Southeast-Asian J. of Sciences Vol. 5, No. 1 (2017) pp. 47-60

CYCLIC AND NEGACYCLIC CODES OF LENGTH 28 OVER $\mathbb{F}_7 + u\mathbb{F}_7$

Nguyen Trong Bac

Department of Basic Sciences,
University of Economics and Business Administration,
Thai Nguyen University, Thai Nguyen, Vietnam.
e-mail: bacnt2008@gmail.com

Abstract

The aim of this paper is to study algebraic structure of each cyclic and negacyclic code of length 28 over $\mathbb{F}_7 + u\mathbb{F}_7$. Moreover, the number of codewords and the dual of each cyclic and negacyclic code are introduced.

1. Introduction

The class of constacyclic codes plays a very significant role in the theory of error-correcting codes as they are a direct generalization of the important family of cyclic codes. The most important class of these codes is the class of cyclic codes, which have been well studied since the late 1950's. Constacyclic codes also have practical applications as they can be efficiently encoded with simple shift registers, they have rich algebraic structures for efficient error detection and correction, which explains their preferred role in engineering.

Given a nonzero element λ of the field F, λ-constacyclic codes of length n over F are classified as the ideals $\langle g(X)\rangle$ of the quotient ring $F[X]/\langle X^n - \lambda\rangle$, where the generator polynomial $g(X)$ is the unique monic polynimial of minimum degree in the code, which is a divisor of $X^n - \lambda$. However, most of the research is concentrated on the situation when the code length n is relatively prime to the characteristic of the field F. This condition implies that every root of $X^n - \lambda$ is a simple root in an extension field of F, which provides

Key words: cyclic codes, negacyclic codes, dual codes, repeated-root codes.
2000 AMS Mathematics classification:

a description of all such roots, and hence, λ-constacyclic codes, by cyclotomic cosets modulo n.

The case when the code length n is divisible by the characteristic p of the field yields the so-called repeated-root codes, which were first studied since 1967 by Berman [5], and then in the 1970's and 1980's by several authors such as Massey *et al.* [28], Falkner *et al.* [21], Roth and Seroussi [34]. However, repeated-root codes were investigated in the most generality in the 1990's by Castagnoli *et al.* [11], and van Lint [39], where they showed that repeated-root cyclic codes have a concatenated construction, and are asymptotically bad. Nevertheless, such codes are optimal in a few cases, that motivates researchers to further study this class of codes (see, for example, [31, 37, 41]).

Recently, Dinh, in a series of papers ([15], [16], [17]), determined the generator polynomials of all constacyclic codes of lengths $2p^s$, $3p^s$ and $6p^s$ over finite fields $\mathbb{F}_{p^m}$. The class of finite rings of the form $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ has been widely used as alphabets of certain constacyclic codes. For example, the structure of $\mathbb{F}_2 + u\mathbb{F}_2$ is interesting, it is lying between $\mathbb{F}_4$ and $\mathbb{Z}_4$ in the sense that it is additively analogous to $\mathbb{F}_4$, and multiplicatively analogous to $\mathbb{Z}_4$. It has been studied by a lot of researchers (see, for example, [2, 3, 8, 24, 36, 38]). The classification of codes plays an important role in studying their structures, but in general, it is very difficult. Only some codes of certain lengths over certain finite fields or finite chain rings are classified. All constacyclic codes of length 2^s over the Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$ are classified and their detailed structures are also established in [13]. Then in 2010 [14], we classified and gave the detailed structures of all constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$; and in 2012 [15], we provided that for all constacyclic codes of length $2p^s$ over the finite field $\mathbb{F}_{p^m}$.

The rest of the paper is arranged as follows. After presenting preliminary concepts and results in Section 2, we proceed by first obtaining the algebraic structures of all cyclic and negacyclic codes of length 28 over $\mathbb{F}_7+u\mathbb{F}_7$ in Section 3, where such negacyclic codes are classified by categorizing the ideals of the ring $\frac{(\mathbb{F}_7+u\mathbb{F}_7)[x]}{\langle x^{28}-1\rangle}$ and $\frac{(\mathbb{F}_7+u\mathbb{F}_7)[x]}{\langle x^{28}+1\rangle}$, respectively. The detailed structures of ideals are provided. We also establish the number of codewords, and the dual of each cyclic and negacyclic code.

2. Preliminaries

An ideal I of a ring R is called *principal* if it is generated by one element. A ring R is a principal ideal ring if its ideals are principal. R is called a local ring if $R/radR$ is a division ring, or equivalently, if R has a unique maximal right (left) ideal. Furthermore, a ring R is called a chain ring if the set of all right (left) ideals of R is linearly ordered under set-theoretic inclusion. While we will only consider finite commutative rings in this paper, it is worth noting that a finite chain ring need not be commutative. The smallest noncommutative chain ring has order 16 [26, 29], that can be represented as $R = \mathbb{F}_4 \oplus \mathbb{F}_4$, where the operations $+, \cdot$ are defined as

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1 a_2^2).$$

The following equivalent conditions are known for the class of finite commutative rings (cf. [19, Proposition 2.1]).

Proposition 2.1. *Let R be a finite commutative ring, then the following conditions are equivalent:*

(i) R is a local ring and the maximal ideal M of R is principal, i.e., $M = \langle \gamma \rangle$ for some $\gamma \in R$,

(ii) R is a local principal ideal ring,

(iii) R is a chain ring whose ideals are $\langle \gamma^i \rangle$, $0 \leq i \leq \varpi$, where ϖ is the nilpotency of γ.

Let R be a finite ring, a code C of length n over R is a nonempty subset of R^n, and the ring R is refered to as the alphabet of the code. If this subset is, in addition, a R-submodule of R^n, then C is called *linear*. For a unit λ of R, the λ-constacyclic (λ-twisted) shift τ_λ on R^n is the shift

$$\tau_\lambda(x_0, x_1, \dots, x_{n-1}) = (\lambda x_{n-1}, x_0, x_1, \dots, x_{n-2}),$$

and a code C is said to be λ-constacyclic if $\tau_\lambda(C) = C$, i.e., if C is closed under the the λ-constacyclic shift τ_λ. In case $\lambda = 1$, those λ-constacyclic codes are called cyclic codes, and when $\lambda = -1$, such λ-constacyclic codes are called negacyclic codes.

Each codeword $c = (c_0, c_1, \dots, c_{n-1})$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $\frac{R[x]}{\langle x^n - \lambda \rangle}$, $xc(x)$ corresponds to a λ-constacyclic shift of $c(x)$. From that, the following fact is well known (cf. [25, 27]) and straightforward:

Proposition 2.2. *A linear code C of length n is λ-constacyclic over R if and only if C is an ideal of $\frac{R[x]}{\langle x^n - \lambda \rangle}$.*

Given n-tuples $x = (x_0, x_1, \dots, x_{n-1}), y = (y_0, y_1, \dots, y_{n-1}) \in R^n$, their inner product or dot product is defined as usual

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

evaluated in R. Two n-tuples x, y are called *orthogonal* if $x \cdot y = 0$. For a linear code C over R, its *dual code* $C^\perp$ is the set of n-tuples over R that are orthogonal to all codewords of C, i.e.,

$$C^\perp = \{x \mid x \cdot y = 0, \forall y \in C\}.$$

A code C is called *self-orthogonal* if $C \subseteq C^\perp$, and it is called *self-dual* if $C = C^\perp$. The following result is well known (cf. [12, 25, 27, 33]).

Proposition 2.3. *Let p be a prime and R be a finite chain ring of size p^α. The number of codewords in any linear code C of length n over R is p^k, for some integer $k \in \{0, 1, \ldots, \alpha n\}$. Moreover, the dual code $C^\perp$ has p^l codewords, where $k + l = \alpha n$, i.e., $|C| \cdot |C^\perp| = |R|^n$.*

In general, we have the following implication of the dual of a λ-constacyclic code.

Proposition 2.4. *The dual of a λ-constacyclic code is a λ^{-1}-constacyclic code.*

For any odd prime p, we will consider negacycic codes of length $2p^s$ over the ring $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. The ring $\mathcal{R}$ consists of all p^m-ary polynomials of degree 0 and 1 in indeterminate u, it is closed under p^m-ary polynomial addition and multiplication modulo u^2. Thus, $\mathcal{R} = \frac{\mathbb{F}_{p^m}[u]}{\langle u^2 \rangle} = \{a + ub \,|\, a, b \in \mathbb{F}_{p^m}\}$ is a local ring with maximal ideal $u\mathbb{F}_{p^m}$, and hence, it is a chain ring.

Hereafter, let

$$\mathcal{R}_{2p^s} = \frac{\mathcal{R}[x]}{\langle x^{2p^s} + 1 \rangle}.$$

Then, by Proposition 2.2, negacyclic codes of length $2p^s$ over $\mathcal{R}$ are ideals of $\mathcal{R}_{2p^s}$.

Proposition 2.5. *Let*

$$a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

and

$$b(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}.$$

Then $a(x)b(x) = 0$ in $\mathcal{R}$ if and only if $(a_0, a_1, \ldots, a_{n-1})$ is orthogonal to $(b_{n-1}, b_{n-2}, \ldots, b_0)$ and all its negacyclic shifts.

Definition 2.6. *If*

$$f(x) = a_0 + a_1 x + \cdots + a_r x^r,$$

then the reciprocal of $f(x)$ is the polynomial

$$f^*(x) = a_r + a_{r-1} x + a_{r-2} x^2 + \cdots + a_0 x^r.$$

Symbolically, $f^*(x)$ can be expressed by $f^*(x) = x^r f(\frac{1}{x})$. If I is an ideal of $\mathcal{R}_{2p^s}$, then $I^* = \{f^*(x) : f(x) \in I\}$ is also an ideal.

Definition 2.7. *Let I be an ideal of $\mathcal{R}_{2p^s}$. We define $\mathcal{A}(I) = \{g(x) | f(x)g(x) = 0, \forall f(x) \in I\}$. Then $\mathcal{A}(I)$ is called the annihilator of I, which is also an ideal of $\mathcal{R}_{2p^s}$.*

From the above definition we can see that if C is a constacyclic code of length n over $\mathcal{R}$ with associated ideal I, then the associated ideal of $C^\perp$ is $\mathcal{A}(I)^*$. The following two lemmas are easy to prove and are needed in Section 4.

Lemma 2.8. *a) If $\deg f \geq \deg g$, then*

$$(f(x) + g(x))^* = f^*(x) + x^{\deg f - \deg g} g^*(x).$$

b) $(f(x)g(x))^* = f^*(x)g^*(x)$.

Lemma 2.9. *Let $I = \langle f(x), ug(x) \rangle$, then $I^* = \{h^*(x) | h(x) \in I\} = \langle f^*(x), ug^*(x) \rangle$.*

In [14], all cyclic codes of length p^s over $\mathcal{R}$ are classified into 4 types, and the detailed structures of each type are provided. More importantly, a one-to-one correspondence between cyclic and γ-constacyclic codes of length p^s over $\mathcal{R}$ is built via a the ring isomorphism, which enables to apply all results about cyclic codes to γ-constacyclic codes over $\mathcal{R}$. In the next two theorems, following [14, Section 6], we list the classification and structures of all γ-constacyclic codes of length p^s over $\mathcal{R}$, as well as the number of codewords in each such code.

Since γ is a nonzero element of the field $\mathbb{F}_{p^m}$, $\gamma^{-p^m} = \gamma^{-1}$. By the Division Algorithm, there exist nonnegative integers γ_q, γ_r such that $s = \gamma_q m + \gamma_r$, and $0 \leq \gamma_r \leq m-1$. Let $\gamma_0 = \gamma^{-p^{(\gamma_q+1)m-s}} = \gamma^{-p^{m-\gamma_r}}$. Then $\gamma_0^{p^s} = \gamma^{-p^{(\gamma_q+1)m}} = \gamma^{-1}$.

3. Cyclic and negacyclic codes of length 28 over $\mathbb{F}_7 + u\mathbb{F}_7$

We begin this section with a remark as follows.

Proposition 3.1. *Any non-zero polynomial $ax + b \in \mathbb{F}_7[x]$ is invertible in $\frac{\mathcal{R}[x]}{\langle x^{28}+1 \rangle}$.*

Proof. If $a = 0$, then $b \neq 0$. It is clear that b is invertible in $\frac{\mathcal{R}[x]}{\langle x^{28}+1 \rangle}$. In $\mathcal{R}$, we have

$$(x+b)^7(x-b)^7(x^2+b^2)^7 = (x^4 - b^4)^7 = x^{28} - b^{28} = -1 - b^{28}.$$

Since -1 is not a square in $\mathbb{F}_7$, $-1-b^{28}$ is invertible and

$$(ax+b)^{-1} = a^{-1}(x+a^{-1}b)^{-1} = a^{-1}(x+a^{-1}b)^6(x-a^{-1}b)^7(x^2+a^{-2}b^2)^7(-1-b^{28}).$$

It follows that $ax+b$ is a unit in $\frac{\mathcal{R}[x]}{\langle x^{28}+1\rangle}$. $\square$

We can see that 2 is a quadratic residue modulo 7. This means that there exists $\alpha \in \mathbb{F}_7$ such that $2 = \alpha^2$. From this,

$$x^4+1 = (x^4+2x^2+1)-2x^2 = (x^2+1)^2-(\alpha x)^2 = (x^2+\alpha x+1)(x^2-\alpha x+1).$$

In [20], it is well-known that $x^2+\alpha x+1$ and $x^2-\alpha x+1$ are irreducible over $\mathbb{F}_7$. Therefore, $x^{28}+1$ can be expressed as

$$x^{28}+1 = (x^2+\alpha x+1)^7(x^2-\alpha x+1)^7.$$

Let $\delta \in \{1,-1\}$. Then the following lemma is useful.

Lemma 3.2.
The polynomial $x^2+\delta\alpha x+1$ is irreducible over $\mathcal{R}$, where $\alpha^2 = 2 \in \mathbb{F}_7$.

Proof. Suppose that $x^2+\delta\alpha x+1$ is reducible over $\mathcal{R}$. Then there exists an element λ such that $\lambda^2+\delta\alpha\lambda+1=0$, where $\lambda = \lambda_1+u\lambda_2, \lambda_1, \lambda_2 \in \mathbb{F}_{p^m}$. Since $\lambda^2+\delta\alpha\lambda+1=0$, we can see that $\lambda_1^2+\delta\alpha\lambda+1=0$ and $2\lambda_1\lambda_2+\delta\alpha\lambda_2=0$. This shows that $\lambda_1^2+\delta\alpha\lambda_1+1=0$. From $2\lambda_1\lambda_2+\delta\alpha\lambda_2=0$, it is easy to see that $\lambda_2=0$ or $\lambda_1=\frac{-\delta\alpha}{2}$. If $\lambda_2=0$, then $x^2+\delta\alpha x+1$ is reducible over $\mathbb{F}_7$, which is a contradiction. If $\lambda_1=\frac{-\delta\alpha}{2}$, then $\lambda_1^2+\delta\alpha\lambda+1 \neq 0$. This contradicts with assumption, proving that $x^2+\delta\alpha x+1$ is irreducible over $\mathcal{R}$.

Negacyclic codes and their dual codes of length 28 over $\mathcal{R}$ are determined as follows.

Theorem 3.3. *Let C be a negacyclic code of length 28 over $\mathcal{R}$.*

(i) Negacyclic codes of length 28 over $\mathcal{R}$ can be expressed as $C = C_1 \oplus C_2$, where C_1 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (x^2+\alpha x+1)^7\rangle}$ and C_2 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (x^2-\alpha x+1)^7\rangle}$,

(ii) $|C| = |C_1||C_2|$,

(iii) The dual code $C^\perp$ of C is given by $C^\perp = C_1^\perp \oplus C_2^\perp$,

(iv) $C_i^\perp = \mathrm{ann}(C_i)^\star$ for $i=1,2$. Moreover, $C_1^\perp$ is an ideal of $\frac{\mathcal{R}[x]}{\langle (x^2-\alpha x+1)^7\rangle}$, and $C_2^\perp$ is an ideal of $\frac{\mathcal{R}[x]}{\langle (x^2+\alpha x+1)^7\rangle}$.

Proof.

(i) From the isomorphism

$$\frac{\mathcal{R}[x]}{\langle x^{28}+1\rangle} \cong \frac{\mathcal{R}[x]}{\langle (x^2+\alpha x+1)^7\rangle} \oplus \frac{\mathcal{R}[x]}{\langle (x^2-\alpha x+1)^7\rangle},$$

we can see that every negacyclic code of length 28 over $\mathcal{R}$ can be expressed as $C = C_1 \oplus C_2$, where C_1 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (x^2+\alpha x+1)^7\rangle}$ and C_2 is an ideal of the ring $\frac{\mathcal{R}[x]}{\langle (x^2-\alpha x+1)^7\rangle}$.

(ii) It is routine to check that $|C| = |C_1||C_2|$.

To investigate negacyclic codes and their duals of length 28 over $\mathcal{R}$, we need to determine all ideals of the rings $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$ and $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\beta x-1)^7\rangle}$. We get an important lemma.

Lemma 3.4. *Any non-zero polynomial $cx+d \in \mathbb{F}_7[x]$ is invertible in $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$ and $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\beta x-1)^7\rangle}$.*

Proof. If $c = 0$, then $d \neq 0$. This implies that d is invertible in $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$. If $c \neq 0$, we have

$$\begin{aligned}
(cx+d)^{-1} &= c(x+c^{-1}d)^{-1}\\
&= c(x+c^{-1}d)^6(x-c^{-1}d+\delta\alpha)^7(x+c^{-1}d)^{-7}(x-c^{-1}d+\delta\alpha)^{-7}\\
&= c^{-1}(x+c^{-1}d)^6(x-c^{-1}d+\delta\alpha)^7(x^2+\delta\alpha x-(c^{-1}d)^2)+\delta\alpha(c^{-1}d)^{-7}\\
&= c(x+c^{-1}d)^6(x-c^{-1}d+\delta\alpha)^6((-1)^7-(c^{-1}d)^{14}+(\delta\alpha c^{-1}d)^7)^{-1}\\
&= -c(x+c^{-1}d)^6(x-c^{-1}d+\delta\alpha)^7(1+(c^{-1}d)^2-(\delta\alpha)c^{-1}d)^{-7}.
\end{aligned} \tag{1}$$

It is clear that $1+(c^{-1}d)^2-(\delta\alpha)c^{-1}d$ is non-zero for all $c^{-1}d \in \mathbb{F}_7$. Hence, $cx+d$ is invertible in $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$. Similarly, we also prove that $cx+d$ is invertible in $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\beta x-1)^7\rangle}$. $\square$

Lemma 3.5.

(i) Let $f(x) \in \frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$. *Then* $f(x)$ *can be uniquely expressed as*

$$\begin{aligned} f(x) &= \sum_{i=0}^{p^s-1}(c_{0i}x + d_{0i})(x^2+\delta\alpha x+1)^i + u\sum_{i=0}^{p^s-1}(c_{1i}x+d_{1i})(x^2+\delta\alpha x+1) \\ &= c_{00}x + d_{00} + (x^2+\delta\alpha x+1)\sum_{i=1}^{6}(c_{00}x+d_{0i})(x^2+\delta\alpha x+1)^{i-1} + \\ &\quad + u\sum_{i=0}^{6}(c_{1i}x+d_{1i})(x^2+\delta\alpha x+1)^i, \end{aligned} \tag{2}$$

where $c_{0i}, d_{0i}, c_{1i}, d_{1i} \in \mathbb{F}_{p^m}$ *for* $0 \le i \le p^s - 1$. *Moreover,* $f(x)$ *is non-invertible if and only if* $c_{00} = d_{00} = 0$.

(ii) Let $g(x) \in \frac{\mathcal{R}[x]}{\langle (x^2+\delta\beta x-1)^{p^s}\rangle}$. *Then* $g(x)$ *can be uniquely expressed as*

$$\begin{aligned} g(x) &= \sum_{i=0}^{6}(c'_{0i}x + d'_{0i})(x^2+\delta\beta x-1)^i + u\sum_{i=0}^{p^s-1}(c'_{1i}x+d'_{1i})(x^2+\delta\beta x-1) \\ &= c'_{00}x + d'_{00} + (x^2+\delta\beta x-1)\sum_{i=1}^{6}(c'_{00}x+d'_{0i})(x^2+\delta\beta x-1)^{i-1} \\ &\quad + u\sum_{i=0}^{6}(c'_{1i}x+d'_{1i})(x^2+\delta\beta x-1)^i, \end{aligned} \tag{3}$$

where $c'_{0i}, d'_{0i}, c'_{1i}, d'_{1i}$ *for* $0 \le i \le 6$. *Moreover,* $g(x)$ *is non-invertible if and only if* $c'_{00} = d'_{00} = 0$.

Proof. The representation of $f(x)$ follows from the fact that it can be viewed as a polynomial of degree less than 6 over $\mathcal{R}$. We have $(x^2+\delta\alpha x+1)^6 = 0$ and $u^2 = 0$ in $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^6\rangle}$. This shows that $(x^2+\delta\alpha x+1)^6$ are nilpotent elements of $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^6\rangle}$. Hence, $f(x)$ is non-invertible if and only if $c_{00} = d_{00} = 0$ by Lemma 3.4, proving part (i).
Part (ii) can be proved by using in a similar way as in the proof of part (i). □

Applying Lemma 3.4 and 3.5, we give some characterizations of the ring $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$ and $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\beta x-1)^7\rangle}$ as follows.

Theorem 3.6.
The polynomial $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$ *is a local ring with maximal ideal* $\langle x^2+\delta\alpha x+1, u\rangle$ *but not a chain ring. In particular,* $\langle x^2+\delta\alpha x+1\rangle$ *is a nilpotent element of* $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$ *with the nilpotency index* 7.

Proof. By using Lemma 3.4, we see that all the non-invertible of $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$ are ideals $\langle x^2+\delta\alpha x+1, u\rangle$. It is equivalent to say that $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$ is a local ring with the maximal ideal $\langle x^2+\delta\alpha x+1, u\rangle$. It is easy to see that $u \notin \langle x^2+\delta\alpha x+1\rangle$. Obviously, $x^2+\delta\alpha x+1 \notin \langle u\rangle$. Hence, $\langle x^2+\delta\alpha x+1, u\rangle$ is not a principal ideal of $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$, implying that $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$ is not a chain ring according to Proposition 2.1.

We now determine all ideals of $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$ and $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\beta x-1)^7\rangle}$ in the following theorem.

Theorem 3.7. *The all ideals in* $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$ *are listed as follows:*

- *Type 1: (trivial ideals)*
$$\langle 0\rangle,\ \langle 1\rangle.$$
- *Type 2: (principal ideals with nonmonic polynomial generators)*
$$\langle u(x^2+\delta\alpha x+1)^i\rangle,$$
where $0 \le i \le 6$.
- *Type 3: (principal ideals with monic polynomial generators)*
$$\langle (x^2+\delta\alpha x+1)^i + u(x^2+\delta\alpha x+1)^t h(x)\rangle,$$
where $1 \le i \le 6, 0 \le t < i$, *and either* $h(x)$ *is 0 or* $h(x)$ *is a unit which can be represented as* $h(x) = \sum_j (h_{0j}x + h_{1j})(x^2+\delta\alpha x+1)^j$, *with* $h_{0j}, h_{1j} \in \mathbb{F}_7$, *and* $h_{00}x + h_{10} \neq 0$.
- *Type 4: (nonprincipal ideals)*
$$\langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{\omega-1}(c_jx+d_j)(x^2+\delta\alpha x+1)^j, u(x^2+\delta\alpha x+1)^\omega\rangle,$$
where $1 \le i \le 6, c_j, d_j \in \mathbb{F}_7$, *and* $\omega < T$, *where* T *is the smallest integer such that*
$$u(x^2+\delta\alpha x+1)^T \in \langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{i-1}(c_jx+d_j)(x^2+\delta\alpha x+1)^j\rangle;$$
or equivalently,
$$\langle (x^2+\delta\alpha x+1)^i + u(x^2+\delta\alpha x+1)^t h(x), u(x^2+\delta\alpha x+1)^\omega\rangle,$$
with $h(x)$ *as in Type 3, and* $\deg h(x) \le \omega - t - 1$.

Proof. Firstly, it is easy to see that ideals of Type 1 are trivial ideals. Let I be an arbitrary nontrivial ideal of $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$. We proceed by establishing all possible forms that ideal I can have.

Case 1. $I \subseteq \langle u\rangle$: Suppose that $c(x) \in I$. Then $v(x)$ must be of the form $u\sum_{i=0}^{6}(c_{1i}x + d_{1i})(x^2+\delta\alpha x+1)^i$, where $c_{1i}, d_{1i} \in \mathbb{F}_7$. This implies that there exists an element $a \in I$ that has the smallest k such that $c_{1k}x + d_{1k} \neq 0$. Hence each element $c(x) \in I$ have the form $c(x) = u(x^2+\delta\alpha x+1)^k \sum_{i=k}^{6}(c_{1i}x + d_{1i})(x^2+\delta\alpha x+1)^{i-k}$, implying that $I \subseteq \langle u(x^2+\delta\alpha x+1)^k\rangle$. However, we have $a \in I$ with

$$\begin{aligned} a &= u(x^2+\delta\alpha x+1)^k \sum_{i=k}^{6}(c_{1i}x + d_{1i})(x^2+\delta\alpha x+1)^{i-k} \\ &= u(x^2+\delta\alpha x+1)^k \left[c_{1k}x + d_{1k} + \sum_{i=k+1}^{p^s-1}(c_{1i}x + d_{1i})(x^2+\delta\alpha x+1)^{i-k}\right]. \end{aligned}$$

From $c_{1k}x + d_{1k} \neq 0$, we can see that $c_{1k}x + d_{1k} + \sum_{i=k+1}^{p^s-1}(c_{1i}x + d_{1i})(x^2+\delta\alpha x+1)^{i-k}$ is invertible, proving that $u(x^2+\delta\alpha x+1)^k \in I$. Therefore, $I = \langle u(x^2+\delta\alpha x+1)^k\rangle$, which means that the nontrivial ideals of $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$ contained in $\langle u\rangle$ are $\langle u(x^2+\delta\alpha x+1)^k\rangle, 0 \leq k \leq 6$, which are ideals of Type 2, as desired.

Case 2. $I \not\subseteq \langle u\rangle$: Let I_u denote the set of elements in I which are reduced modulo u. Note that I_u is a nonzero ideal of the ring $\frac{\mathbb{F}_7[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle}$, which is a finite chain ring with ideals $\langle (x^2+\delta\alpha x+1)^j\rangle$, where $0 \leq j \leq 7$, according to [15, Theorem 3.2]. Then there is an integer $i \in \{0, 1, \ldots, 6\}$ such that $I_u = \langle (x^2+\delta\alpha x+1)^i\rangle \subseteq \frac{\mathbb{F}_7[x]}{\langle x^2+\delta\alpha x+1\rangle}$. This follows that there exists an element

$$c(x) = \sum_{j=0}^{p^s-1}(c_{0j}x+d_{0j})(x^2+\delta\alpha x+1)^j + u\sum_{j=0}^{6}(c_{1j}x+d_{1j})(x^2+\delta\alpha x+1)^j \in \frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^7\rangle},$$

where $c_{0j}, c_{1j}, d_{0j}, d_{1j} \in \mathbb{F}_7$, such that $(x^2+\delta\alpha x+1)^i + uc(x) \in I$. Since

$$(x^2+\delta\alpha x+1)^i + uc(x) = (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{p^s-1}(c_{0j}x+d_{0j})(x^2+\delta\alpha x+1)^j \in I,$$

and $u(x^2+\delta\alpha x+1)^k = u[(x^2+\delta\alpha x+1)^i + uc(x)](x^2+\delta\alpha x+1)^{k-i} \in I$ with $i \leq k \leq 6$, we have $(x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{i-1}(c_{0j}x + d_{0j})(x^2+\delta\alpha x+1)^j \in I$. We now divided into two subcases.

Case 2a. $I = \langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{i-1}(c_jx+d_j)(x^2+\delta\alpha x+1)^j\rangle$, then I can be expressed as

$$I = \langle (x^2+\delta\alpha x+1)^i + u(x^2+\delta\alpha x+1)^t h(x)\rangle,$$

where $h(x)$ is 0 or a unit. If $h(x)$ is a unit, then $h(x)$ can be represented as $h(x) = \sum_j (h_{0j}x+h_{1j})(x^2+\delta\alpha x+1)^j$, with $h_{0j}, h_{1j} \in \mathbb{F}_{p^m}$ and $h_{00}x+h_{10} \neq 0$, it follows that I is of Type 3.

Case 2b. $\langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})(x^2+\delta\alpha x+1)^j\rangle \subsetneq I$. Then there exists $f(x) \in I \setminus \langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})(x^2+\delta\alpha x+1)^j\rangle$, hence there is a polynomial $g(x) \in \frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^{p^s}\rangle}$ such that

$$0 \neq h(x) = f(x) - g(x)\left[(x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})(x^2+\delta\alpha x+1)^j\right] \in I,$$

showing that $h(x)$ can be expressed as

$$h(x) = \sum_{j=0}^{i-1}(h_{0j}x+h'_{0j})(x^2+\delta\alpha x+1)^j + u\sum_{j=0}^{i-1}(h_{1j}x+h'_{1j})(x^2+\delta\alpha x+1)^j,$$

where $h_{0j}, h'_{0j}, h_{1j}, h'_{1j} \in \mathbb{F}_{p^m}$. Hence, $h(x)$ reduced modulo u is in $I_u = \langle (x^2+\delta\alpha x+1)^i\rangle$, and thus, $h_{0j}, h'_{0j} = 0$ for all $0 \leq j \leq i-1$, i.e., $h(x) = u\sum_{j=0}^{i-1}(h_{1j}x+h'_{1j})(x^2+\delta\alpha x+1)^j$. Since $h(x) \neq 0$, there exists a smallest integer $k, 0 \leq k \leq i-1$, such that $h_{1k}x+h'_{1k} \neq 0$. Then

$$\begin{aligned} h(x) &= u\sum_{j=k}^{i-1}(h_{1j}x+h'_{1j})(x^2+\delta\alpha x+1)^j \\ &= u(x^2+\delta\alpha x+1)^k\left[h_{1k}x+h'_{1k}+\sum_{j=k+1}^{i-1}(h_{1j}x+h'_{1j})(x^2+\delta\alpha x+1)^{j-k}\right]. \end{aligned}$$

As $h_{1k}x+h'_{1k} \neq 0, h_{1k}x+h'_{1k}+\sum_{j=k+1}^{i-1}(h_{1j}x+h'_{1j})(x^2+\delta\alpha x+1)^{j-k}$ is an invertible element in $\frac{\mathcal{R}[x]}{\langle (x^2+\delta\alpha x+1)^{p^s}\rangle}$, hence,

$$u(x^2+\delta\alpha x+1)^k = (h_{1k}x+h'_{1k}+\sum_{j=k+1}^{i-1}(h_{1j}x+h'_{1j})(x^2+\delta\alpha x+1)^{j-k})^{-1}h(x) \in I.$$

It has been shown that for any $f(x) \in I \setminus \langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})(x^2+\delta\alpha x+1)^j\rangle$, there is an integer k with $0 \leq k \leq i-1$ such that $u(x^2+\delta\alpha x+1)^k \in I$. Let $\omega = \min\{k \mid f(x) \in I \setminus \langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})(x^2+\delta\alpha x+1)^j\rangle\}$. Then $\langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})(x^2+\delta\alpha x+1)^j, u(x^2+\delta\alpha x+1)^\omega\rangle \subseteq I$. In addition, by the above construction, for any

$f(x) \in I$, there exists a polynomial $g(x) \in I$ satisfying

$$f(x)-g(x)[(x^2+\delta\alpha x+1)^i+u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})(x^2+\delta\alpha x+1)^j] \in \langle u(x^2+\delta\alpha x+1)^\omega\rangle,$$

implying that $f(x) \in \langle (x^2+\delta\alpha x+1)^i+u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})(x^2+\delta\alpha x+1)^j, u(x^2+\delta\alpha x+1)^\omega\rangle$. Thus,

$$\begin{aligned} I &= \langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{i-1}(c_{0j}x+d_{0j})(x^2+\delta\alpha x+1)^j, u(x^2+\delta\alpha x+1)^\omega\rangle \\ &= \langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{\omega-1}(c_{0j}x+d_{0j})(x^2+\delta\alpha x+1)^j, u(x^2+\delta\alpha x+1)^\omega\rangle. \end{aligned}$$

Let T be the smallest integer such that $u(x^2+\delta\alpha x+1)^T \in \langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{i-1}(c_jx+d_j)(x^2+\delta\alpha x+1)^j\rangle$. If $\omega \geq T$, then
$I = \langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{\omega-1}(c_jx+d_j)(x^2+\delta\alpha x+1)^j, u(x^2+\delta\alpha x+1)^\omega\rangle$
$= \langle (x^2+\delta\alpha x+1)^i + u\sum_{j=0}^{i-1}(c_jx+d_j)(x^2+\delta\alpha x+1)^j\rangle$.
This is a contradiction with the assumption of this case. This follows that $\omega < T$, proving that I is of Type 4. □

We also determine all cyclic codes of length 28 over $\mathbb{F}_7 + u\mathbb{F}_7$.

Remark 3.8. We can express the factorization of $x^{28} - 1$ into product of unique monic irreducible factors as follows:

$$x^{28} - 1 = (x^4 - 1)^7 = (x^7 - 1)(x^7 + 1)(x^{14} + 1).$$

By Chinese remainder theorem, we can see that

$$\frac{\mathcal{R}[x]}{\langle x^{28}-1\rangle} \cong \frac{\mathcal{R}[x]}{\langle x^{28}-1\rangle} \oplus \frac{\mathcal{R}[x]}{\langle x^{7}+1\rangle} \oplus \frac{\mathcal{R}[x]}{\langle x^{14}+1\rangle}.$$

From this isomorphism, using arguments similar to those in the proof of Theorem 3.1 and 3.2, we can determine the algebraic structures of all cyclic codes of length 28 over $\mathcal{R}$. Moreover, the number of codewords in each cyclic code are provided. Similar to the Theorem 3.3, we also give some self-dual cyclic codes of length 28 over $\mathcal{R}$.

Theorem 3.9. *Let C be a cyclic code of length 28 over $\mathcal{R}$. Then we have*

(i) $C = C_1 \oplus C_2 \oplus C_3$, *where C_1, C_2, C_3 are ideals of the rings* $\frac{\mathcal{R}[x]}{\langle x^7-1\rangle}$, $\frac{\mathcal{R}[x]}{\langle x^7+1\rangle}$, $\frac{\mathcal{R}[x]}{\langle x^{14}+1\rangle}$, *respectively.*

(ii) $|C| = |C_1||C_2||C_3|$.

(iii) The dual code $C^\perp$ of C is computed by $C^\perp = C_1^\perp \oplus C_2^\perp \oplus C_3^\perp$, where C_i is the dual code of C_i $(i = 1, 2, 3)$.

Theorem 3.10. *Let $C = C_1 \oplus C_2 \oplus C_3$ be a cyclic code of length 28 over $\mathcal{R}$, where C_1, C_2, C_3 are ideals of the rings $\frac{\mathcal{R}[x]}{\langle x^7-1\rangle}, \frac{\mathcal{R}[x]}{\langle x^7+1\rangle}, \frac{\mathcal{R}[x]}{\langle x^{14}+1\rangle}$, respectively. Then the following hold:*

(i) If $C_1 = \langle u\rangle, C_2 = \langle u\rangle$ and $C_3 = \langle u\rangle$, then $C = C_1 \oplus C_2 \oplus C_3 = \langle u\rangle$ is a self-dual cyclic code of length 28 over $\mathcal{R}$.

(ii) If $C_1 = \langle (x-1)^i, u(x-1)^{7-i}\rangle, C_2 = \langle (x+1)^j, u(x+1)^{7-j}\rangle$ and $C_3 = \langle (x^2+1)^k, u(x^2+1)^{7-k}\rangle$, then $C = C_1 \oplus C_2 \oplus C_3$ is a self-dual cyclic code of length 28 over $\mathcal{R}$, where $1 \le i, j, k < 7$.

References

[1] T. Abualrub and R. Oehmke, *On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e*, IEEE Trans. Inform. Theory **49** (2003), 2126-2133.

[2] M.M. Al-Ashker, *Simplex codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$*, Arab. J. Sci. Eng. Sect. A Sci. **30** (2005), 277-285.

[3] E. Bannai, M. Harada, T. Ibukiyama, A. Munemasa, and M. Oura, *Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and applications to Hermitian modular forms*, Abh. Math. Sem. Univ. Hamburg **73** (2003), 13-42.

[4] E. R. Berlekamp, *Negacyclic codes for the Lee metric,* in: Proceedings of the Conference on Combinatorial Mathematics and Its Application, Chapel Hill, NC, 1968, 298-316.

[5] S.D. Berman, *Semisimple cyclic and Abelian codes. II*, Kibernetika (Kiev) **3**, 1967, 21-30 (Russian); translated as Cybernetics **3** (1967), 17-23.

[6] T. Blackford, *Negacyclic codes over $\mathbb{Z}_4$ of even length*, IEEE Trans. Inform. Theory **49** (2003), 1417-1424.

[7] T. Blackford, *Cyclic codes over $\mathbb{Z}_4$ of oddly even length*, International Workshop on Coding and Cryptography (WCC 2001) (Paris), Appl. Discr. Math. **128** (2003), 27-46.

[8] A. Bonnecaze and P. Udaya, *Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$*, IEEE Trans. Inform. Theory **45** (1999), 1250-1255.

[9] B. Chen, H.Q. Dinh, H. Liu and L.Wang, *Constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$,* **36** 2016, 108-130.

[10] A.R. Calderbank, A.R. Hammons, P.V. Kumar, N.J. A. Sloane, and P. Solé, *A linear construction for certain Kerdock and Preparata codes*, Bull. AMS **29** (1993), 218-222.

[11] G. Castagnoli, J.L. Massey, P.A. Schoeller, and N. von Seemann, *On repeated-root cyclic codes*, IEEE Trans. Inform. Theory **37** (1991), 337-342.

[12] H.Q. Dinh, *Negacyclic codes of length 2^s over Galois rings*, IEEE Trans. Inform. Theory **51** (2005), 4252-4262.

[13] H. Q. Dinh, *Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$*, IEEE Trans. Inform. Theory **55** (2009), 1730-1740.

[14] H.Q. Dinh, *Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, J. Algebra **324** (2010), 940-950.

[15] H.Q. Dinh, *Repeated-root constacyclic codes of length $2p^s$*, Finite Fields & Appl. **18** (2012), 133-143.

[16] H. Q. Dinh, *Structure of repeated-root constacyclic codes of length* $3p^s$ *and their duals*, Discrete Math. **313**(2013), 983-991.

[17] H. Q. Dinh, *Structure of repeated-root cyclic and negacyclic codes of length* $6p^s$ *and their duals,* AMS Contemporary Mathematics 609 (2014), 69-87.

[18] , H. Q. Dinh, Liqi Wang and Shixin Zhu, *Negacyclic codes of length* $2p^s$ *over* $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, Finite Fields & Appl. **31** (2015), 178-201.

[19] H.Q. Dinh and S.R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50** (2004), 1728-1744.

[20] H.Q. Dinh, Sompong Dhompongsa, and Songsak Sriboonchitta, *On constacyclic codes of length* $4p^s$ *over* $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, Discrete Mathematics, accepted for publication.

[21] G. Falkner, B. Kowol, W. Heise, and E. Zehendner, *On the existence of cyclic optimal codes*, Atti Sem. Mat. Fis. Univ. Modena **28** (1979), 326-341.

[22] S.T. Dougherty, S. Ling, *Cyclic codes over* $\mathbb{Z}_4$ *of even length*, Des. Codes Cryptogr. **39** (2006), 127-153.

[23] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301-319.

[24] W.C. Huffman, *On the decomposition of self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$ *with an automorphism of odd prime order*, Finite Fields & Appl. **13** (2007), 681-712.

[25] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[26] E. Kleinfeld, *Finite Hjelmslev planes*, Illinois J. Math. **3** (1959), 403-407.

[27] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, 10^{th} impression, North-Holland, Amsterdam, 1998.

[28] J.L. Massey, D.J. Costello, and J. Justesen, *Polynomial weights and code constructions*, IEEE Trans. Inform. Theory **19** (1973), 101-110.

[29] B.R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, Vol. **28**, Marcel Dekker, New York, 1974.

[30] A.A. Nechaev, *Kerdock code in a cyclic form*, (in Russian), Diskr. Math. (USSR) **1** (1989), 123-139. English translation: Discrete Math. and Appl. **1** (1991), 365-384.

[31] C.-S. Nedeloaia, *Weight distributions of cyclic self-dual codes*, IEEE Trans. Inform. Theory **49** (2003), 1582-1591.

[32] G. Norton and A. Sălăgean-Mandache, *On the structure of linear cyclic codes over finite chain rings*, Appl. Algebra Engrg. Comm. Comput. **10** (2000), 489–506.

[33] V. Pless and W.C. Huffman, *Handbook of coding theory*, Elsevier, Amsterdam, 1998.

[34] R.M. Roth and G. Seroussi, *On cyclic MDS codes of length* q *over* GF(q)*,* IEEE Trans. Inform. Theory **32** (1986), 284-285.

[35] A. Sălăgean, *Repeated-root cyclic and negacyclic codes over finite chain rings*, Discrete Appl. Math. **154** (2006), 413-419.

[36] I. Siap, *Linear codes over* $\mathbb{F}_2 + u\mathbb{F}_2$ *and their complete weight enumerators*, Codes and designs (Columbus, OH, 2000), Ohio State Univ. Math. Res. Inst. Publ. **10** (2002), de Gruyter, Berlin, 259-271.

[37] L.-z. Tang, C.B. Soh and E. Gunawan, *A note on the q-ary image of a* q^m*-ary repeated-root cyclic code*, IEEE Trans. Inform. Theory **43** (1997), 732-737.

[38] P. Udaya and A. Bonnecaze, *Decoding of cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory **45** (1999), 2148-2157.

[39] J.H. van Lint, *Repeated-root cyclic codes*, IEEE Trans. Inform. Theory **37** (1991), 343-345.

[40] J. Wolfmann, *Negacyclic and cyclic codes over* $\mathbb{Z}_4$, IEEE Trans. Inform. Theory **45** (1999), 2527-2532.

[41] K.-H. Zimmermann, *On generalizations of repeated-root cyclic codes*, IEEE Trans. Inform. Theory **42** (1996), 641-649.