Vol. 35 (2015)
No. 5

数 学 杂 志
J. of Math. (PRC)

CYCLIC AND CONSTACYCLIC CODES OVER $F_3 + vF_3$

LIU Xiu-sheng [1], XU Xiao-fang [1], HUANG Zheng-hua [2]

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

(*2. College of Mathematics and Statistics, Hubei Normal University, Huangshi 435002, China*)

Abstract: In this paper, we focus on cyclic and constacyclic codes over the ring $F_3+vF_3(v^2 = 1)$, which is not a finite chain ring. We study the relationship between cyclic codes over $F_3 + vF_3$ and ternary cyclic codes, and prove that cyclic codes over the ring are generated by a polynomial over $F_3 + vF_3$. Then, using similar method, we obtain the generator polynomial of v-constacyclic codes.

Keywords: cyclic codes; constacyclic codes; Gray map; generator polynomial

2010 MR Subject Classification: 94B05; 94B99

Document code: A **Article ID:** 0255-7797(2015)05-1115-12

1 Introduction

Codes over finite rings received much attention recently after it was proved that important families of binary non-linear codes are in fact images under a Gray map of linear codes over Z_4, see [3], and the references cited there. In order to obtain a complete understanding about binary codes which have certain structural properties, we need to examine cyclic codes over large families of rings. Cyclic and constacyclic codes over $F_2 + uF_2(u^2 = 0)$ were studied in [4–7]. The structure of cyclic codes over $Z_2 + uZ_2(u^2 = 0)$ and $Z_2 + uZ_2 + u^2Z_2(u^3 = 0)$ were determined in [8]. Moreover, cyclic and constacyclic codes over ring $F_2 + uF_2 + vF_2 + uvF_2(u^2 = v^2 = 0, uv = vu)$ were described in [9, 10]. However, not much work was done on the structure of cyclic and constacyclic codes over $F_3 + vF_3(v^2 = 1)$.

The purpose of this paper is to obtain structure theorems for cyclic, negacyclic, constacyclic codes and their duals over $R_3 := F_3 + vF_3$, defined with $v^2 = 1$. The ring R_3 is a Semi-local ring like Z_6, as noticed in [1] abstractly isomorphic to $F_3 \times F_3$. The main technical tool in that context is therefore the Chinese Remainder Theorem.

In Section 2, we recall some backgrounds and notation about this ring, and define a Gray map φ from R_3^n to F_3^{2n}. In Section 3, by means of the decomposition of the linear

* **Received date:** 2013-09-22 **Accepted date:** 2013-11-06

Foundation item: Supported by Scientific Research Foundation of Hubei Provincial Education Department of China (B2013069) and the National Science Foundation of Hubei Polytechnic University of China (12xjz14A).

Biography: Liu Xiusheng(1960–), male, born at Daye, Hubei, professor, major in groups and algebraic coding, multiple linear algebra.

codes H over R_3, we obtain that $\varphi(H)$ are the linear codes over F_3. We tackle with the issues of duality, Lee weight enumerators and MacWilliams identities for linear codes over R_3. In Section 4, the structure of cyclic codes and cyclic self-dual codes over R_3 is described, and the relationship between cyclic codes over R_3 and ternary cyclic codes is studied. We prove that every cyclic codes over R_3 is principally generated and determine the generator polynomials of cyclic codes over the ring. In Section 5, a v-contacyclic code over R_3 are defined. We discuss the generator element of a v-contacyclic code over R_3. Some examples are given in Section 6 to illustrate the discussed results.

2 Notations and Definitions

Let R_3 denote the commutative ring with 9 elements $F_3 + vF_3 = \{0, 1, 2, v, 1 + v, 2 + v, 2v, 1 + 2v, 2 + 2v\}$, where $v^2 = 1$. It is easy to verify that R is a semi-local ring with two maximal ideals given by $\langle v-1\rangle$ and $\langle v+1\rangle$. Observe that both of $R_3/\langle v - 1\rangle$ and $R_3/\langle v + 1\rangle$ are F_3. The CRT tells us that

$$R_3 = \langle v - 1\rangle \oplus \langle v + 1\rangle.$$

More concretely, linear algebra over F_3 shows that

$$a + vb = (a - b)(v - 1) - (a + b)(v + 1)$$

for all $a, b \in F_3^n$.

A linear code H over R_3 of length n is an R_3-submodule of R_3^n. Let $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$ be two elements of R^n, the Euclidean inner product of x and y in R_3^n is defined by

$$x \cdot y = \sum_{i=1}^{n} x_i y_i,$$

where the operation is performed in R_3. The dual code of H is defined as $H^\perp = \{x \in R_3^n | x \cdot y = 0, \forall y \in H\}$. By the results in [12], we obtain that a linear codes H satisfies $|H| \cdot |H^\perp| = |R_3|^n$. We say that a code is self-orthogonal if $C \subset C^\perp$ and self-dual if $C = C^\perp$.

Let H be a linear code over R_3 of length n and $P(H)$ be its polynomial representation, i.e.,

$$P(H) = \{\sum_{i=0}^{n-1} h_i x^i | (h_0, h_1, \cdots, h_{n-1}) \in H\}.$$

Let σ and γ be maps from R_3^n to R_3^n given by

$$\sigma(h_0, h_1, \cdots, h_{n-1}) = (h_{n-1}, h_0, h_1, \cdots, h_{n-2})$$

and

$$\gamma(h_0, h_1, \cdots, h_{n-1}) = (-h_{n-1}, h_0, h_1, \cdots, h_{n-2}),$$

respectively. Then H is said to be cyclic if $\sigma(H) = H$, and negacyclic of $\gamma(H) = H$. A linear code H over R_3 of length n is cyclic if and only if $P(H)$ is an ideal of $R_3[x]/\langle x^n - 1\rangle$,

and a linear code H over R_3 of length n is negacyclic if and only if $P(H)$ is an ideal of $R_3[x]/\langle x^n + 1\rangle$.

The Gray map φ from R_3^n to F_3^{2n} is defined as $\varphi(x + vy) = (-(x + y), y - x)$ for all $x, y \in F_3^n$. The Lee weight of $x + vy$ is the Hamming weight of its Gray image. Then, φ is weight-preserving map from (R_3^n, Lee weight) to (F_3^{2n}, Hamming weight), that is, $w_L(h) = w_H(\varphi(h))$.

3 Linear Codes Over $F_3 + vF_3$

If A and B are codes, we denote that $A \otimes B = \{(a, b)|a \in A, b \in B\}$ and $A \oplus B = \{a + b|a \in A, b \in B\}$.

The following results can be found in [2].

A nonzero linear code C over R has a generator matrix which after a suitable permutation of the coordinate can be written in the form

$$G = \begin{pmatrix} I_{k_1} & (1-v)B_1 & (1+v)A_1 & (1+v)A_2 + (1-v)B_2 & (1+v)A_3 + (1-v)B_3 \\ 0 & (1+v)I_{k_2} & 0 & (1+v)A_4 & 0 \\ 0 & 0 & (1-v)I_{k_3} & 0 & (1-v)B_4 \end{pmatrix}, \tag{3.1}$$

where A_i and B_j are ternary matrices, and $|C| = 9^{k_1}3^{k_2}3^{k_3}$.

Let H be a code over R_3. Define

$$H^+ = \{s|\exists t \in F_3^n|(1 + v)s + (1 - v)t \in H\}$$

and

$$H^- = \{t|\exists s \in F_3^n|(1 + v)s + (1 - v)t \in H\}.$$

We have $H = (1 + v)H^+ \oplus (1 - v)H^-$. Obviously, the code H^+ is permutation-equivalent to a code with generator matrix of the form

$$G_1 = \begin{pmatrix} I_{k_1} & 0 & 2A_1 & 2A_2 & 2A_3 \\ 0 & I_{k_2} & 0 & A_4 & 0 \end{pmatrix}, \tag{3.2}$$

where A_i are ternary matrices. And the ternary code H^- is permutation-equivalent to a code with generator matrix of the form

$$G_2 = \begin{pmatrix} I_{k_1} & 2B_1 & 0 & 2B_2 & 2B_3 \\ 0 & 0 & I_{k_3} & 0 & B_4 \end{pmatrix}, \tag{3.3}$$

where B_i are ternary matrices.

Theorem 3.1 If H is a linear code of length n over R_3, then $\varphi(H) = H^+ \otimes H^-$, and $\varphi(H)$ is linear.

Proof For any $(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n) \in \varphi(H)$, let

$$h_i = x_i(1 + v) + y_i(1 - v) = (x_i + y_i) + v(x_i - y_i), i = 1, 2, \cdots, n$$

and let $h = (h_1, \cdots, h_n)$. Then $\varphi(h) = (x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n)$. Since φ is a bijection, $h = (h_1, \cdots, h_n) \in H$. By the definitions of H^+ and H^-, we have

$$(x_1, x_2, \cdots, x_n) \in H^+, (y_1, y_2, \cdots, y_n) \in H^-,$$

hence $(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n) \in H^+ \otimes H^-$. This implies that $\varphi(H) \subseteq H^+ \otimes H^-$.

Conversely, for any $(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n) \in H^+ \otimes H^-$, where $(x_1, x_2, \cdots, x_n) \in H^+$, $(y_1, y_2, \cdots, y_n) \in H^-$, there are $s = (s_1, \cdots, s_n), t = (t_1, \cdots, t_n) \in H$, such that

$$s_i = (1+v)x_i + (1-v)a_i, t_i = (1+v)b_i + (1-v)y_i,$$

where $a_i, b_i \in F_3$, $1 \leq i \leq n$. Since H is linear, we obtain that

$$h = -(1+v)s - (1-v)t = (1+v)x + (1-v)y \in H,$$

where $x = (x_1, x_2, \cdots, x_n) \in F_3^n, y = (y_1, y_2, \cdots, y_n) \in F_3^n$. It follows that $\varphi(h) = (x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n)$, which gives $H^+ \otimes H^- \subseteq \varphi(H)$. Therefore $\varphi(H) = H^+ \otimes H^-$.

The second result is easy to be verified.

Corollary 3.2 Let $H = (1+v)H^+ \oplus (1-v)H^-$ be a linear code of length n over R_3. Then $d_L(H) = min\{d(H^+), d(H^-)\}$, where $d(H^+)$ and $d(H^-)$ denote the minimum weight of ternary codes of H^+ and H^-, respectively.

Theorem 3.3 Let $H^\perp$ be the dual code of H. Then $\varphi(H^\perp) = \varphi(H)^\perp$. Moreover, if H is a self-dual code, so is $\varphi(H)$.

Proof To prove the theorem, we first show

$$\varphi(H^\perp) \subset \varphi(H)^\perp,$$

i.e., $\forall h_1, h_2 \in R_3^n$,

$$[h_1, h_2] = 0 \Rightarrow [\varphi(h_1), \varphi(h_2)] = 0. \tag{3.4}$$

To this extent, we assume that

$$h_1 = x_1 + vy_1, h_2 = x_2 + vy_2.$$

Then we have

$$[h_1, h_2] = [x_1, x_2] + [y_1, y_2] + ([x_1, y_2] + [y_1, x_2])v.$$

Note that $[h_1, h_2] = 0$ if and only if

$$[x_1, x_2] + [y_1, y_2] = 0, \tag{3.5}$$

$$[x_1, y_2] + [y_1, x_2] = 0, \tag{3.6}$$

since $\varphi(h_1) = (-(x_1 + y_1), y_1 - x_1), \varphi(h_2) = (-(x_2 + y_2), y_2 - x_2)$, then we have

$$[\varphi(h_1), \varphi(h_2)] = 2([x_1, x_2] + [y_1, y_2]) = 0,$$

by (3.5), this completes the proof of (3.4). Therefore

$$\varphi(H^{\perp}) \subset \varphi(H)^{\perp}. \tag{3.7}$$

By Theorem 3.1, $\varphi(H)$ is a ternary linear code of length $2n$ of size $|H|$. So by the usual properties of the dual of ternary codes, we know that

$$|\varphi(H)^{\perp}| = \frac{3^{2n}}{|\varphi(H)|} = \frac{3^{2n}}{|H|}.$$

Since R_3 is a Frobenius ring, we have $|H| \cdot |H^{\perp}| = 3^{2n}$. Hence, this implies

$$|\varphi(H^{\perp})| = |\varphi(H)^{\perp}|. \tag{3.8}$$

Combining (3.7) and (3.8), we have $\varphi(H^{\perp}) = \varphi(H)^{\perp}$.

Corollary 3.4 Let $H = (1+v)H^{+} \oplus (1-v)H^{-}$ be a linear code of length n over R_3. Then $\varphi(H^{\perp}) = (H^{+})^{\perp} \otimes (H^{-})^{\perp}$. Moreover, we have $H^{\perp} = (1+v)(H^{+})^{\perp} \oplus (1-v)(H^{-})^{\perp}$.

Proof Follows by applying Theorem 3.1 and Theorem 3.3.

We want to finish this section by remarking a MacWilliams identity for the Lee weight enumerators of linear codes over R_3. Suppose $H = (1+v)H^{+} \bigoplus (1-v)H^{-}$ is a linear code of length n over R_3 and let

$$\mathrm{Lee}_H(\bar{X}, \bar{Y}) = \sum_{h \in H} \bar{X}^{2n - w_L(h)} \bar{Y}^{w_L(h)}$$

be the Lee weight enumerator of H. Now, since φ maps H to a ternary linear code of length $2n$ and since φ is weight preserving, we see that

$$\mathrm{Lee}_H(\bar{X}, \bar{Y}) = \mathrm{Ham}_{\varphi(H)}(\bar{X}, \bar{Y}),$$

where $\mathrm{Ham}_{\varphi(H)}(\bar{X}, \bar{Y})$ denotes the Hamming weight enumerator of $\varphi(H)$.

We see, by Theorem 3.3 that $\varphi(H^{\perp}) = \varphi(H)^{\perp}$, and since we have the ordinary MacWilliams identity for Hamming weight enumerator of ternary linear codes, we get

$$\begin{aligned}
\mathrm{Lee}_{H^{\perp}}(\bar{X}, \bar{Y}) &= \mathrm{Ham}_{\varphi(H^{\perp})}(\bar{X}, \bar{Y}) = \mathrm{Ham}_{\varphi(H)^{\perp}}(\bar{X}, \bar{Y}) \\
&= \frac{1}{|\varphi(H)|} \mathrm{Ham}_{\varphi(H)}(\bar{X} + 2\bar{Y}, \bar{X} - \bar{Y}) \\
&= \frac{1}{|H^{+}| \cdot |H^{-}|} \mathrm{Ham}_{H^{+} \otimes H^{-}}(\bar{X} + 2\bar{Y}, \bar{X} - \bar{Y}) \\
&= \frac{1}{|H^{+}| \cdot |H^{-}|} \mathrm{Ham}_{H^{+}}(\bar{X} + 2\bar{Y}, \bar{X} - \bar{Y}) \cdot \mathrm{Ham}_{H^{-}}(\bar{X} + 2\bar{Y}, \bar{X} - \bar{Y}) \\
&= \mathrm{Ham}_{(H^{+})^{\perp}}(\bar{X}, \bar{Y}) \cdot \mathrm{Ham}_{(H^{-})^{\perp}}(\bar{X}, \bar{Y}).
\end{aligned}$$

Thus we have proved the following corollary.

Corollary 3.5 Suppose that $H = (1+v)H^{+} \oplus (1-v)H^{-}$ is a linear code of length n over R_3 and let $\mathrm{Lee}_H(\bar{X}, \bar{Y})$ denote its Lee weight enumerator as defined above, then

$$\mathrm{Lee}_{H^{\perp}}(\bar{X}, \bar{Y}) = \mathrm{Ham}_{(H^{+})^{\perp}}(\bar{X}, \bar{Y}) \cdot \mathrm{Ham}_{(H^{-})^{\perp}}(\bar{X}, \bar{Y}).$$

4 Cyclic and Negacyclic Codes $F_3 + vF_3$

Theorem 4.1 If $H = (1+v)H^+ \oplus (1-v)H^-$ is a linear code of length n over R_3, then H is a cyclic code over R_3 if and only if H^+, H^- are ternary cyclic codes.

Proof For any $h = (h_0, h_1, \cdots, h_{n-1}) \in H$, where

$$h_i = x_i(v+1) + y_i(1-v) = (x_i + y_i) + v(x_i - y_i), i = 0, 1, \cdots, n-1.$$

Taking $x = (x_0, x_1, \cdots, x_{n-1}), y = (y_0, y_1, \cdots, y_{n-1})$, we obtain that $x \in H^+, y \in H^-$. If H^+, H^- are ternary cyclic codes, then $\sigma(x) \in H^+, \sigma(y) \in H^-$. Hence $\sigma(h) = (v+1)\sigma(x) + (1-v)\sigma(y) \in H$, which implies that H is a cyclic code over R_3.

Conversely, for any $x = (x_1, x_2, \cdots, x_n) \in H^+, y = (y_1, y_2, \cdots, y_n) \in H^-$, writing $h = x(v+1) + y(1-v)$, then $h \in H$. Suppose that H is a cyclic code over R_3. Then we have

$$\sigma(h) = (v+1)\sigma(x) + (1-v)\sigma(y) = (\sigma(x) + \sigma(y)) + v(\sigma(x) - \sigma(y)) \in H.$$

Therefore $\varphi(\sigma(h)) = (\sigma(x), \sigma(y)) \in H^+ \otimes H^-$. We obtain that $\sigma(x) \in H^+, \sigma(y) \in H^-$, which proves that H^+, H^- are ternary cyclic codes.

Similarly, we can prove the following theorem.

Theorem 4.2 If $H = (1+v)H^+ \oplus (1-v)H^-$ is a linear code over R_3, then H is a negacyclic code over R_3 if and only if H^+, H^- are ternary negacyclic codes.

The following corollary is easy to be proved.

Corollary 4.3 If H is a cyclic (or negacyclic) code over R_3, then the dual code $H^\perp$ is also cyclic (or negacyclic).

Theorem 4.4 If $H = (1+v)H^+ \oplus (1-v)H^-$ is a cyclic code of length n over R_3, then $H = \langle (1+v)g_1(x) + (1-v)g_2(x) \rangle$ and $|H| = 3^{2n - \deg(g_1(x)) - \deg(g_2(x))}$, where $g_1(x)$ and $g_2(x)$ are the monic generator polynomials of H^+ and H^-, respectively.

Proof By Theorem 4.1, we have

$$H^+ = \langle g_1(x) \rangle \subset \frac{F_3[x]}{\langle x^n - 1 \rangle}, H^- = \langle g_2(x) \rangle \subset \frac{F_3[x]}{\langle x^n - 1 \rangle}$$

and

$$H = \{h(x) | h(x) = (1+v)f_1(x) + (1-v)f_2(x), f_1(x) \in H^+, f_2(x) \in H^-\}.$$

Therefore,

$$H \subset \langle (1+v)g_1(x), (1-v)g_2(x) \rangle.$$

Note that

$$-(1+v)[(1+v)g_1(x) + (1-v)g_2(x)] = (1+v)g_1(x)$$

and $-(1-v)[(1+v)g_1(x) + (1-v)g_2(x)] = (1-v)g_2(x)$, so

$$H \subset \langle (1+v)g_1(x) + (1-v)g_2(x) \rangle.$$

On the other hand, for any

$$h(x)[(1+v)g_1(x) + (1-v)g_2(x)] \in \langle (1+v)g_1(x) + (1-v)g_2(x)\rangle,$$

where

$$h(x) \in R_3[x]/\langle x^n - 1\rangle,$$

there are $m_1(x), m_2(x) \in F_3[x]$ such that $(1+v)h(x) = (1+v)m_1(x)$ and

$$(1-v)h(x) = (1-v)m_2(x).$$

So $\langle (1+v)g_1(x) + (1-v)g_2(x)\rangle \subseteq H$. This implies that

$$H = \langle (1+v)g_1(x) + (1-v)g_2(x)\rangle.$$

Since $|H| = |H^+| \cdot |H^-|$, then $|H| = 3^{2n-\deg(g_1(x))-\deg(g_2(x))}$.

Corollary 4.5 Every ideal of $\frac{R_3[x]}{\langle x^n-1\rangle}$ is principal.

If $f(x) = a_0 + a_1x + \cdots + a_rx^r$, then the reciprocal of $f(x)$ is the polynomial

$$f^*(x) = a_r + a_{r-1}x + \cdots + a_0x^r.$$

Symbolically, $f^*(x)$ can be expressed by $f^*(x) = x^rf(\frac{1}{x})$.

Corollary 4.6 With the notations as in Theorem 4.4. Let

$$x^n - 1 = h_1(x)g_1(x) = h_2(x)g_2(x),$$

then $H^\perp = \langle (1+v)g_1^*(x) + (1-v)g_2^*(x)\rangle$ and $|H^\perp| = 3^{\deg(g_1(x))+\deg(g_2(x))}$.

Theorem 4.7 Let $x^n - 1 = \prod_{i=1}^r p_i^{s_i}(x)$ be unique representations of $x^n - 1$ as a product of ireducible pairwise-comprime polynomial in $F_3[x]$. Then the number of the cyclic code of length n over R_3 is $\prod_{i=1}^r (s_i+1)^2$.

Proof The result directly follows from the fact that the number of ternary cyclic code of length n is $\prod_{i=1}^r (s_i+1)$.

5 v-Constacyclic Codes Over R_3

A v-constacyclic shift τ acts on R_3^n as

$$\tau(k_0, k_1, \cdots, k_{n-1}) = (vk_{n-1}, k_0, k_1, \cdots, k_{n-2}).$$

A linear code H over R_3 of length n is said to be a v-constacyclic code if invariant under the v-constacyclic shift, i.e., $\tau(H) = H$.

Theorem 5.1 Let $H = (1+v)H^+ \oplus (1-v)H^-$ be a linear code of length n over R_3. Then H is a v-constacyclic code of length n over R_3 if and only if H^+, H^- are cyclic and negacyclic codes of length n over F_3, respectively.

Proof For any $h = (h_0, h_1, \cdots, h_{n-1}) \in H$, we can write its components as $h_i = x_i(v+1) + y_i(1-v)$, where $x_i, y_i \in F_3, 0 \leq i \leq n-1$. Let

$$x = (x_0, x_1, \cdots, x_{n-1}), y = (y_0, y_1, \cdots, y_{n-1}),$$

then $x \in H^+, y \in H^-$. If H^+, H^- are cyclic and negacyclic codes over F_3, respectively, then $\sigma(x) \in H^+, \gamma(y) \in H^-$. Therefore, we have

$$\begin{aligned}\tau(h) &= (v(x_{n-1}(1+v) + y_{n-1}(1-v)), x_0(1+v) + y_0(1-v), \cdots, x_{n-2}(1+v) + y_{n-2}(1-v)) \\ &= (x_{n-1}(1+v) + y_{n-1}(v-1), x_0(1+v) + y_0(1-v), \cdots, x_{n-2}(1+v) + y_{n-2}(1-v)) \\ &= (x_{n-1}, x_0, x_1, \cdots, x_{n-2})(1+v) + (-y_{n-1}, y_0, y_1, \cdots, y_{n-2})(1-v) \\ &= (1+v)\sigma(x) + (1-v)\gamma(y) \in H.\end{aligned}$$

This proves that H is a v-constacyclic code over R_3.

Conversely, for any $x = (x_0, x_1, \cdots, x_{n-1}) \in H^+, y = (y_0, y_1, \cdots, y_{n-1}) \in H^-$. Let $h_i = x_i(v+1) + y_i(1-v), 0 \leq i \leq n-1$. Then $h = (h_0, h_1, \cdots, h_{n-1}) \in H$. Suppose that H is a v-constacyclic code over R_3, then $\tau(h) = (v+1)\sigma(x) + (1-v)\gamma(y) \in H$, thus $\sigma(x) \in H^+$ and $\gamma(y) \in H^-$. Therefore, H^+, H^- are cyclic and negacyclic codes over F_3, respectively.

Theorem 5.2 If $H = (1+v)H^+ \oplus (1-v)H^-$ is a v-constacyclic code of length n over R_3, then $H = \langle (1+v)g_1(x), (1-v)g_2(x) \rangle$ and $|H| = 3^{2n-\deg(g_1(x))-\deg(g_2(x))}$, where $g_1(x)$ and $g_2(x)$ are the monic generator polynomials of H^+ and H^-, respectively.

Proof By Theorem 5.1, we have

$$H^+ = \langle g_1(x) \rangle \subset \frac{F_3[x]}{\langle x^n - 1 \rangle}, H^- = \langle g_2(x) \rangle \subset \frac{F_3[x]}{\langle x^n + 1 \rangle}$$

and

$$H = \{h(x) | h(x) = (1+v)f_1(x) + (1-v)f_2(x), f_1(x) \in H^+, f_2(x) \in H^-\}.$$

Therefore,

$$H \subset \langle (1+v)g_1(x), (1-v)g_2(x) \rangle \subseteq \frac{R_3[x]}{\langle x^n - v \rangle}.$$

For any

$$(1+v)g_1(x)h_1(x) + (1-v)g_2(x)h_2(x) \in \langle (1+v)g_1(x), (1-v)g_2(x) \rangle \subseteq \frac{R_3[x]}{\langle x^n - v \rangle},$$

where $h_1(x), h_2(x) \in \frac{R_3[x]}{\langle x^n - v \rangle}$, there are $m_1(x), m_2(x) \in F_3[x]$ such that

$$(1+v)h_1(x) = (1+v)m_1(x)$$

and $(1-v)h_2(x) = (1-v)m_2(x)$. So $\langle (1+v)g_1(x), (1-v)g_2(x) \rangle \subseteq H$. This implies that $H = \langle (1+v)g_1(x), (1-v)g_2(x) \rangle$. Since $|H| = |H^+| \cdot |H^-|$, then $|H| = 3^{2n-\deg(g_1(x))-\deg(g_2(x))}$.

Theorem 5.3 With the notations as in Theorem 5.2. If $H = \langle (1+v)g_1(x), (1-v)g_2(x) \rangle$, then there is a unique polynomial $g(x)$ such that $H = \langle g(x) \rangle$ and $g(x) | x^n - v$, where

$$g(x) = (1+v)g_1(x) + (1-v)g_2(x).$$

Proof Since $g(x) = (1+v)g_1(x) + (1-v)g_2(x)$, $\langle g(x)\rangle \subset H$. Note that

$$-(1+v)g(x) = (1+v)g_1(x)$$

and $-(1-v)g(x) = (1-v)g_2(x)$, so $H \subset \langle g(x)\rangle$. Hence $H = \langle g(x)\rangle$. Since $g_1(x)|x^n - 1$ and $g_2(x)|x^n + 1$, there are $r_1(x), r_2(x) \in F_3[x]$ such that $x^n - 1 = g_1(x)r_1(x)$ and

$$x^n + 1 = g_2(x)r_2(x).$$

It follows that

$$x^n - v = g(x)[2(v+1)(x^n - 1) + 2(1-v)(x^n + 1)].$$

Hence, $g(x)|x^n - v$. Then uniqueness of $g(x)$ can be followed from that of $g_1(x)$ and $g_2(x)$.

Corollary 5.4 Every ideal of $\frac{R_3[x]}{\langle x^n - v\rangle}$ is principal.

Now, we consider the dual codes of v-constacyclic codes of length n over R_3 and we have the following results.

Theorem 5.5 If H is a v-constacyclic code of length n over R_3, then its dual code $H^\perp$ is also a v-constacyclic code over R_3.

Proof The proof is trivial since $v = v^{-1}$ and the dual of a v-constacyclic code is a v^{-1}-constacyclic.

By Theorem 5.5 and Corollary 3.4, it is easy to see that the above results of v-constacyclic codes can be carried over respectively to their dual codes. We list them here for the sake of completeness.

Corollary 5.6 Let $H = \langle (1+v)g_1(x), (1-v)g_2(x)\rangle$ be a v-constacyclic code of length n over R_3, $g_1(x)$ and $g_2(x)$ be the monic generator polynomials of H^+ and H^-, respectively, and $x^n - 1 = g_1(x)p_1(x)$ and $x^n + 1 = g_2(x)p_2(x)$. Then

(1) $H^\perp = \langle (1+v)p_1^*(x), (1-v)p_2^*(x)\rangle$ and $|H^\perp| = 2^{\deg g_1(x) + \deg g_2(x)}$;

(2) $H^\perp = \langle p(x)\rangle$, where $p(x) = (1+v)p_1^*(x) + (1-v)p_2^*(x)$ and $p(x)|x^n - v$, where $p_1^*(x)$ and $p_2^*(x)$ are the reciprocal polynomial of $p_1(x)$ and $p_2(x)$, respectively.

6 Examples

Now, we give the following two examples to illustrate the above results.

Example 6.1 Consider all cyclic codes over R_3 of length 2. Since $x^2 - 1 = (x-1)(x+1)$ in $F_3[x]$, there are 15 nonzero cyclic codes over R_3 of length 2. Table 1 gives the list of all cyclic codes. The ones marked with * denote the optimal ones.

Example 6.2 Consider all v-constacyclic codes over R_3 of length 4. Since

$$x^4 - 1 = (x-1)(x+1)(x^2+1)$$

and $x^4 + 1 = (x^2 + x - 1)(x^2 - x - 1)$ in $F_3[x]$, there are 31 nonzero v-constacyclic codes over R_3 of length 4. Table 2 gives the list of all v-constacyclic codes. The ones marked with * denote the optimal ones.

Table 1 All cyclic codes over R_3 of length 2 and ternary images

code	generator matrices	order	generators	d_L	Gray images
H_1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	3^4	2	1	$[4,4,1]^*$
H_2	$\begin{pmatrix} 2 & 2 \\ 0 & 1+v \end{pmatrix}$	3^2	$2+(1-v)x$	1	[4,3,1]
H_3	$\begin{pmatrix} -1 & 1 \\ 0 & 1+v \end{pmatrix}$	3^3	$2+(v-1)x$	1	[4,3,1]
H_4	$\begin{pmatrix} 1+v & 0 \\ 0 & 1+v \end{pmatrix}$	3^2	$1+v$	1	[4,2,1]
H_5	$\begin{pmatrix} 1 & 1 \\ 0 & v \end{pmatrix}$	3^3	$2+(1+v)x$	1	[4,3,1]
H_6	$\begin{pmatrix} 2 & 0 \\ 0 & 2+v \end{pmatrix}$	3^2	$(1+v)+2x$	2	$[4,2,2]^*$
H_7	$\begin{pmatrix} 2 & 2 \end{pmatrix}$	3^2	$2+2x$	2	$[4,2,2]^*$
H_8	$\begin{pmatrix} 1+v & 1+v \end{pmatrix}$	3^2	$(1+v)+(1+v)x$	2	$[4,3,2]^*$
H_9	$\begin{pmatrix} 1 & -1 \\ 0 & v \end{pmatrix}$	3^3	$v+(1+v)x$	1	[4,3,1]
H_{10}	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$	3^2	$v+2x$	2	$[4,2,2]^*$
H_{11}	$\begin{pmatrix} 1 & -1 \end{pmatrix}$	3^2	$1+2x$	2	$[4,2,2]^*$
H_{12}	$\begin{pmatrix} -(1+v) & 1+v \end{pmatrix}$	3^3	$-(1+v)+(1+v)x$	2	$[4,3,2]^*$
H_{13}	$\begin{pmatrix} 1-v & 0 \\ 0 & 1-v \end{pmatrix}$	3^2	$1-v$	1	[4,2,1]
H_{14}	$\begin{pmatrix} 1-v & 1-v \end{pmatrix}$	3	$(1-v)+(1-v)x$	2	[4,1,2]
H_{15}	$\begin{pmatrix} 1-v & -(1-v) \end{pmatrix}$	3	2	2	[4,1,2]

Table 2 All v-constacyclic codes over R_3 of length 4 and ternary images

code	generator polynomials	Gray images
H_1	2	$[8,8,1]^*$
H_2	$(1+v)+(1-v)(x^2+x+1)$	[8,6,1]
H_3	$(1+v)+(1-v)(x^2-x-1)$	[8,6,1]
H_4	$1+v$	[8,4,1]
H_5	$(1+v)(x-1)+(1-v)$	[8,7,1]
H_6	$(1+v)(x-1)+(1-v)(x^2+x+1)$	$[8,5,2]^*$
H_7	$(1+v)(x-1)+(1-v)(x^2-x-1)$	$[8,5,2]^*$
H_8	$(1+v)(x-1)$	[8,3,2]
H_9	$(1+v)(x+1)+(1-v)$	[8,7,1]
H_{10}	$(1+v)(x+1)+(1-v)(x^2+x-1)$	$[8,5,2]^*$
H_{11}	$(1+v)(x+1)+(1-v)(x^2-x-1)$	$[8,5,2]^*$
H_{12}	$(1+v)(x+1)$	[8,3,2]
H_{13}	$(1+v)(x^2+1)+(1-v)$	[8,6,1]
H_{14}	$(1+v)(x^2+1)+(1-v)(x^2+x+1)$	[8,4,2]
H_{15}	$(1+v)(x^2+1)+(1-v)(x^2-x-1)$	[8,4,2]
H_{16}	$(1+v)(x^2+1)$	[8,2,2]
H_{17}	$(1+v)(x^2-1)+(1-v)$	[8,6,1]
H_{18}	$(1+v)(x^2-1)+(1-v)(x^2+x-1)$	[8,4,2]
H_{19}	$(1+v)(x^2+1)+(1-v)(x^2-x-1)$	[8,4,2]
H_{20}	$(1+v)(x^2+1)$	[8,2,2]
H_{21}	$(1+v)(x-1)(x^2+1)+(1-v)$	[8,5,1]
H_{22}	$(1+v)(x-1)(x^2+1)+(1-v)(x^2+x-1)$	[8,2,3]
H_{23}	$(1+v)(x-1)(x^2+1)+(1-v)(x^2-x-1)$	[8,2,3]
H_{24}	$(1+v)(x-1)(x^2+1)$	[8,1,4]
H_{25}	$(1+v)(x+1)(x^2+1)+(1-v)$	[8,5,1]
H_{26}	$(1+v)(x+1)(x^2+1)+(1-v)(x^2+x-1)$	[8,3,3]
H_{27}	$(1+v)(x+1)(x^2+1)+(1-v)(x^2-x-1)$	[8,3,3]
H_{28}	$(1+v)(x+1)(x^2+1)$	[8,1,4]
H_{29}	$1-v$	[8,3,1]
H_{30}	$(1-v)(x^2+x-1)$	[8,2,3]
H_{31}	$(1-v)(x^2-x-1)$	[8,2,3]

7 Conclusion

In this paper, we studied cyclic and v-constacyclic codes over R_3 with an arbitrary length. The dual of the cyclic and v-constacyclic of codes are studied as well. An example of the cyclic and constacyclic codes over R_3 with fixed length is given, respectively. With two

examples in hand, we can urge the researchers to search for new ternary codes with good paraments as images of two families of codes. Another two important families for study would be the families of cyclic and constacyclic codes over $F_p + vF_p$ where p is a prime number and $p > 3$.

References

[1] Bachoc C. Application of coding Theory to the construction of modular lattices[J]. J. Combin. Theory, Ser. A, 1998, 78: 92–119.

[2] Chapan R, Dougherty S T, Gabort P, Sole P. Self-dual codesover $F_3 + vF_3$[J]. http://academic.scranton.edu/faculty/doughertys1/sd.htm.

[3] Hammons A R, Kumar Jr P V, Calderbank A R, Sloane N J A, Sole P. The Z_4 linearity of Kerdock, Preparata, Gethals and related codes[J]. IEEE Trans. Inform. Theory, 1994, 40: 301–319.

[4] Bonnecaze A, Udayu P. Cyclic codes and self-dual codes over$F_2 + uF_2$[J]. IEEE Trans. Inform. Theory, 1999, 45: 1250–1255.

[5] Udayu P, Bonnecaze A. Decoding of cyclic codes over $F_2 + uF_2$[J]. IEEE Trans. Inform. Theory, 1999, 45: 2148–2157.

[6] Abualrub T, Siap I. Constacyclic codes over $F_2 + uF_2$[J]. J. Frank. Inst., 2009, 346: 520–529.

[7] Qian J F, Zhang L, Zhu S X. $(1 + u)-$constacyclic and cyclic code over $F_2 + uF_2$[J]. Applied Mathematics Letters, 2006, 19: 820–823.

[8] Abualrub T, Siap I. Cyclic codes over the ring $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$[J]. Des. Codes Crypt., 2007, 42: 273–287.

[9] Yildiz B, Karadeniz S. Linear codes over $F_2 + uF_2 + vF_2 + uvF_2$[J]. Des. Codes Crypt., 2010, 54: 61–81.

[10] Karadeniz S, Yildiz B. $(1 + v)-$constacyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$[J]. Journal of the Franklin Institute, 2011, 348(9): 2625–2632.

[11] Liu X S. MDR codes and self-dual codes on Cartesian product codes[J]. Journal on Communications, 2010, 31(3): 123–125.

[12] Wood J. Duality for modules over finite rings and applications to coding theory[J]. Amer. J. Math., 1999, 121: 555–575.

环$F_3 + vF_3$上的循环码与常循环码

刘修生[1], 许小芳[1], 黄振华[2]

(1. 湖北理工学院数理学院, 湖北 黄石 435003)

(2. 湖北师范学院数学与统计学院, 湖北 黄石 435002)

摘要: 本文研究了环$F_3 + vF_3$上的循环码与常循环码. 通过环$F_3 + vF_3$与域F_3上的循环码之间关系, 证明了环$F_3 + vF_3$上循环码是由一个多项式生成的. 最后, 用类似的方法, 得到了环$F_3 + vF_3$上v -常循环码也是由一个多项式生成的.

关键词: 循环码; 常循环码; Gray 映射; 生成多项式

MR(2010)**主题分类号**: 94B05; 94B99 **中图分类号**: O157.4