Vol. 37 (2017)
No. 5

数 学 杂 志
J. of Math. (PRC)

ON COMPLEMENTARY-DUAL CONSTACYCLIC CODES OVER $F_p + vF_p$

LIU Xiu-sheng

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

Abstract: In this paper, we investigate the complementary-dual $(1-2v)$-constacyclic codes over the ring $\mathbb{F}_p+v\mathbb{F}_p(v^2=v)$, where p is a prime. Using the decomposition $C = vC_{1-v} \oplus (1-v)C_v$ of a $(1-2v)$-constacyclic code over F_p+vF_p, we obtain generator polynomial of the complementary-dual $(1-2v)$-constacyclic code C. Then by means of the Gray map from $\mathbb{F}_p+v\mathbb{F}_p$ to $\mathbb{F}_p^2$, we show that Gray images of complementary-dual $(1-2v)$-constacyclic codes over $\mathbb{F}_p+v\mathbb{F}_p$ are complementary-dual cyclic codes over $\mathbb{F}_p$.

Keywords: complementary-dual $(1-2v)$-constacyclic codes; cyclic codes; negacyclic codes; constacyclic codes; generator polynomials

2010 MR Subject Classification: 94B05; 94B15; 11T71

Document code: A **Article ID:** 0255-7797(2017)05-0916-09

1 Introduction

A linear code with a complementary-dual (an LCD code) was defined in [3] to be a linear code C whose dual code $C^\perp$ satisfies $C \cap C^\perp = \{0\}$. It was shown in [3] that asymptotically good LCD codes exist and those LCD codes have certain other attractive properties. Yang and Massy showed that the necessary and sufficient condition for a cyclic code of length n to be an LCD code is that the generator polynomial $g(x)$ is self-reciprocal and all the monic irreducible factors of $g(x)$ have the same multiplicity in $g(x)$ and in x^n-1 (see [4]). In [9], Sendrier indicated that linear code with complementary-duals meet the asymptotic Gilbert-Varshamov bound. Emaeili and Yari discussed in [8] the complementary-dual QC codes, and provided a sufficient condition for an ρ-generator QC code C to be an LCD code, and a necessary and sufficient condition under which a given maximal 1-generator index-2 QC code C is LCD.

In recent years, Dinh established the algebrac structure in terms of polynomial generators of all repeated-root constacyclic codes of length $3p^s, 4p^s, 6p^s$ over F_{p^m}. Using these structures, LCD codes were identified among them (see [5–7]).

* **Received date:** 2016-04-07 **Accepted date:** 2016-09-05

Foundation item: Supported by Scientific Research Foundation of Hubei Provincial Education Department of China (D20144401) 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.

The purpose of this paper is to give the algebraic structure in terms of generator polynomials of all complementary-dual $(1-2v)$-constacyclic codes of length n over $F_p + vF_p$. The necessary background materials on constacyclic codes and a Gray map are given in Section 2. In Section 3, we give the generator polynomials of the complementary-dual cyclic and negacyclic codes of length $n = p^t m$ over F_p, and show an enumeration formula for the complementary-dual cyclic and negacyclic codes of length n over F_p. In Section 4, Theorem 4.5 provides a necessary and sufficient condition under which a given $(1-2v)$-constacyclic code C of length n over $F_p + vF_p$ is an LCD. The generator polynomials and enumeration of $(1-2v)$-constacyclic codes length n over $F_p + vF_p$ are given by Theorem 4.7 under which C is an LCD code of length n over $F_p + vF_p$.

2 Preliminaries

Throughout this paper, p is an odd prime, F_p is a finite field with p elements. Let R be the commutative ring $F_p + vF_p = \{a + vb | a, b \in F_p\}$ with $v^2 = v$. The ring R is a semi-local ring, it has two maximal ideals $\langle v \rangle = \{av | a \in F_p\}$ and $\langle 1-v \rangle = \{b(1-v) | b \in F_p\}$. It is easy to see that both $\frac{R}{\langle v \rangle}$ and $\frac{R}{\langle 1-v \rangle}$ are isomorphic to F_p. From Chinese remainder theorem, we have $R = \langle v \rangle \oplus \langle 1-v \rangle$. We denote $1-2v$ by μ for simplicity. The following notations for codes over R are also valid for codes over F_p. A code of length n over R is a nonempty subset of R^n, and a code is linear over R if it is an R-submodule of R^n . Let $x = (x_0, x_1, \cdots, x_{n-1})$ and $y = (y_0, y_1, \cdots, y_{n-1})$ be any two elements of R^n, we define an inner product over R by $x \cdot y = x_0 y_0 + \cdots + x_{n-1} y_{n-1}$. If $x \cdot y = 0$, we say x and y are orthogonal.

The dual code $C^\perp$ of C is defined by $C^\perp = \{x \in R^n | x \cdot y = 0 \text{ for all } y \in C\}$. It is easy to verify that $C^\perp$ is always a linear code over R for any code C code over R.

Let C be a code of length n over R (or F_p) and $P(C)$ be its polynomial representation, i.e.,

$$P(C) = \{\sum_{i=0}^{n-1} c_i x^i | (c_0, c_1, \cdots, c_{n-1}) \in C\}.$$

Let σ and γ be maps from R^n(or F_p^n) to R^n (or F_p^n) given by $\sigma(c_0, c_1, \cdots c_{n-1}) = (c_{n-1}, c_0, \cdots, c_{n-2})$, and $\gamma(c_0, c_1, \cdots c_{n-1}) = (-c_{n-1}, c_0, \cdots, c_{n-2})$, respectively. Then a code C is said to be cyclic if $\sigma(C) = C$, negacyclic if $\gamma(C) = C$.

Let τ be map from R^n to R^n given by $\tau(c_0, c_1, \cdots c_{n-1}) = (\mu c_{n-1}, c_0, \cdots, c_{n-2})$. Then code C is said to be μ-constacyclic if $\tau(C) = C$.

It is well known that a code C of length n over R (or F_p) is cyclic if and only if $P(C)$ is an ideal of $\frac{R[x]}{\langle x^n - 1 \rangle}$ (or$\frac{F_p[x]}{\langle x^n - 1 \rangle}$), a code C of length n over R (or F_p) is negacyclic if and only if $P(C)$ is an ideal of $\frac{R[x]}{\langle x^n + 1 \rangle}$ (or$\frac{F_p[x]}{\langle x^n + 1 \rangle}$), a code C of length n over R is $\mu-$constacyclic if and only if $P(C)$ is an ideal of $\frac{R[x]}{\langle x^n - \mu \rangle}$.

Now we give the definition of the Gray map on R^n. Observe that any element $c \in R$ can be expressed as $c = a + vb$, where $a, b \in F_p$. The Gray map $\Phi : R \to F_p^2$ is given by

$\Phi(c) = (-b, 2a + b)$. This map can be extended to R^n in a natrual way:

$$\begin{aligned} \Phi : R^n &\rightarrow F_p^{2n}, \\ (c_0, c_1, \cdots, c_{n-1}) &\mapsto (-b_0, -b_1, \cdots, -b_{n-1}, 2a_0 + b_0, 2a_1 + b_1, \cdots, 2a_{n-1} + b_{n-1}), \end{aligned}$$

where $c_i = a_i + vb_i, 0 \leq i \leq n-1$.

A code C is a complementary-dual cyclic (or negacyclic) code of length n over R (or F_p) if it is a cyclic (or negacyclic) and LCD code of length n over R (or F_p), and a code C is a complementary-dual μ-constacyclic code of length n over R if it is a μ-constacyclic and LCD code of length n over R .

3 Generator Polynomials of the Complementary-Dual Cyclic Codes over F_p

We begin with two concepts.

Given a ring $\widetilde{R}$, for a nonempty subset S of $\widetilde{R}$, the annihilator of S, denoted by ann(S), is the set $\text{ann}(S) = \{f | fg = 0 \text{ for all } g \in S\}$. If, in addition, S is an ideal of $\widetilde{R}$, then ann(S) is also an ideal of $\widetilde{R}$.

For any polynomial $f(x) = \sum\limits_{i=0}^{k} a_i x^i$ of degree k ($a_k \neq 0$) over F_p, let $f^*(x)$ denote the reciprocal polynomial of $f(x)$ given by $f^*(x) = x^k f(\frac{1}{x}) = \sum\limits_{i=0}^{k} a_{k-i} x^i$. Note that $(f^*)^* = f$ if and only if the constant term of f is nonzero, if and only if deg(f)=deg(f^*). Furthermore, by definition, it is easy to see that $(fg)^* = f^* g^*$. We denote $A^* = \{f^*(x) | f(x) \in A\}$. It is easy to see that if A is an ideal, then A^* is also an ideal. Hereafter, we will use $\text{ann}^*(C)$ to denote $(\text{ann}(C))^*$. The following proposition can be found in [2, 10].

Proposition 3.1 If C is a cyclic (or negacyclic) code of length n over F_p, then the dual $C^\perp$ of C is $\text{ann}^*(C)$.

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 $\widetilde{f}(x) = c^{-1} f^*(x)$. We recall a result about LCD codes which can be found in [5].

Proposition 3.2 If $g_1(x)$ is the generator polynomial of a cyclic code C of length n over F_p, then C is an LCD code if and only if $g_1(x)$ is self-reciprocal (i.e., $\widetilde{g}_1(x) = g_1(x)$) and all the monic irreducible factors of $g_1(x)$ have the same multiplicity in $g_1(x)$ and in $x^n - 1$.

Similar to the discussions in [5], we have the following proposition.

Proposition 3.3 If $g_2(x)$ is the generator polynomial of a negacyclic code C of length n over F_p, then C is an LCD code if and only if $g_2(x)$ is self-reciprocal (i.e., $\widetilde{g}_2(x) = g_2(x)$) and all the monic irreducible factors of $g_2(x)$ have the same multiplicity in $g_2(x)$ and in $x^n + 1$.

We first investigate the generator polynomials of the complementary-dual cyclic codes over F_p.

It is well known that each cyclic code over F_p is uniquely determined by its generator polynomial, a monic divisor of $x^n - 1$ over F_p. In order to describe the generator polynomials

of the complementary-dual cyclic codes, we need to know the factorization of the polynomial $x^n - 1$ over F_p. Write $n = p^t m$, where t is a nonnegative integer depending on n and $\gcd(m, p) = 1$. Then $x^n - 1 = (x^m - 1)^{p^t}$.

For any irreducible polynomial dividing $x^m - 1$ over F_p, its reciprocal polynomial also divides $x^m - 1$ over F_p and is also irreducible over F_p. Since $\gcd(m, p) = 1$, the polynomial $x^m - 1$ factors completely into irreducible factors in $F_p[x]$ as

$$x^m - 1 = \delta f_1(x) f_2(x) \cdots f_k(x) h_1(x) h_1^*(x) \cdots h_s(x) h_s^*(x),$$

where $\delta \neq 0$ in F_p, $f_1(x), f_2(x), \cdots, f_k(x)$ are irreducible polynomials that are associates to their own reciprocals, and $h_1(x), h_1^*(x); \cdots; h_s(x), h_s^*(x)$ are pairs of mutually reciprocal irreducible polynomials. Therefore

$$x^n - 1 = \delta^{p^t} (f_1(x))^{p^t} (f_2(x))^{p^t} \cdots (f_k(x))^{p^t} (h_1(x))^{p^t} (h_1^*(x))^{p^t} \cdots (h_s(x))^{p^t} (h_s^*(x))^{p^t}. \quad (3.1)$$

We can describe the generator polynomials of the complementary-dual cyclic codes as soon as we know the factorization of $x^n - 1$ over F_p.

Theorem 3.4 Let $x^n - 1$ be factorized as in (3.1). A cyclic code C of length n over F_p is an LCD code if and only if its generator polynomial is of the form

$$(f_1(x))^{\alpha_1} (f_2(x))^{\alpha_2} \cdots (f_k(x))^{\alpha_k} (h_1(x))^{\beta_1} (h_1^*(x))^{\beta_1} \cdots (h_s(x))^{\beta_s} (h_s^*(x))^{\beta_s}, \quad (3.2)$$

where $\alpha_i \in \{0, p^t\}$ for each $1 \leq i \leq k$, and $\beta_j \in \{0, p^t\}$ for each $1 \leq j \leq s$.

Proof Let C be a cyclic code of length n over F_p, and let $g(x)$ be its generator polynomial. We need to show that C is an LCD code if and only if $g(x)$ is of the form as in (3.2).

Suppose that

$$g(x) = \varepsilon (f_1(x))^{\alpha_1} (f_2(x))^{\alpha_2} \cdots (f_k(x))^{\alpha_k} (h_1(x))^{\beta_1} (h_1^*(x))^{\gamma_1} \cdots (h_s(x))^{\beta_s} (h_s^*(x))^{\gamma_s}$$

with leading coefficient 1, where $0 \leq \alpha_i \leq p^t$ for each $1 \leq i \leq k$, and $0 \leq \beta_j, \gamma_j \leq p^t$ for each $1 \leq j \leq s$. Then

$$g^*(x) = \eta (f_1(x))^{\alpha_1} (f_2(x))^{\alpha_2} \cdots (f_k(x))^{\alpha_k} (h_1(x))^{\gamma_1} (h_1^*(x))^{\beta_1} \cdots (h_s(x))^{\gamma_s} (h_s^*(x))^{\beta_s}.$$

Therefore

$$\widetilde{g}(x) = \frac{1}{g(0)} g^*(x) = \varepsilon (f_1(x))^{\alpha_1} (f_2(x))^{\alpha_2} \cdots (f_k(x))^{\alpha_k} (h_1(x))^{\gamma_1} (h_1^*(x))^{\beta_1} \cdots (h_s(x))^{\gamma_s} (h_s^*(x))^{\beta_s}.$$

By Proposition 3.2, C is an LCD code if and only if $g(x) = \widetilde{g}(x)$ and all the monic irreducible factors of $g(x)$ have the same multiplicity in $g(x)$ and in $x^n - 1$, i.e., $\beta_j = \gamma_j$ for each $1 \leq j \leq s$, $\alpha_i \in \{0, p^t\}$ for each $1 \leq i \leq k$, and $\beta_j \in \{0, p^t\}$ for each $1 \leq j \leq s$.

Therefore, C is an LCD code if and only if its generator polynomial $g(x)$ is of the form as in (3.2).

Obviously, $C = \{0\}$ and $C = F_p^n$ are complementary-dual cyclic codes, which are called the trivial LCD codes over F_p.

The following corollary is obvious.

Corollary 3.5 Let $x^n - 1$ be factorized as in (3.1). Then the number of nontrivial complementary-dual cyclic codes is exactly $2^{k+s} - 2$.

Now we discuss the complementary-dual negacyclic codes.

Since $n = p^t m$, $gcd(m, p) = 1$, we have $x^n + 1 = (x^m + 1)^{p^t}$. For any irreducible polynomial dividing $x^m + 1$ over F_p, its reciprocal polynomial also divides $x^m + 1$ over F_p and is also irreducible over F_p. Since $\gcd(m, p) = 1$, the polynomial x^m+1 factors completely into irreducible factors in $F_p[x]$ as

$$x^m + 1 = \zeta \overline{f}_1(x)\overline{f}_2(x) \cdots \overline{f}_{\overline{k}}(x)\overline{h}_1(x)\overline{h}_1^*(x) \cdots \overline{h}_{\overline{s}}(x)\overline{h}_{\overline{s}}^*(x),$$

where $\zeta \neq 0$ in F_p, $\overline{f}_1(x), \overline{f}_2(x), \cdots, \overline{f}_{\overline{k}}(x)$ are irreducible polynomials that are associates to their own reciprocals, and $\overline{h}_1(x), \overline{h}_1^*(x); \cdots; \overline{h}_{\overline{s}}(x), \overline{h}_{\overline{s}}^*(x)$ are pairs of mutually reciprocal irreducible polynomials. Therefore

$$x^n + 1 = \zeta^{p^t}(\overline{f}_1(x))^{p^t}(\overline{f}_2(x))^{p^t} \cdots (\overline{f}_{\overline{k}}(x))^{p^t}(\overline{h}_1(x))^{p^t}(\overline{h}_1^*(x))^{p^t} \cdots (\overline{h}_{\overline{s}}(x))^{p^t}(\overline{h}_{\overline{s}}^*(x))^{p^t}. \quad (3.3)$$

In light of Proposition 3.3 and (3.3), the following theorem is easy to vertify.

Theorem 3.6 Let $x^n + 1$ be factorized as in (3.3). A negacyclic code C of length n is LCD code if and only if its generator polynomial is of the form

$$(\overline{f}_1(x))^{\overline{\alpha}_1}(\overline{f}_2(x))^{\overline{\alpha}_2} \cdots (\overline{f}_{\overline{k}}(x))^{\overline{\alpha}_{\overline{k}}}(\overline{h}_1(x))^{\overline{\beta}_1}(\overline{h}_1^*(x))^{\overline{\beta}_1} \cdots (\overline{h}_s(x))^{\overline{\beta}_{\overline{s}}}(\overline{h}_{\overline{s}}^*(x))^{\overline{\beta}_{\overline{s}}}, \quad (3.4)$$

where $\overline{\alpha}_i \in \{0, p^t\}$ for each $1 \leq i \leq \overline{k}$, and $\overline{\beta}_j \in \{0, p^t\}$ for each $1 \leq j \leq \overline{s}$.

Obviously, $C = 0$ and $C = F_p^n$ are complementary-dual negacyclic codes, which are called the trivial complementary-dual negacyclic codes over F_p. The following corollary is easy to obtain.

Corollary 3.7 Let $x^n + 1$ be factorized as in (3.3). Then the number of nontrivial complementary-dual cyclic codes is exactly $2^{\overline{k}+\overline{s}} - 2$.

4 Generator Polynomials of Complementary-Dual μ-Constacyclic Codes over R

Let C_1, C_2 be codes over R. We denote $C_1 \oplus C_2 = \{a + b | a \in C_1, b \in C_2\}$. For a code C over R, let us take

$$C_{1-v} = \{a \in F_p^n | \text{ there exists } b \in F_p^n \text{ such that } va + (1 - v)b \in C\}$$

and

$$C_v = \{b \in F_p^n | \text{ there exists } a \in F_p^n \text{ such that } va + (1 - v)b \in C\}.$$

It is easy to vertify that $| C |=| C_v || C_{1-v} |$, and $C = vC_{1-v} \oplus (1 - v)C_v$.

The following four lemmas can be found in [1].

Lemma 4.1 Let $C = vC_{1-v} \oplus (1-v)C_v$ be a linear code of length n over R. Then C is a μ-constacyclic code length n over R if and only if C_{1-v} and C_v are negacyclic and cyclic codes of length n over F_p, respectively.

Lemma 4.2 If $C = vC_{1-v} \oplus (1-v)C_v$ is a μ-constacyclic code of length n over R, then there is a unique polynomial $g(x) = vg_1(x) + (1-v)g_2(x)$ such that $C = \langle g(x)\rangle, g(x)|x^n - \mu$, and $\mid C \mid= p^{2n-\deg(g_1)-\deg(g_2)}$, where $g_1(x)$ and $g_2(x)$ are the generator polynomials of C_{1-v} and C_v over F_p, respectively.

Lemma 4.3 Let $C = vC_{1-v} \oplus (1-v)C_v$ be a μ-constacyclic code length n over R, and $C = \langle vg_1(x) + (1-v)g_2(x)\rangle$, where $g_1(x)$ and $g_2(x)$ are the generator polynomials of C_{1-v} and C_v over F_p, respectively. Then $\Phi(C) = \langle g_1(x)g_2(x)\rangle$, and $\Phi(C^\perp) = \Phi(C)^\perp$.

Lemma 4.4 Let $C = vC_{1-v} \oplus (1-v)C_v$ be a μ-constacyclic code length n over R. Then its dual code $C^\perp$ is also a μ-constacyclic code length n over R, and $C^\perp = vC_{1-v}^\perp \oplus (1-v)C_v^\perp$.

Theorem 4.5 Let $C = vC_{1-v} \oplus (1-v)C_v = \langle vg_1(x) + (1-v)g_2(x)\rangle$ be a μ-constacyclic code of length n over R. Then C is an LCD code of length n over R if and only if C_{1-v} and C_v are the complementary-dual negacyclic and cyclic codes of length n over F_p, respectively.

Proof By Lemma 4.4 , we know that $C \cap C^\perp = \{0\}$ if and only if $C_{1-v} \cap C_{1-v}^\perp = \{0\}$, and $C_v = \cap C_v^\perp = \{0\}$.

Form the above proof, the following corollary can be obtained at once.

Corollary 4.6 Let $C = vC_{1-v} \oplus (1-v)C_v$ be a μ-constacyclic code of length n over R. Then C is an LCD code of length n over R if and only if $\Phi(C)$ is a complementary-dual cyclic codes of length $2n$ over F_p.

Proof By Lemma 4.1 and Lemma 4.3, we have $C_{1-v} = \langle g_1(x)\rangle$, and $C_v = \langle g_2(x)\rangle$.

Since C_{1-v} is a complementary-dual negacyclic code, $g_1(x) = \widetilde{g}_1(x)$ and all the monic irreducible factors of $g_1(x)$ have the same multiplicity in $g_1(x)$ and in $x^n + 1$.

Similarly, $g_2(x) = \widetilde{g}_2(x)$ and all the monic irreducible factors of $g_2(x)$ have the same multiplicity in $g_2(x)$ and in $x^n - 1$.

In light of Lemma 4.2, $\Phi(C) = \langle g_1(x)g_2(x)\rangle$. Write $g(x) = g_1(x)g_2(x)$. Then

$$\widetilde{g}(x) = \frac{1}{g(0)}g^*(x) = \frac{1}{g_1(0)g_2(0)}g_1^*(x)g_2^*(x) = \widetilde{g}_1(x)\widetilde{g}_2(x) = g_1(x)g_2(x) = g(x),$$

which implies that $\widetilde{g}(x)$ is self-reciprocal.

Let $x^n + 1 = g_1(x)h_1(x)$, and $x^n - 1 = g_2(x)h_2(x)$. Then

$$x^{2n} - 1 = g_1(x)g_2(x)h_1(x)h_2(x) = g(x)h_1(x)h_2(x).$$

Therefore all the monic irreducible factors of $g(x)$ have same multiplicity in $g(x)$ have the same multiplicity in $g(x)$ in $x^{2n} - 1$.

We summarize the above fact to conclude that $\Phi(C)$ is a complementary-dual cyclic code of length $2n$ over F_p.

Conversely, if $\alpha \in C \cap C^\perp$, i.e., $\alpha \in C$, and $\alpha \in C^\perp$, then $\Phi(\alpha) \in \Phi(C)$, and $\Phi(\alpha) \in \Phi(C^\perp) = \Phi(C)^\perp$. Therefore $\Phi(\alpha) \in \Phi(C) \cap \Phi(C)^\perp = \{0\}$, i.e., $\Phi(\alpha) = 0$. It is implies that

$\alpha = 0$ since Φ is bijective from R^n to F_p^{2n}. Hence $C \cap C^{\perp} = \{0\}$, i.e., C is a complementary-dual cyclic code of length n over R.

By Theorem 3.5, Theorem 3.7, Corollary 3.6 and Corollary 3.8, we get the following statements.

Theorem 4.7 Let $C = vC_{1-v} \oplus (1-v)C_v$ be a μ-constacyclic code of length n over R, $x^n - 1$ and $x^n + 1$ be factorized as in (3.2) and (3.3), respectively. Then

(1) C is an LCD code of length n over R if and only if its generator polynomial is of the form

$$v\prod_{l=1}^{\overline{k}}(\overline{f}_l(x))^{\overline{\alpha}_l}\prod_{q=1}^{\overline{s}}(\overline{h}_q(x))^{\overline{\beta}_q}(\overline{h}_q^*(x))^{\overline{\beta}_q} + (1-v)\prod_{i=1}^{k}(f_i(x))^{\alpha_i}\prod_{j=1}^{s}(h_j(x))^{\beta_j}(h_j^*(x))^{\beta_j},$$

where $f_i(x), \overline{f}_l(x), h_j(x), h_j^*(x), \overline{h}_q(x), \overline{h}_q^*(x) \in F_p[x]$, and $\alpha_i, \overline{\alpha}_l, \beta_j, \overline{\beta}_q \in \{0, p^t\}$.

(2) $\Phi(C)$ is an LCD code of length $2n$ over F_p if and only if its generator polynomial is of the form

$$\prod_{i=1}^{k}(f_i(x))^{\alpha_i}\prod_{l=1}^{\overline{k}}(\overline{f}_l(x))^{\overline{\alpha}_l}\prod_{j=1}^{s}(h_j(x))^{\beta_j}(h_j^*(x))^{\beta_j}\prod_{q=1}^{\overline{s}}(\overline{h}_q(x))^{\overline{\beta}_q}(\overline{h}_q^*(x))^{\overline{\beta}_q},$$

where $f_i(x), \overline{f}_l(x), h_j(x), h_j^*(x), \overline{h}_q(x), \overline{h}_q^*(x) \in F_p[x]$, and $\alpha_i, \overline{\alpha}_l, \beta_j, \overline{\beta}_q \in \{0, p^t\}$.

(3) The number of nontrivial complementary-dual μ-constacyclic codes of length n over R is exactly $2^{k+s+\overline{k}+\overline{s}} - 2$.

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

Example 1 In $F_5[x]$,

$$\begin{aligned} x^6 - 1 &= (x-1)(x+1)(x^2+x+1)(x^2+4x+1), \\ x^6 + 1 &= -3(x+2)(1+2x)(x^2+2x-1)(1+2x-x^2). \end{aligned}$$

Observe that the polynomials $x-1, x+1, x^2+x+1$, and x^2+4x+1 are irreducible polynomials that are associates to their own reciprocals, and $x+2, 1+2x; x^2+2x-1, 1+2x-x^2$ are two pairs of mutually reciprocal irreducible polynomials over F_5. There are 62 nontrivial complementary-dual μ-constacyclic codes of length 6 over $R = F_5 + vF_5$, i.e.,

$$\begin{aligned} C_{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6} \quad = \quad & \langle v(x+2)^{\alpha_1}(x-2)^{\alpha_1}(x^2+2x-1)^{\alpha_2}(1+2x-x^2)^{\alpha_2} \\ & +(1-v)(x-1)^{\alpha_3}(x+1)^{\alpha_4}(x^2+x+1)^{\alpha_5}(x^2+4x+1)^{\alpha_6}\rangle, \end{aligned}$$

where $\alpha_i \in \{0,1\}$ for $1 \le i \le 6$, and $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6) \neq (0,0,0,0,0,0), (1,1,1,1,1,1)$.

Now we list some optimal codes obtained from complementary-dual μ-constacyclic codes over $R = F_5 + vF_5$ in Table 1.

Example 2 In $F_7[x]$,

$$\begin{aligned} x^8 - 1 &= (x-1)(x+1)(x^2+1)(x^2-3x+1)(x^2+3x+1), \\ x^8 + 1 &= (x^2+x-1)(1+x-x^2)(x^2+3x-1)(1+3x-x^2). \end{aligned}$$

Table 1: Optimal codes of length 12 over $\mathbb{F}_5$
from complementary-dual μ-constacyclic codes over $R = F_5 + vF_5$

Generator of C	$\phi(C)$
$v-(v-1)(x^2+4x+1)$	[12,10,2]
$v-(v-1)(x+1)$	[12,11,2]
$v(x-2)(x+2)-(v-1)(x^2+4x+1)$	[12,8,4]
$v(x^2+2x-1)(2x-x^2+1)-(v-1)(x-1)(x^2+4x+1)$	[12,5,6]
$v(x-2)(x+2)(x^2+2x-1)(2x-x^2+1)-(v-1)(x+1)(x^2+x+1)$	[12,3,8]
$v(x-2)(x+2)(x^2+2x-1)(2x-x^2+1)-(v-1)(x+1)(x^2+4x+1)(x^2+x+1)$	[12,1,12]

Observe that the polynomials $x-1, x+1, x^2+1, x^2-3x+1$, and x^2+3x+1 are irreducible polynomials that are associates to their own reciprocals, and $x^2+x-1, 1+x-x^2; x^2+3x-1, 1+3x-x^2$ are two pairs of mutually reciprocal irreducible polynomials over F_7. There are 126 nontrivial complementary-dual μ-constacyclic codes of length 8 over $R = F_7 + vF_7$, i.e.,

$$\begin{aligned} C_{\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7} &= \langle v(x^2+x-1)^{\beta_1}(1+x-x^2)^{\beta_1}(x^2+3x-1)^{\beta_2}(1+3x-x^2)^{\beta_2} \\ &\quad +(1-v)(x-1)^{\beta_3}(x+1)^{\beta_4}(x^2+1)^{\beta_5}(x^2-3x+1)^{\beta_6}(x^2+3x+1)^{\beta_7}\rangle, \end{aligned}$$

where $\beta_j \in \{0,1\}$ for $1 \le j \le 7$, and

$$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7) \neq (0,0,0,0,0,0,0), (1,1,1,1,1,1,1).$$

Now we list some optimal linear codes obtained from complementary-dual μ-constacyclic codes over $R = F_7 + vF_7$ in Table 2.

Table 2: Optimal codes of length 16 over $\mathbb{F}_7$
from complementary-dual μ-constacyclic codes over $R = F_7 + vF_7$

Generator of C	$\phi(C)$
$v-(v-1)(x+1)$	[16,15,2]
$v-(v-1)(x^2+3x+1)$	[16,14,2]
$v(x^2+3x-1)(3x-x^2+1)-(v-1)(x+1)(x^2+3x+1)$	[16,9,6]
$v(x-x^2+1)(x^2+3x-1)(3x-x^2+1)(x^2+x-1)$ $-(x^2+1)(v-1)(x+1)(x^2+3x+1)$	[16,3,12]
$v(x-x^2+1)(x^2+3x-1)(3x-x^2+1)(x^2+x-1)$ $-(x^2+1)(v-1)(x+1)(x^2-3x+1)(x^2+3x+1)$	[16,1,16]

References

[1] Zhu S, Wang L. A class of constacyclic ocdes over $F_p + vF_p$ and its Gray image[J]. Disc. Math., 2011, 311: 677–2682.

[2] Bakshi G K, Raka M. Self-dual and self-orthogonal negacyclic codes of length $2p^s$ over a finite field[J]. Finite Field Appl., 2013, 19: 39–54.

[3] Massey J L. Linear codes with complementary duals[J]. Disc. Math., 1992, 106/107: 337–342.

[4] Yang X, Massey J L. The condition for a cyclic code to have a complementary dual[J]. Disc. Math., 1994, 126: 391–393.

[5] Dinh H Q. Structure of repeated-root constacyclic codes of length $3p^s$ and their duals[J]. Disc. Math., 2013, 313: 983–991.

[6] Dinh H Q. On repeated-root constacyclic codes of length $4p^s$[J]. Asian-European J. Math., 2010, 1: 1–25.

[7] Dinh H Q. Repeated-root cyclic codes of length $6p^s$[J]. MAS Contem. Math., 2014, 609: 69–87.

[8] Esmaeili M, Yari S. On complementary-dual quasi-cyclic codes[J]. Finite Field Appl., 2009, 15: 357–386.

[9] Sendrier N.Linear codes with complementary duals meet the Gilbert-Varshamov bound[J]. Discrete Math., 2004, 304: 345–347.

[10] Huffman W C, Pless V. Fundamentals of error-correcting codes[M]. Cambridge: Cambridge University Press, 2003.

环F_p+vF_p上互补对偶常循环码

刘修生

(湖北理工学院数理学院, 湖北 黄石 435003)

摘要: 本文研究了环F_p+vF_p上互补对偶 $(1-2v)$-常循环码. 利用环 F_p+vF_p上 $(1-2v)$-常循环码的分解式 $C=vC_{1-v}\oplus(1-v)C_v$, 得到了环 F_p+vF_p上互补对偶 $(1-2v)$-常循环码的生成多项式. 然后借助从 F_p+vF_p 到 F_p^2 的Gray映射, 证明了环 F_p+vF_p上互补对偶 $(1-2v)$-常循环码的Gray像是 F_p的互补对偶循环码.

关键词: 互补对偶$(1-2v)$-常循环码; 循环码; 负循环码; 常循环码; 生成多项式

MR(2010)**主题分类号**: 94B05; 94B15; 11T71 **中图分类号**: O157.4