{F}_q + v\mathbb{F}_q$ with different automorphisms, respectively. Recently, Yan, Shi and Solé in [8] investigated skew cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + v\mathbb{F}_q$.

In this work, let $R$ denote the ring $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$ where $u^2 = u, v^2 = v$ and $uv = vu = 0$. In Section 2, we give some properties of ring $R$ and define the Gray map $\varphi$ from $R$ to $\mathbb{F}_q^3$. Moreover, we investigate some results about linear codes over $R$. In Section 3, we first give a sufficient and necessary condition which a code $C$ is a skew cyclic code over $R$. We then characterize the generator polynomials of skew cyclic codes and their dual over $R$. Finally, in Section 4, we address the relationship of LCD codes between $R$ and $\mathbb{F}_q$. By means of the

* Received date: 2016-11-01 Accepted date: 2017-02-16
Foundation item: Supported by Educational Commission of Hubei Province of China (D20144401); Research Project of Hubei Polytechnic University (17xjz03A).
Biography: Li Hui (1981–), female, born at Huangshi, Hubei, lecturer, major in algebraic coding.
Corresponding author: Hu Peng.
Gray map from $R$ to $\mathbb{F}_q^3$, we obtain that Gray images of LCD codes over $R$ are LCD codes over $\mathbb{F}_q$.

**2 Linear Codes Over $R$**

The ring $R$ is a finite commutative ring with characteristic $p$ and it contains three maximal ideals which are

$$I_1 = \langle u, v \rangle, \quad I_2 = \langle u - 1, v \rangle, \quad I_3 = \langle u, v - 1 \rangle.$$  

It is easy to verify that $\frac{R}{I_1}$, $\frac{R}{I_2}$, and $\frac{R}{I_3}$ are isomorphic to $\mathbb{F}_q^3$. Therefore $R \cong \mathbb{F}_q^3$. This means that $R$ is a principal ideal ring, i.e., $R$ is a Frobenius ring.

Let $R^n = \{ x = (x_1, \ldots, x_n) \mid x_j \in R \}$ be $R$-module. A $R$-submodule $C$ of $R^n$ is called a linear code of length $n$ over $R$. We assume throughout that all codes are linear.

Let $x, y \in R^n$, the Euclidean inner product of $x, y$ is defined as follows

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n.$$  

We call $C^\perp = \{ x \in R^n \mid x \cdot c = 0, \forall c \in C \}$ as the dual code of $C$. Notice that $C^\perp$ is linear if $C$ is linear or not.

In [8], it was proved that for any linear code $C$ over a finite Frobenius ring,

$$|C| \cdot |C^\perp| = R^n. \quad (2.1)$$

The Gray map $\varphi : R^n \rightarrow \mathbb{F}_q^{3n}$ is defined by $\varphi(x) = (\beta(x_1), \ldots, \beta(x_n))$ for $x = (x_1, \ldots, x_n)$, where $\beta(a + ub + vc) = (a, a + b, a + c)$ for $a + ub + vc \in R$ with $a, b, c \in \mathbb{F}_q$. By using this map, we can define the Lee weight $W_L$ and Lee distance $d_L$ as follows.

**Definition 2.1** For any element $x = (x_1, \ldots, x_n) \in R^n$, we define $W_L(x) = W_H(\varphi(x))$, where $W_H$ denotes the ordinary Hamming weight for codes over $\mathbb{F}_q$. The Lee distance $d_L(x, y)$ between two codewords $x$ and $y$ is the Lee weight of $x - y$.

**Lemma 2.2** The Gray map $\varphi$ is a distance-preserving map from $(R^n, \text{Lee distance})$ to $(\mathbb{F}_q^{3n}, \text{Hamming distance})$ and also $\mathbb{F}_q$-linear.

**Proof** From the definition, it is clear that $\varphi(x - y) = \varphi(x) - \varphi(y)$ for $x$ and $y \in R^n$. Thus $d_L(x, y) = d_H(\varphi(x), \varphi(y))$.

For any $x, y \in R^n$, $a, b \in \mathbb{F}_q$, from the definition of the Gray map, we have $\varphi(ax + by) = a \varphi(x) + b \varphi(y)$, which implies that $\varphi$ is an $\mathbb{F}_q$-linear map.

The following theorem is obvious.

**Theorem 2.3** If $C$ is a linear code of length $n$ over $R$, size $q^k$ and Lee distance $d_L$, then $\varphi(C)$ is a linear code over $\mathbb{F}_q$ with parameters $[3n, k, d_L]$.

**Theorem 2.4** If $C$ is a linear code of length $n$ over $R$, then $\varphi(C^\perp) = \varphi(C)^\perp$. Moreover, if $C$ is a self-dual code, so is $\varphi(C)$.

**Proof** Let $x_1 = a_1 + ub_1 + vc_1, x_2 = a_2 + ub_2 + vc_2 \in C$ be two codewords, where $a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{F}_q^n$, and $\cdot$ be the Euclidean inner product on $R^n$ or $\mathbb{F}_q^n$. Then

$$x_1 \cdot x_2 = a_1 \cdot a_2 + (a_1 b_2 + a_2 b_1 + b_1 b_2)u + (a_1 c_2 + a_2 c_1 + c_1 c_2)v$$
and
\[ \varphi(x_1) \cdot \varphi(x_2) = 3a_1 \cdot a_2 + (a_1b_2 + a_2b_1 + b_1b_2) + (a_1c_2 + a_2c_1 + c_1c_2). \]

It is easy to check that \( x_1 \cdot x_2 = 0 \) implies \( \varphi(x_1) \cdot \varphi(x_2) = 0. \) Therefore
\[ \varphi(C^\perp) \subset \varphi(C)^\perp. \] (2.2)

But by Theorem 2.3, \( \varphi(C) \) is a linear code of length \( 3n \) of size \( |C| \) over \( \mathbb{F}_q. \) So by usual properties of the dual of linear codes over finite fields, we know that \( |\varphi(C)^\perp| = \frac{3^n}{|C|}. \) So (2.1), this implies
\[ |\varphi(C^\perp)| = |\varphi(C)^\perp|. \] (2.3)

Combining (2.2) with (2.3), we get the desired equality.

Let \( e_1 = 1 - u - v, e_2 = u, e_3 = v. \) It is easy to check that \( e_ie_j = \delta_{ij}e_i \) and \( \sum_{k=1}^{3} e_k = 1, \)
where \( \delta_{ij} \) stands for Dirichlet function, i.e., \( \delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases} \) According to [9], we have
\[ R = e_1R \oplus e_2R \oplus e_3R. \]

Now, we mainly consider some familiar structural properties of a linear code \( C \) over \( R. \) The proof of following results can be found in [10], so we omit them here.

Let \( A_i (i = 1, 2, 3) \) be codes over \( R. \) We denote
\[ A_1 \oplus A_2 \oplus A_3 = \{a_1 + a_2 + a_3| a_i \in A_1, a_2 \in A_2, a_3 \in A_3 \}. \]

If \( C \) is a linear code of length \( n \) over \( R, \) we define that
\[ C_1 = \{a \in \mathbb{F}_q^n | \text{there are } b, c \in \mathbb{F}_q^n \text{ such that } e_1a + e_2b + e_3c \in C\}, \]
\[ C_2 = \{b \in \mathbb{F}_q^n | \text{there are } a, c \in \mathbb{F}_q^n \text{ such that } e_1a + e_2b + e_3c \in C\}, \]
\[ C_3 = \{c \in \mathbb{F}_q^n | \text{there are } a, b \in \mathbb{F}_q^n \text{ such that } e_1a + e_2b + e_3c \in C\}. \]

It is easy to verify that \( C_i (i = 1, 2, 3) \) are linear codes of length \( n \) over \( \mathbb{F}_q. \) Furthermore, \( C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3 \) and \( |C| = |C_1| |C_2| |C_3|. \) Throughout this paper, \( C_i (i = 1, 2, 3) \) will be reserved symbols referring to these special subcodes.

According to above definition and [10], we have the following theorem.

**Theorem 2.5** If \( C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3 \) is a linear code of length \( n \) over \( R, \) then \( C^\perp = e_1C_1^\perp \oplus e_2C_2^\perp \oplus e_3C_3^\perp. \)

The next theorem gives a computation for minimum Lee distance \( d_L \) of a linear code of length \( n \) over \( R. \)

**Theorem 2.6** If \( C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3 \) is a linear code of length \( n \) over \( R, \) then
\[ d_L(C) = \min\{d_H(C_1), d_H(C_2), d_H(C_3)\}. \]

**Proof** By Theorem 2.3, we have \( d_L(C) = d_H(\varphi(C)). \)

For any codeword \( x, \) it can be written as \( x = e_1a + e_2b + e_3c, \) where \( a \in C_1, b \in C_2, c \in C_3. \) Thus
\[ \varphi(x) = (a, b, c) = (a, 0, 0) + (0, b, 0) + (0, 0, c). \]
This means that \( d_L(C) = \min\{d_H(C_1), d_H(C_2), d_H(C_3)\} \).

3 Skew Cyclic Codes Over \( R \)

Let \( R = F_q + uF_q + vF_q \), where \( q = p^m \), \( p \) is a prime. For integer \( 0 \leq s \leq m \), we consider the automorphisms

\[
\Theta_s : F_q + uF_q + vF_q \rightarrow F_q + uF_q + vF_q, \\
a + ub + vc \rightarrow a^{p^s} + ub^{p^s} + vc^{p^s}.
\]

In this section, we first define skew polynomial rings \( R[x, \Theta_s] \) and skew cyclic codes over \( R \). Next, we investigate skew cyclic codes over \( R \) through a decomposition theorem.

**Definition 3.1** We define the skew polynomial ring as \( R[x, \Theta_s] = \{a_0 + a_1x + \cdots + a_nx^n | a_i \in R, i = 0, 1, \cdots, n\} \), where the coefficients are written on the left of the variable \( x \).

The addition is the usual polynomial addition and the multiplication is defined by the rule \( xa = \Theta_s(a)x \) (\( a \in R \)).

It is easy to prove that the ring \( R[x, \Theta_s] \) is not commutative unless \( \Theta_s \) is the identity automorphism on \( R \).

**Definition 3.2** A linear code \( C \) of length \( n \) over \( R \) is called skew cyclic code if for any codeword \( c = (c_0, c_1, \cdots, c_{n-1}) \in C \), the vector \( \Theta_s(c) = (\Theta_s(c_{n-1}), \Theta_s(c_0), \cdots, \Theta_s(c_{n-2})) \) is also a codeword in \( C \).

The following theorem characterizes skew cyclic codes of length \( n \) over \( R \).

**Theorem 3.3** Let \( C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3 \) be a linear code of length \( n \) over \( R \). Then \( C \) is a skew cyclic code of length \( n \) over \( R \) if and only if \( C_1, C_2 \) and \( C_3 \) are skew cyclic codes of length \( n \) over \( F_q \), respectively.

**Proof** Suppose that \( x_i = e_1a_i + e_2b_i + e_3c_i \), where \( a_i, b_i, c_i \in F_q, i = 0, 1, \cdots, n - 1 \), and \( x = (x_0, x_1, \cdots, x_{n-1}) \). Then

\[
x = e_1(a_0, a_1, \cdots, a_{n-1}) + e_2(b_0, b_1, \cdots, b_{n-1}) + e_3(c_0, c_1, \cdots, c_{n-1}) \in C.
\]

Set \( a = (a_0, a_1, \cdots, a_{n-1}) \), \( b = (b_0, b_1, \cdots, b_{n-1}) \), \( c = (c_0, c_1, \cdots, c_{n-1}) \), thus \( x = e_1a + e_2b + e_3c \) and \( a \in C_1 \), \( b \in C_2 \), \( c \in C_3 \). If \( C \) is a skew cyclic code of length \( n \) over \( R \), then

\[
\Theta_s(x) = e_1\Theta_s(a) + e_2\Theta_s(b) + e_3\Theta_s(c) \in C.
\]

Therefore \( \Theta_s(a) \in C_1, \Theta_s(b) \in C_2, \Theta_s(c) \in C_3 \). This means that \( C_1, C_2 \) and \( C_3 \) are skew cyclic codes.

Conversely, if \( C_i \) are skew cyclic codes over \( F_q \), then

\[
\Theta_s(x) = e_1\Theta_s(a) + e_2\Theta_s(b) + e_3\Theta_s(c) \in C.
\]

This implies that \( C \) is a skew cyclic code over \( R \).

**Theorem 3.4** Let \( C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3 \) be a skew cyclic code of length \( n \) over \( R \). Then
(1) \( C = (e_1 g_1(x), e_2 g_2(x), e_3 g_3(x)) \) and \( |C| = q^{3n - \sum_{i=1}^3 \deg g_i(x)} \), where \( g_i(x) \) is a generator polynomial of skew cyclic codes \( C_i \) of length \( n \) over \( \mathbb{F}_q \) for \( i=1,2,3 \).

(2) There is a unique polynomial \( g(x) \) such that \( C = \langle g(x) \rangle \) and \( g(x) \mid x^n - 1 \), where \( g(x) = e_1 g_1(x) + e_2 g_2(x) + e_3 g_3(x) \). Moreover, every left submodule of \( R[x, \Theta]/\langle x^n - 1 \rangle \) is principally generated.

**Proof** (1) Since \( C_i = \langle g_i(x) \rangle \subset \mathbb{F}_q[x, \Theta]/\langle x^n - 1 \rangle \) for \( i=1,2,3 \) and \( C = e_1 C_1 \oplus e_2 C_2 \oplus e_3 C_3 \), \( C = \langle c(x) | c(x) = e_1 f_1(x) + e_2 f_2(x) + e_3 f_3(x), f_i(x) \in C_i, i = 1, 2, 3 \rangle \). Thus

\[
C \subset \langle e_1 g_1(x), e_2 g_2(x), e_3 g_3(x) \rangle.
\]

On the other hand, for any \( e_1 r_1(x) g_1(x) + e_2 r_2(x) g_2(x) + e_3 r_3(x) g_3(x) \in \langle e_1 g_1(x), e_2 g_2(x), e_3 g_3(x) \rangle \subset R[x, \Theta]/\langle x^n - 1 \rangle \), where \( r_1(x), r_2(x) \) and \( r_3(x) \in R[x, \Theta]/\langle x^n - 1 \rangle \), there exist \( s_1(x), s_2(x) \) and \( s_3(x) \in \mathbb{F}_q[x, \Theta]/\langle x^n - 1 \rangle \) such that \( e_1 r_1(x) = e_1 s_1(x), e_2 r_2(x) = e_2 s_2(x) \) and \( e_3 r_3(x) = e_3 s_3(x) \). Hence

\[
e_1 r_1(x) g_1(x) + e_2 r_2(x) g_2(x) + e_3 r_3(x) g_3(x) = e_1 s_1(x) g_1(x) + e_2 s_2(x) g_2(x) + e_3 s_3(x) g_3(x),
\]

which implies that \( \langle e_1 g_1(x), e_2 g_2(x), e_3 g_3(x) \rangle \subset C \). Therefore \( C = \langle e_1 g_1(x), e_2 g_2(x), e_3 g_3(x) \rangle \).

In light of \( |C| = |C_1| \cdot |C_2| \cdot |C_3| \), we have \( |C| = q^{3n - \sum_{i=1}^3 \deg g_i(x)} \).

(2) Obviously, \( \langle e_1 g_1(x) + e_2 g_2(x) + e_3 g_3(x) \rangle \subset \langle e_1 g_1(x), e_2 g_2(x), e_3 g_3(x) \rangle \).

Note that \( g(x) = e_1 g_1(x), e_2 g_2(x) = e_2 g_2(x) \) and \( e_3 g_3(x) = e_3 g_3(x) \), we have \( C \subset \langle g(x) \rangle \). Therefore, \( C = \langle g(x) \rangle \).

Since \( g_1(x), g_2(x) \) and \( g_3(x) \) are monic right divisors of \( x^n - 1 \), there exist \( h_1(x), h_2(x) \) and \( h_3(x) \in \mathbb{F}_q[x, \Theta]/\langle x^n - 1 \rangle \) such that \( x^n - 1 = h_1(x) g_1(x) = h_2(x) g_2(x) = h_3(x) g_3(x) \). Therefore \( x^n - 1 = [e_1 h_1(x) + e_2 h_2(x) + e_3 h_3(x)] g(x) \). It follows that \( g(x) \mid x^n - 1 \). The uniqueness of \( g(x) \) can be followed from that of \( g_1(x), g_2(x) \) and \( g_3(x) \).

Let \( g(x) = g_0 + g_1 x + \cdots + g_k x^k \) and \( h(x) = h_0 + h_1 x + \cdots + h_{n-k} x^{n-k} \) be polynomials in \( \mathbb{F}_q[x, \Theta] \) such that \( x^n - 1 = h(x) g(x) \) and \( C \) be the skew cyclic code generated by \( g(x) \) in \( \mathbb{F}_q[x, \Theta] \). Then the dual code of \( C \) is a skew cyclic code generated by the polynomial \( \overline{h}(x) = h_{n-k} + \Theta_s(h_{n-k-1}) x + \cdots + \Theta_s^{n-k}(h_0) x^{n-k} \) (see [11]).

**Corollary 3.5** Let \( C_1, C_2, C_3 \) be skew cyclic codes of length \( n \) over \( \mathbb{F}_q \) and \( g_1(x), g_2(x), g_3(x) \) be their generator polynomials such that

\[
x^n - 1 = h_1(x) g_1(x) = h_2(x) g_2(x) = h_3(x) g_3(x)
\]

in \( \mathbb{F}_q[x, \Theta] \). If \( C = e_1 C_1 \oplus e_2 C_2 \oplus e_3 C_3 \), then

(1) \( C^\perp = \langle \overline{h}(x) \rangle \) is also a skew cyclic code of length \( n \) over \( R \), where \( \overline{h}(x) = e_1 \overline{h}_1(x) + e_2 \overline{h}_2(x) + e_3 \overline{h}_3(x) \), and \( |C^\perp| = q^{3n - \sum_{i=1}^3 \deg \overline{h}_i(x)} \).

(2) \( C \) is a self-dual skew cyclic code over \( R \) if and only if \( C_1, C_2 \) and \( C_3 \) are self-dual skew cyclic codes of length \( n \) over \( \mathbb{F}_q \).

**Proof** (1) In light of Theorem 2.5, we obtain \( C^\perp = e_1 C_1^\perp \oplus e_2 C_2^\perp \oplus e_3 C_3^\perp \).
Since $C_1^\perp = \langle \overline{t}_1(x) \rangle$, $C_2^\perp = \langle \overline{t}_2(x) \rangle$ and $C_3^\perp = \langle \overline{t}_3(x) \rangle$, we have $C^\perp = \langle \overline{t}(x) \rangle$ and $|C^\perp| = q^{\frac{3}{2} \deg_9(x)}$ by Theorem 3.2.

(2) $C$ is a self-dual skew cyclic code over $R$ if and only if $g(x) = \overline{h}(x)$, i.e., $g_1(x) = \overline{h}_1(x)$, $g_2(x) = \overline{h}_2(x)$ and $g_3(x) = \overline{h}_3(x)$. Thus $C$ is a self-dual skew cyclic code over $R$ if and only if $C_1$, $C_2$ and $C_3$ are self-dual skew cyclic codes of length $n$ over $\mathbb{F}_q$.

**Example 1** Let $\omega$ a primitive element of $\mathbb{F}_9$ (where $\omega = 2\omega + 1$) and $\Theta$ be the Frobenius automorphism over $\mathbb{F}_9$, i.e., $\Theta(a) = a^3$ for any $a \in \mathbb{F}_9$. Then

$$x^6 - 1 = (2 + (2 + \omega)x + (1 + 2\omega)x^3 + x^4)(1 + (2 + \omega)x + x^2) = (2 + x + (2 + 2\omega)x^2 + x^3)(1 + x + 2\omega x^2 + x^3) \in \mathbb{F}_9[x; \Theta].$$

Let $g_1(x) = 2 + (2 + \omega)x + (1 + 2\omega)x^3 + x^4$ and $g_2(x) = g_3(x) = 2 + x + (2 + 2\omega)x^2 + x^3$. Then $C_1 = \langle g_1(x) \rangle$ and $C_2 = C_3 = \langle g_2(x) \rangle$ are skew cyclic codes of length 6 over $\mathbb{F}_9$ with dimensions $k_1 = 2$, $k_2 = k_3 = 3$, respectively. Take $g(x) = e_1 g_1(x) + e_2 g_2(x) + e_3 g_3(x)$, then $C$ is a skew cyclic code of length 6 over $R$. Thus the Gray image of $C$ is a $[18, 8, 4]$ code over $\mathbb{F}_9$.

## 4 LCD Codes over $R$

Linear complementary dual codes (which is abbreviated to LCD codes) are linear codes that meet their dual trivially. These codes were introduced by Massey in [12] and showed that asymptotically good LCD codes exist, and provide an optimum linear coding solution for the two-user binary adder channel. In [13], Sendrier indicated that linear codes with complementary-duals meet the asymptotic Gilbert-Varshamov bound. They are also used in counter measure to passive and active side channel analyses on embedded crypto-systems (see [14]). In recent, we in [15] investigated LCD codes finite chain ring. Motivated by these works, we will consider the LCD codes over $R$.

Suppose that $f(x)$ is a monic (i.e., leading coefficient 1) polynomial of degree $k$ with $f(0) = c \neq 0$. Then by monic reciprocal polynomial of $f(x)$ we mean the polynomial $\tilde{f}(x) = c^{-1}f^*(x)$.

We recall a result about LCD codes which can be found in [16].

**Proposition 4.1** If $g_1(x)$ is the generator polynomial of a cyclic code $C$ of length $n$ over $\mathbb{F}_q$, then $C$ is an LCD code if and only if $g_1(x)$ is self-reciprocal (i.e., $\overline{g}_1(x) = g_1(x)$) and all the monic irreducible factors of $g_1(x)$ have the same multiplicity in $g_1(x)$ and in $x^n - 1$.

**Theorem 4.2** If $C = e_1 C_1 \oplus e_2 C_2 \oplus e_3 C_3$ is a linear code over $R$, then $C$ is a LCD code over $R$ if and only if $C_1, C_2$ and $C_3$ are LCD codes over $\mathbb{F}_q$.

**Proof** $C$ is a LCD code over $R$ if and only if $C \cap C^\perp = \{0\}$. By Theorem 2.5, we know that $C \cap C^\perp = \{0\}$ if and only if $C_1 \cap C_1^\perp = \{0\}$, $C_2 \cap C_2^\perp = \{0\}$, and $C_3 \cap C_3^\perp = \{0\}$, i.e., $C_1, C_2$ and $C_3$ are LCD codes over $\mathbb{F}_q$.

By means of Proposition 4.1 and above theorem, we have the following corollary.
Corollary 4.3 Let $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3$ is a cyclic code of length $n$ over $R$, and let $C_1 = \langle g_1(x) \rangle$, $C_2 = \langle g_2(x) \rangle$ and $C_3 = \langle g_3(x) \rangle$ be cyclic codes of length $n$ over $\mathbb{F}_q$. Then $C$ is a LCD code over $R$ if and only if $g_1(x)$ is self-reciprocal (i.e., $\bar{g}_i(x) = g_i(x)$) and all the monic irreducible factors of $g_i(x)$ have the same multiplicity in $g_i(x)$ and in $x^n - 1$ for $i = 1, 2, 3$.

Theorem 4.4 A linear code $C \subset R^n$ is LCD if and only if the linear code $\varphi(C) \subset \mathbb{F}^{3n}_q$ is LCD.

Proof If $x \in C \cap C^\perp$, then $x \in C$ and $x \in C^\perp$. It follows that $\varphi(x) \in \varphi(C)$ and $\varphi(x) \in \varphi(C^\perp)$. Hence $\varphi(C \cap C^\perp) \subset \varphi(C) \cap \varphi(C^\perp)$.

On the other hand, if $\varphi(x) \in \varphi(C) \cap \varphi(C^\perp)$, then there are $y \in C$ and $z \in C^\perp$ such that $\varphi(x) = \varphi(y) = \varphi(z)$. Since $\varphi$ is an injection, $x = y = z \in C \cap C^\perp$, which implies that $\varphi(x) \in \varphi(C \cap C^\perp)$, i.e., $\varphi(C) \cap \varphi(C^\perp) \subset \varphi(C \cap C^\perp)$.

Thus $\varphi(C) \cap \varphi(C^\perp) = \varphi(C \cap C^\perp)$.

By Theorem 2.3, we $\varphi(C \cap C^\perp) = \varphi(C) \cap \varphi(C^\perp)$ and $\varphi(C \cap C^\perp)$ follows that $C \subset R^n$ is LCD if and only if the linear code $\varphi(C) \subset \mathbb{F}^{3n}_q$ is LCD.

Example 2 $x^4 - 1 = (x + 1)(x + 2)(x + w^2)(x + w^6)$ in $\mathbb{F}_9$. Let $g_1(x) = g_2(x) = g_3(x) = x + 1$. Then $C_1 = C_2 = C_3 = \langle g_1(x) \rangle$ are LCD cyclic codes over $\mathbb{F}_9$ with parameters $[4, 3, 2]$, respectively. Suppose that $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3$ is a cyclic code of length $n$ over $R$. By Theorem 2.6 and Theorem 4.5, $\varphi(C)$ is a LCD code with parameters $[12, 9, 2]$, which is an optimal code.

References

环$\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$上的斜循环码和LCD码

李 慧, 胡 鹏, 刘修生
(湖北理工学院数学学院, 湖北 黄石 453003)

摘要：本文研究了环$R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$ $(u^2 = u, v^2 = v, uv = vu = 0)$上的斜循环码和LCD码，其中$q$为素数$2$. 利用线性码与其对偶码在环$R$上的分解，得到了环$R$上斜循环码及其对偶码的生成多项式，最后，讨论了环$R$与有限域$\mathbb{F}_q$上LCD码的关系，通过环$R$到域$\mathbb{F}_q$的Gray映射，得到了环$R$上LCD码的Gray像是$\mathbb{F}_q$上的LCD码。

关键词：斜循环码; LCD码; 对偶码

MR(2010) 主题分类号：94B15 ; 11A15 中图分类号：O236.2