Thai Journal of Mathematics
Volume 17 (2019) Number 2 : 413–429
http://thaijmath.in.cmu.ac.th
ISSN 1686-0209

The Structure of Constacyclic Codes of Length $2p^s$ over Finite Chain Rings

Wateekorn Sriwirach and Chakkrid Klin-eam[1]

Department of Mathematics, Faculty of Science
Naresuan University, Phitsanulok 65000, Thailand
e-mail : `wateekorns@hotmail.com (W. Sriwirach)`
`chakkridk@nu.ac.th (C. Klin-eam)`

Abstract : Let R be a finite commutative chain ring with identity of characteristic p^a that has maximal ideal $\langle z\rangle$. In this paper, we study λ-constacyclic codes of length $2p^s$ over R, for any unit λ of R. If the unit λ is not a square, the rings $\mathcal{R}_\lambda = \frac{R[x]}{\langle x^{2p^s}-\lambda\rangle}$ is a local ring with maximal ideal $\langle x^2-r, z\rangle$, where $r \in R$ such that $\lambda - r^{p^s}$ is not invertible. When there exists a unit λ_0 of R such that $\lambda = \lambda_0^{p^s}$, we prove that $x^2-\lambda_0$ is nilpotent with nilpotency index $ap^s-(a-1)p^{s-1}$. When $\lambda = \lambda_0^{p^s} + z\omega$, for some unit ω of R, we show that $\mathcal{R}_\lambda$ is also a chain ring with maximal ideals $\langle x^2-\lambda_0\rangle$. Furthermore, the algebraic structure and dual of all λ-constacyclic codes are obtained.

Keywords : constacyclic codes; repeated-root codes, local rings; code over rings; finite chain rings.
2010 Mathematics Subject Classification : 94B15; 94B05; 11T71.

1 Introduction

The most important class of codes is that of cyclic codes, which has been well studied since the late 1950's. Cyclic codes are the most studied of all codes such as BCH, Kerdock, Golay, Reed-Muller, Preparata, Justesen, and binary Hamming codes, are either cyclic codes or constructed from cyclic codes. However, most of this research is concentrated on the situation in which the code length n is relatively

[1] Corresponding author.

prime to the characteristic of finite field F. The class of constacyclic codes play a very significant role in the theory of error-correcting codes. Constacyclic codes can be efficiently encoded using shift registers, which explains their preferred role in engineering. Given a nonzero element λ of the finite field F, λ-constacyclic codes of length n are classified as the ideals $\langle f(x)\rangle$ of the quotient ring $\frac{F[x]}{\langle x^n-\lambda\rangle}$, where the $f(x)$ is a divisor of $x^n-\lambda$.

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 [1]. In the 1990's [2–4] that many important yet seemingly non-linear binary codes such as Kerdock and Preparata codes are actually closely related to linear codes over the ring of integers modulo four via the Gray map, codes over $\mathbb{Z}_4$ in particular, and codes over finite rings in general, have received a great deal of attention. A code C of length n over a finite ring R is a nonempty subset of R^n, and the ring R is referred to as the alphabet of the code. If this subset is, in addition, an R-submodule of R^n, then C is called *linear code.* For a unit λ of R, the λ-constacyclic (λ-twisted) shift τ_λ on R^n is the shift

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

and a code C is said to be λ-*constacyclic* if $\tau_\lambda(C)=C$, i.e., if C is closed under the λ-constacyclic shift τ_λ, for $\lambda=1$, they are called *cyclic codes*, and when $\lambda=-1$, they are called *negacyclic codes.* Each codeword $c=(c_0,c_1,...,c_{n-1})$ is identified with its polynomial repesentation $c(x)=c_0+c_1x+...+c_{n-1}x^{n-1}$, 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 $c(x)$. The following is known.

Proposition 1.1. [5, 6] *A linear code C of length n is λ-constacyclic over R if and only if C is an ideal of the quotient ring $\frac{R[x]}{\langle x^n-\lambda\rangle}$.*

Over the last few years, many researchers studied that repeated-root constacyclic codes over class of finite chain rings, such as Abualrub and Ochmke [7, 8], Blackford [9, 10], Dinh [11–14], Ling et al. [15–17], Sălăgean et al. [18, 19], etc. Recently, Dinh [20] studied the algebraic structure of repeated-root λ-constacyclic codes of prime power length p^s over finite chain ring in general.

The structure of the paper is as follows. In Section 2, Preliminary concepts and give some properties of chain rings and constacyclic codes. In Section 3, we study λ-constacyclic codes of length $2p^s$ over a finite commutative chain ring R of characteristic p^a with unique maximal ideal $\langle z\rangle$. By the Chinese Remainder Theorem, we can prove that if the unit λ is a square in R, i.e., $\lambda=\alpha^2$, for some unit α of R, then every λ-constacyclic codes of length $2p^s$ over R can be represented as a direct sum of an $(-\alpha)$-constacyclic code and an α-constacyclic code of length p^s over R. In the main case, we consider λ is not a square. we prove that the rings $\mathcal{R}_\lambda=\frac{R[x]}{\langle x^{2p^s}-\lambda\rangle}$ is a local ring with maximal ideal $\langle x^2-r,z\rangle$, where $r\in R$ such that $\lambda-r^{p^s}$ is not invertible. When there exists a unit λ_0 of R such that

$\lambda = \lambda_0^{p^s}$, we get that $x^2 - \lambda_0$ is nilpotent with nilpotency index $ap^s - (a-1)p^{s-1}$. When $\lambda = \lambda_0^{p^s} + z\omega$, for some unit ω of R, we show that $\mathcal{R}_\lambda$ is also a chain ring with maximal ideals $\langle x^2 - \lambda_0 \rangle$. Furthermore, the algebraic structure and dual of all λ-constacyclic codes are obtained.

2 Preliminaries

An ideal I of a ring is called *principal* if it is generated by single element. A ring R is a *principal ideal ring* if its ideals are principal. R is called a *local ring* 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. The following equivalent conditions are known for the class of finite commutative rings (see, [21, Proposition 2.1]).

Proposition 2.1. *If R is a finite commutative ring with identity, then the following conditions are equivalent:*

(a) *R is a local ring and the maximal ideal M of R is principal,*

(b) *R is a local principal ideal ring,*

(c) *R is a chain ring.*

Let z be a fixed generator of the maximal ideal M of a finite commutative chain ring R. Then z is nilpotent and we denote its nilpotency index by N_z. The ideals of R form a chain:

$$R = \langle z^0 \rangle \supsetneq \langle z^1 \rangle \supsetneq \cdots \supsetneq \langle z^{N_z - 1} \rangle \supsetneq \langle z^{N_z} \rangle = \langle 0 \rangle,$$

Let $\bar{R} = \frac{R}{M}$ be the residue field of R modulo its maximal ideal M. By $^- :$ $R[x] \to \bar{R}[x]$, we denote the natural ring homomorphism that maps $r \mapsto r + M$ and the variable x to x. We have the following well-known properties of finite commutative chain rings (cf. [22]).

Proposition 2.2. *Let R be a finite commutative chain ring with maximal ideal $M = \langle z \rangle$ and let N_z be the nilpotency z. Then*

(a) *For some prime p and positive integer k, l with $k \geq l$ such that $|R| = p^k$, $|\bar{R}| = p^l$, and the characteristic of R is powers of p and $\bar{R}$ are powers of p.*

(b) *There is an element ξ of the multiplicative group of units of R with multiplicative order $|\bar{R}| - 1$ such that any element $r \in R$ can be uniquely expressed as*

$$r = r_0 + r_1 z + \cdots + r_{N_z - 1} z^{N_z - 1},$$

where $r_i \in \mathcal{T} = \{0, 1, \xi, ..., \xi^{|\bar{R}|-2}\}$, the Teichmüller set of R.

(c) *For $i = 0, ..., N_z$, $|\langle z^i \rangle| = |\bar{R}|^{N_z - i}$. In particular, $|R| = |\bar{R}|^{N_z}$, i.e., $k = lN_z$.*

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

$$x \cdot y = x_0y_0 + x_1y_1 + ... + x_{n-1}y_{n-1},$$

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 proposition can be found in [23].

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

Note that the dual of cyclic code is a cyclic code, and the dual of a negacyclic code is a negacyclic code. In general, we have the following implication of dual of a λ-constacyclic code.

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

For a nonempty subset S of the ring R, the *annihilator* of S, denoted by $\mathrm{ann}(S)$, is the set

$$\mathrm{ann}(S) = \{f \in R \mid fg = 0, \text{ for all } g \in R\}.$$

Then $\mathrm{ann}(S)$ is an ideal of R.

Customarily, for a polynomial f of degree k, its reciprocal polynomial $x^k f(x^{-1})$ will be denoted by $f^*(x)$. Thus, for example, if

$$f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + a_kx^k,$$

then

$$\begin{aligned} f^*(x) &= x^k(a_0 + a_1x^{-1} + \cdots + a_{k-1}x^{-(k-1)} + a_kx^{-k}) \\ &= a_k + a_{k-1}x + \cdots + a_1x^{k-1} + a_0x^k. \end{aligned}$$

Note that $(f^*)^*(x) = f(x)$ if and only if the constant term of f is nonzero, if and only if $\deg(f) = \deg(f^*)$. We denote $A^* = \{f^*(x) \mid f(x) \in A\}$. It is easy to see that if A is an ideal, then A^* is also an ideal.

Proposition 2.5. (cf. [13, 21]) *Let R be a finite commutative chain ring, and λ be a unit of R.*

(a) *Let $a(x), b(x) \in R[x]$ be given as*

$$a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1},$$
$$b(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}.$$

Then $a(x)b(x) = 0$ in $\frac{R[x]}{\langle x^n-\lambda\rangle}$ if and only if $(a_0, a_1, ..., a_{n-1})$ is orthogonal to $(b_{n-1}, b_{n-2}, ..., b_0)$ and all its λ^{-1}-constacyclic shifts.

(b) *Let C be a λ-constacyclic code of length n over R. Then the dual $C^\perp$ of C is $(\mathrm{ann}(C))^*$, and $|C| \cdot |C^\perp| = |R|^n$.*

Let R be a finite chain ring of characteristic p^a that has maximal ideal $\langle z\rangle$. Let N_z denote the nilpotency index of z. For any unit λ of R, by Proposition 1.1, λ-constacyclic codes of length $2p^s$ over R are the ideals of the ambient ring $\mathcal{R}_\lambda = \frac{R[x]}{\langle x^{2p^s}-\lambda\rangle}$.

3 λ-Constacyclic Codes of Length $2p^s$ over a Finite Chain Ring

In this section, we consider λ-constacyclic codes of length $2p^s$ over finite chain ring R. Now, if the unit λ is a square in R, i.e., there exists a unit $\alpha \in R$ such that $\lambda = \alpha^2$. Then we have

$$x^{2p^s} - \lambda = x^{2p^s} - \alpha^2 = (x^{p^s} + \alpha)(x^{p^s} - \alpha).$$

By the Chinese Remainder Theorem, we get that

$$\mathcal{R}_\lambda = \frac{R[x]}{\langle x^{p^s} + \alpha\rangle} \oplus \frac{R[x]}{\langle x^{p^s} - \alpha\rangle}.$$

It implies that ideals of $\mathcal{R}_\lambda$ are of the form $A \oplus B$, where A and B are ideals of $\frac{R[x]}{\langle x^{p^s}+\alpha\rangle}$ and $\frac{R[x]}{\langle x^{p^s}-\alpha\rangle}$, respectively, i.e., they are $(-\alpha)$ and α-constacyclic codes of length p^s over R. This means that any λ-constacyclic code of length $2p^s$ over R, i.e., an ideal C of $\mathcal{R}_\lambda$, is represented as a direct sum of $C_{-\alpha}$ and C_α:

$$C = C_{-\alpha} \oplus C_\alpha,$$

where $C_{-\alpha}$ and C_α are ideals of $\frac{R[x]}{\langle x^{p^s}+\alpha\rangle}$ and $\frac{R[x]}{\langle x^{p^s}-\alpha\rangle}$, respectively. Hence, we can determine the classification, detailed structure, and number of codewords of $(-\alpha)$ and α-constacyclic codes length p^s were invertigated in [20]. Thus, when λ is a square in R, we obtain λ-constacyclic codes C of length $2p^s$ over R from that of the direct summands $C_{-\alpha}$ and C_α (see [20]). Now, we have the dual code $C^\perp$ of C including a direct sum of the the dual codes of the direct summands $C_{-\alpha}^\perp$ and $C_\alpha^\perp$.

Theorem 3.1. *Let the unit λ is a square, i.e. $\lambda = \alpha^2$ for some $\alpha \in R$, and $C = C_{-\alpha} \oplus C_{\alpha}$ be a λ-constacyclic code of length $2p^s$ over R, where $C_{-\alpha}$ and C_{α} are ideals of $\frac{R[x]}{\langle x^{p^s}+\alpha\rangle}$ and $\frac{R[x]}{\langle x^{p^s}-\alpha\rangle}$, respectively. Then*

$$C^{\perp} = C^{\perp}_{-\alpha} \oplus C^{\perp}_{\alpha}.$$

In particular, C is a self-dual constacyclic code of length $2p^s$ over R if and only if $C_{-\alpha}$ and C_{α} are self-dual $(-\alpha)$ and α-constacyclic code of length p^s over R, respectively.

Proof. We have $C^{\perp}_{-\alpha} \oplus C^{\perp}_{\alpha} \subseteq C^{\perp}$. Now, we consider

$$|C^{\perp}_{-\alpha} \oplus C^{\perp}_{\alpha}| = |C^{\perp}_{-\alpha}| \cdot |C^{\perp}_{\alpha}| = \frac{|R|^{p^s}}{|C_{-\alpha}|} \cdot \frac{|R|^{p^s}}{|C_{\alpha}|} = \frac{|R|^{2p^s}}{|C_{-\alpha}| \cdot |C_{\alpha}|} = \frac{|R|^{2p^s}}{|C|} = |C^{\perp}|.$$

Hence, $C^{\perp} = C^{\perp}_{-\alpha} \oplus C^{\perp}_{\alpha}$. □

Next, we will consider on the main case where λ is not square in R. We have the following.

Lemma 3.2. *Let R be a finite chain ring of characteristic p^a and maximal ideal $\langle z\rangle$, and λ be a unit of R. For any element $r \in R$, $x^2 - r$ is invertible in $\mathcal{R}_{\lambda}$ if and only if $\lambda - r^{p^s}$ is invertible in R. Moreover, when $x^2 - r$ is not invertible, it is nilpotent in $\mathcal{R}_{\lambda}$.*

Proof. In $\mathcal{R}_{\lambda}$, $x^{2p^s} = \lambda$, and $p \mid \binom{p^s}{i}$ for $1 \le i \le p^s - 1$, then

$$\begin{aligned}(x^2 - r)^{p^s} &= x^{2p^s} + \left[\sum_{i=1}^{p^s-1} \binom{p^s}{i} (x^2)^{p^s-i}(-r)^i\right] - r^{p^s} \\ &= (\lambda - r^{p^s}) + ph(x),\end{aligned}$$

where $h(x) = \sum_{i=1}^{p^s-1} \frac{\binom{p^s}{i}}{p} (x^2)^{p^s-i}(-r)^i$. We obtain that $x^2 - r$ is invertible in $\mathcal{R}_{\lambda}$ if and only if $(x^2-r)^{p^s}$ is invertible, which is equivalent to the condition that $\lambda - r^{p^s}$ is invertible in R. Next, suppose that $x^2 - r$ is not invertible in $\mathcal{R}_{\lambda}$, we get that $\lambda - r^{p^s}$ is not invertible in R, that is, $\lambda - r^{p^s} = z_1 z$, for some $z_1 \in R$. Since p is also not invertible in R, $p = z_2 z$, for some $z_2 \in R$. Hence,

$$(x^2 - r)^{p^s} = (\lambda - r^{p^s}) + ph(x) = z(z_1 + z_2 h(x)).$$

Therefore,

$$(x^2 - r)^{p^s N_z} = z^{N_z}(z_1 + z_2 h(x))^{N_z} = 0.$$

We have $x^2 - r$ is nilpotent in $\mathcal{R}_{\lambda}$. The proof is complete. □

Thus, we can find an element r such that $\lambda - r^{p^s}$ is nilpotent in R, for any unit λ of R.

Proposition 3.3. *Let R be a finite chain ring of characteristic p^a and maximal ideal $\langle z\rangle$, and λ be unit of R. Then there always exists an element r such that $\lambda - r^{p^s}$ is nilpotent, i.e., non-invertible, in R.*

Proof. Let $\bar{R} = R/\langle z\rangle$ be the residue field of R. Then $\bar{R}$ has cardinality a power of p, say $|\bar{R}| = q = p^m$. By Proposition 2.2, fix ξ to be an element of the multiplicative group of units of R with multiplicative order $q-1$ such that any element $\eta \in R$ can be uniquely expressed as

$$\eta = \eta_0 + \eta_1 z + \cdots + \eta_{N_z-1} z^{N_z-1},$$

where $\eta_i \in \mathcal{T} = \{0, \xi, ..., \xi^{q-2}, \xi^{q-1} = 1\}$, the Teichmüller set of R. Since λ is a unit of R, λ is uniquely expressed as

$$\lambda = l_0 + l_1 z + \cdots + l_{N_z-1} z^{N_z-1},$$

where $l_i \in \mathcal{T}$, and $l_0 \neq 0$. Note that ξ has multiplicative order $q-1$, it means that $\xi^{q-1} = 1$, i.e., $\xi^{p^m} = \xi$. Thus, for any positive integer k, $\xi^{p^{km}} = \xi$. By the Division Algorithm, there exist nonnegative integer k_q, k_r such that $s = k_q m + k_r$, and $0 \le k_r \le m-1$. Let $\xi_0 = \xi^{p^{(k_q+1)m-s}} = \xi^{p^{m-k_r}}$. Then $\xi_0^{p^s} = \xi^{p^{(k_q+1)m}} = \xi$. Since $0 \neq l_0 \in \mathcal{T}$, $l_0 = \xi^j$, for $1 \le j \le q-1$, we get that $l_0 = \xi_0^{jp^s}$. Choose $r = \xi_0^j$, we have

$$\begin{aligned}
\lambda - r^{p^s} &= \lambda - (\xi_0^j)^{p^s} \\
&= \lambda - l_0 \\
&= l_1 z + \cdots + l_{N_z-1} z^{N_z-1} \\
&= z(l_1 + \cdots + l_{N_z-1} z^{N_z-2}),
\end{aligned}$$

which is nilpotent in R. □

Now, when $\lambda - r^{p^s}$ is nilpotent in R, that is, it is not invertible, we can see that $\mathcal{R}_\lambda$ is a local ring with maximal ideal $\langle x^2 - r, z\rangle$. We start with the following observation.

Proposition 3.4. *Any nonzero linear polynomial $cx + d \in R[x]$ is invertible in $\mathcal{R}_\lambda$.*

Proof. In $\mathcal{R}_\lambda$, we have

$$(x+d)^{p^s}(x-d)^{p^s} = (x^2 - d^2)^{p^s} = x^{2p^s} - d^{2p^s} = \lambda - d^{2p^s}.$$

Since λ is not a square in R, $\lambda - d^{2p^s}$ is invertible in $\mathcal{R}_\lambda$. Thus

$$(x+d)^{-1} = (x+d)^{p^s-1}(x-d)^{p^s}(\lambda - d^{2p^s})^{-1}.$$

Therefore, for any $c \neq 0$ in R,

$$(cx+d)^{-1} = c^{-1}(x + c^{-1}d)^{-1} = (x + c^{-1}d)^{p^s-1}(x - c^{-1}d)^{p^s}(\lambda - c^{-2p^s} d^{2p^s})^{-1}.$$

The proof is complete. □

Proposition 3.5. *Let R be a finite chain ring of characteristic p^a with maximal ideal $\langle z\rangle$, and λ be a unit of R. Fix an element $r \in R$ such that $\lambda - r^{p^s}$ is not invertible, then the ambient ring $\mathcal{R}_\lambda$ is a local ring with maximal ideal $\langle x^2-r, z\rangle$.*

Proof. Let r be an element of R such that $\lambda - r^{p^s}$ is not invertible. By Lemma 3.2, we have x^2-r is nilpotent in $\mathcal{R}_\lambda$. As R is a chain ring, each element $y \in R$ can be written as $y = r_i z^i$, where r_i is a unit of R and $0 \le i \le N_z$. Let $f(x) \in \mathcal{R}_\lambda$, then $f(x)$ can be expressed as

$$f(x) = \sum_{i=0}^{p^s-1} (c_i x + d_i)(x^2-r)^i,$$

where $c_i, d_i \in R$, we can see that

$$\begin{aligned} f(x) &= (c_0x+d_0) + (x^2-r)\sum_{i=1}^{p^s-1}(c_ix+d_i)(x^2-r)^{i-1} \\ &= z^{k_0}(r_0x+r_0') + (x^2-r)\sum_{i=1}^{p^s-1}(c_ix+d_i)(x^2-r)^{i-1}, \end{aligned}$$

where $0 \le k_0 \le N_z$ and r_0, r_0' are units of R. Since both x^2-r and z are nilpotent in $\mathcal{R}_\lambda$, $f(x)$ is invertible in $\mathcal{R}_\lambda$ if and only if $k_0 = 0$. This implies that $\langle x^2-r, z\rangle$ is the set of all non-invertible elements of $\mathcal{R}_\lambda$. Therefore, $\mathcal{R}_\lambda$ is a local ring with maximal ideal $\langle x^2-r, z\rangle$. Now, we will show that $\langle x^2-r, z\rangle$ is not a principle ideal of $\mathcal{R}_\lambda$. Suppose that $z \in \langle x^2-r\rangle$. Then, there is a polynomial $f(x) = \sum_{i=0}^{p^s-1}(c_ix+d_i)(x^2-r)^i \in \mathcal{R}$ such that $z = (x^2-r)f(x)$. Hence,

$$\begin{aligned} z &= (x^2-r)\sum_{i=0}^{p^s-1}(c_ix+d_i)(x^2-r)^i \\ &= (x^2-r)\sum_{i=0}^{p^s-1} z^{k_i}(r_ix+r_i')(x^2-r)^i, \end{aligned}$$

where r_i, r_i' are units of R. Then, there exists $l \in \{0,1,2,...,p^s-1\}$ such that $k_l = 1$, it follows that $(x^2-r)(r_lx+r_l')(x^2-r)^l = 1$. This implies that x^2-r is invertible, which is a contradiction. So, $z \notin \langle x^2-r\rangle$. Obviously, $x^2-r \notin \langle z\rangle$, because $(x^2-r)^{N_z} \neq 0$ in $\mathcal{R}$, but $z^{N_z} = 0$. Thus, $\langle x^2-r, z\rangle$ is not a principle ideal of $\mathcal{R}$, which implies that $\mathcal{R}$ is not chain ring according to Proposition 2.1. □

Next, if there exists $\lambda_0 \in R$ such that $\lambda = \lambda_0^{p^s}$, setting $r = \lambda_0$, we can see that $\lambda - r^{p^s} = 0$, which is not invertible. The following result is straightforword.

Corollary 3.6. *Let λ be a unit of the chain ring R such that there exists $\lambda_0 \in R$ with $\lambda_0^{p^s} = \lambda$. Then the ambient ring $\mathcal{R}_\lambda$ is a local ring with maximal ideal $\langle x^2-\lambda_0, z\rangle$.*

It is worth noting that when there exists $\lambda_0 \in R$ such that $\lambda_0^{p^s} = \lambda$, we can establish a one-to-one correspondence between λ-constacyclic codes and cyclic codes of length $2p^s$ over R via a ring isomorphism that sends $x \mapsto \lambda_0 x$ as follows.

Proposition 3.7. *Let Φ be the map*

$$\Phi : \mathcal{R}_\lambda \to \mathcal{R}_1$$

given by

$$\Phi(f(x)) = f(\lambda_0 x).$$

Then Φ is a ring isomorphism. In particular, A is an ideal of $\mathcal{R}_\lambda$ if and only if $\Phi(A)$ is an ideal of $\mathcal{R}_1$. Equivalent, A is a λ-constacyclic code of length $2p^s$ over R if and only if $\Phi(A)$ is a cyclic code of length $2p^s$ over R.

Now, we use the nilpotency index N_z of the generator z and determine the nilpotency index of the other generator $x^2 - \lambda_0$, which is the structure of ideals of the ambient rings $\mathcal{R}_\lambda$. If k is the highest power to which p divides N, we write $p^k || N$, i.e., $p^k | N$ and $p^{k+1} \nmid N$. We will recall an important fact in number theory proven by Kummer.

Theorem 3.8. [20] (Kummer's Theorem) *For any prime p and integers $n \geq m \geq 0$, let k be the highest power to which p divides the binomial coefficient $\binom{n}{m}$, i.e., $p^k || \binom{n}{m}$. Then k is precisely the numbers of carries when adding $n - m$ and m in base p.*

Kummer's Theorem easily implies the following result.

Proposition 3.9. [20] *Let p be a prime.*

(*a*) *Assume that $p^n > t$, and $p^m || t$. Then $p^{n-m} || \binom{p^n}{t}$.*

(*b*) *For any i with $1 \leq i \leq p - 1$, $p || \binom{p^s}{ip^{s-1}}$.*

Proposition 3.10. *Let $k \geq 0$ and λ be a unit of the chain ring R such that there is an element $\lambda_0 \in R$ such that $\lambda_0^{p^s} = \lambda$. Then in $\mathcal{R}_\lambda$, there exist elements $\alpha_k(x), \beta_k(x)$ such that $\alpha_k(x)$ is invertible, $p^{k+2}(x^2 - \lambda_0) | \beta_k(x)$, and*

$$(x^2 - \lambda_0)^{p^s + k(p-1)p^{s-1}} = p^{k+1}\alpha_k(x)(x^2 - \lambda_0)^{p^{s-1}} + \beta_k(x).$$

Proof. We will prove by induction on k. When $k = 0$, we have

$$0 = x^{2p^s} - \lambda = [(x^2 - \lambda_0) + \lambda_0]^{p^s} - \lambda_0^{p^s} = \sum_{i=1}^{p^s} \binom{p^s}{i} (x^2 - \lambda_0)^i \lambda_0^{p^s - i}.$$

It implies that

$$\begin{aligned}
(x^2-\lambda_0)^{p^s} &= -\sum_{i=1}^{p^s-1}\binom{p^s}{i}(x^2-\lambda_0)^i\lambda_0^{p^s-i} \\
&= -\sum_{i=1}^{p-1}\binom{p^s}{ip^{s-1}}(x^2-\lambda_0)^{ip^{s-1}}\lambda_0^{p^s-ip^{s-1}} \\
&\quad -\sum_{i=1,p^{s-1}\nmid i}^{p^s-1}\binom{p^s}{i}(x^2-\lambda_0)^i\lambda_0^{p^s-i} \\
&= p\alpha_0(x)(x^2-\lambda_0)^{p^{s-1}}+\beta_0(x),
\end{aligned}$$

where

$$\alpha_0(x) = -\frac{1}{p}\sum_{i=1}^{p-1}\binom{p^s}{ip^{s-1}}(x^2-\lambda_0)^{(i-1)p^{s-1}}\lambda_0^{p^s-ip^{s-1}},$$

and

$$\beta_0(x) = -\sum_{i=1,p^{s-1}\nmid i}^{p^s-1}\binom{p^s}{i}(x^2-\lambda_0)^i\lambda_0^{p^s-i}.$$

By Proposition 3.9, $\alpha_0(x)$ is invertible, and $p^s(x^2-\lambda_0)\mid\beta_0(x)$. Hence, the assertion is true for $k=0$. Assume that the assertion is true for any integer up to k, we will show that it is true for $k+1$. We consider

$$\begin{aligned}
(x^2-\lambda_0)^{p^s+(k+1)(p-1)p^{s-1}} &= (x^2-\lambda_0)^{p^s+k(p-1)p^{s-1}}(x^2-\lambda_0)^{(p-1)p^{s-1}} \\
&= [p^{k+1}\alpha_k(x)(x^2-\lambda_0)^{p^{s-1}}+\beta_k(x)](x^2-\lambda_0)^{(p-1)p^{s-1}} \\
&= p^{k+1}\alpha_k(x)(x^2-\lambda_0)^{p^s}+\beta_k(x)(x^2-\lambda_0)^{(p-1)p^{s-1}} \\
&= p^{k+1}\alpha_k(x)[p\alpha_0(x)(x^2-\lambda_0)^{p^{s-1}}+\beta_0(x)] \\
&\quad +\beta_k(x)(x^2-\lambda_0)^{(p-1)p^{s-1}} \\
&= p^{k+2}\alpha_k(x)\alpha_0(x)(x^2-\lambda_0)^{p^{s-1}}+p^{k+1}\alpha_k(x)\beta_0(x) \\
&\quad +\beta_k(x)(x^2-\lambda_0)^{(p-1)p^{s-1}} \\
&= p^{k+2}\left[\alpha_k(x)\alpha_0(x)+\frac{\beta_k(x)}{p^{k+2}}(x^2-\lambda_0)^{(p-2)p^{s-1}}\right] \\
&\quad \times(x^2-\lambda_0)^{p^{s-1}}+p^{k+1}\alpha_k(x)\beta_0(x) \\
&= p^{k+2}\alpha_{k+1}(x)(x^2-\lambda_0)^{p^s-1}+\beta_{k+1}(x),
\end{aligned}$$

where

$$\alpha_{k+1}(x) = \alpha_k(x)\alpha_0(x)+\frac{\beta_k(x)}{p^{k+2}}(x^2-\lambda_0)^{(p-2)p^{s-1}},$$

and

$$\beta_{k+1}(x) = p^{k+1}\alpha_k(x)\beta_0(x).$$

Since $\alpha_0(x), \alpha_k(x)$ are invertible and $(x^2-\lambda_0) \mid \frac{\beta_k(x)}{p^{k+2}}$, we get that $\alpha_{k+1}(x)$ is also invertible. As $p^s(x^2-\lambda_0) \mid \beta_0(x)$, $p^{k+3}(x^2-\lambda_0) \mid \beta_{k+1}(x)$. The proof is complete. □

Theorem 3.11. *Let λ be a unit of the chain ring R such that there is an element $\alpha_0 \in R$ such that $\lambda_0^{p^s} = \lambda$. In R_λ, $x^2-\lambda_0$ is nilpotent with nilpotency index $ap^s-(a-1)p^{s-1}$.*

Proof. By Proposition 3.10, we put $k = a-1$, then there exist $\alpha_{a-1}(x), \beta_{a-1}(x)$ such that $\alpha_{a-1}(x)$ is invertible, $p^{a+1}(x^2-\lambda_0) \mid \beta_{a-1}(x)$, and

$$(x^2-\lambda_0)^{p^s+(a-1)(p-1)p^{s-1}} = p^a\alpha_{a-1}(x)(x^2-\lambda_0)^{p^{s-1}} + \beta_{a-1}(x) = 0.$$

Thus the nilpotency index of $x^2-\lambda_0$ is less than or equal to $p^s+(a-1)(p-1)p^{s-1} = ap^s-(a-1)p^{s-1}$. Next, we will show that $(x^2-\lambda_0)^{ap^s-(a-1)p^{s-1}-1} \neq 0$. If $a = 1$, i.e., R is a chain ring of characteristic p, then $x^2-\lambda_0$ has nilpotency index p^s, which is $ap^s-(a-1)p^{s-1}$. Next, we want to consider $a \geq 2$. Using Proposition 3.10 for $k = a-2$, then there exist $\alpha_{a-2}(x), \beta_{a-2}(x)$ such that $\alpha_{a-2}(x)$ is invertible, $p^a(x^2-\lambda_0) \mid \beta_{a-2}(x)$, and

$$\begin{aligned}(x^2-\lambda_0)^{p^s+(a-2)(p-1)p^{s-1}} &= p^{a-1}\alpha_{a-2}(x)(x^2-\lambda_0)^{p^{s-1}} + \beta_{a-2}(x)\\ &= p^{a-1}\alpha_{a-2}(x)(x^2-\lambda_0)^{p^{s-1}}.\end{aligned}$$

Therefore,

$$\begin{aligned}(x^2-\lambda_0)^{ap^s-(a-1)p^{s-1}-1} &= (x^2-\lambda_0)^{p^s+(a-1)(p-1)p^{s-1}-1}\\ &= (x^2-\lambda_0)^{p^s+(a-2)(p-1)p^{s-1}+(p-1)p^{s-1}-1}\\ &= (x^2-\lambda_0)^{p^s+(a-2)(p-1)p^{s-1}}(x^2-\lambda_0)^{(p-1)p^{s-1}-1}\\ &= p^{a-1}\alpha_{a-2}(x)(x^2-\lambda_0)^{p^{s-1}}(x^2-\lambda_0)^{(p-1)p^{s-1}-1}\\ &= p^{a-1}\alpha_{a-2}(x)(x^2-\lambda_0)^{p^s-1} \neq 0.\end{aligned}$$

The proof is complete. □

When $\lambda = 1$, $\lambda_0 = 1$, and we get the following straightforward result on $\mathcal{R}_1 = \frac{R[x]}{\langle x^2-1\rangle}$, the ambient ring of cyclic codes.

Corollary 3.12. *Let R be a finite chain ring of characteristic p^a and maximal ideal $\langle z\rangle$. The ambient ring $\mathcal{R}_1$ is a local ring with maximal ideal $\langle x^2-1, z\rangle$, and the nilpotency index of x^2-1 in $\mathcal{R}_1$ is $ap^s-(a-1)p^{s-1}$.*

Consider the case $\lambda = 1$ and p is odd prime. Hence, the hypotheses of Proposition 3.5 are satisfied, and therefore it implies that the ambient ring $R_{-1} = \frac{R[x]}{\langle x^2+1\rangle}$ is a local ring with maximal ideal $\langle x^2+1, z\rangle$. Moreover, the nilpotency index of x^2+1 in R_{-1} can still be computed as follows.

Theorem 3.13. *Let R be a finite chain ring of characteristic p^a and maximal ideal $\langle z\rangle$. The ambient ring R_{-1} is a local ring with maximal ideal $\langle x^2+1, z\rangle$. Then x^2+1 is nilpotent with nilpotency index $ap^s-(a-1)p^{s-1}$ when p is odd prime.*

We give some of classes of constacyclic codes of length $2p^s$ over special cases of the chain ring R as particular cases of our results.

Example 3.14. $R = \mathbb{F}_{p^m}+u\mathbb{F}_{p^m}, (u^2=0)$. In this case, $a=1$, $z=u$, and $N_z=2$. In 2016, Dinh [24] classified λ-constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ into two cases. If the unit λ is not a square and $\lambda=\alpha+u\beta$ for nonzero elements α,β of $\mathbb{F}_{p^m}$, it is shown that the ambient ring $(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]/\langle x^{2p^s}-(\alpha+u\beta)\rangle$ is a chain ring with the unique maximal ideal $\langle x^2-\alpha_0\rangle$ for $0\leq i\leq 2p^s$. If the unit λ is not a square and $\lambda=\gamma$ for some nonzero element γ of $\mathbb{F}_{p^m}$, such λ-constacyclic codes are classified into 4 distinct types of ideals. The detailed structures and the number of codewords of ideals in each type, and the dual of every λ-constayclic code are obtained.

Now, by Proposition 3.3, any unit λ of the chain ring R can be expressed as $\lambda=\lambda_0^{p^s}+z\omega$, where λ_0 is a unit of R, $\omega\in R$. Thus, the following result is straightforward from Proposition 3.5.

Corollary 3.15. *Let R be a unit of the chain R can always be expressed as $\langle z\rangle$, and λ be a unit of R. Expressing λ of the form $\lambda=\lambda_0^{p^s}+z\omega$, where λ_0 is a unit of R, $\omega\in R$, then the ambient ring R_λ is a local ring with maximal ideal $\langle x^2-\lambda_0, z\rangle$.*

If, in addition, ω is invertible, we can prove that $z\in\langle x^2-\lambda_0\rangle$, implying that R_λ is in deed a chain ring, as follows.

Theorem 3.16. *Let R be a finite chain ring of characteristic p^a with maximal ideal $\langle z\rangle$, and λ be a unit of R of the form $\lambda=\lambda_0^{p^s}+z\omega$, where λ_0 is a unit of R, ω are unit of R. Then $\langle(x^2-\lambda_0)^{p^s}\rangle=\langle z\rangle$, and the ambient ring $\mathcal{R}_\lambda$ is a chain ring with maximal ideals $\langle x^2-\lambda_0\rangle$, where the nilpotency index of $x^2-\lambda_0$ is p^sN_z.*

Proof. In R_λ, $x^{2p^s}=\lambda=\lambda_0^{p^s}+z\omega$, i.e., $z\omega=x^{2p^s}-\lambda_0^{p^s}$. Since $p|\binom{p^s}{i}$ for $1\leq i\leq p^s-1$, we get that

$$\begin{aligned}
z\omega &= x^{2p^s}-\lambda_0^{p^s}\\
&= [(x^2-\lambda_0)+\lambda_0]^{p^s}-\lambda_0^{p^s}\\
&= (x^2-\lambda_0)^{p^s}+\sum_{i=1}^{p^s-1}\binom{p^s}{i}(x^2-\lambda_0)^i\lambda_0^{p^s-i}\\
&= (x^2-\lambda_0)^{p^s}+p(x^2-\lambda_0)\sum_{i=1}^{p^s-1}\frac{\binom{p^s}{i}}{p}(x^2-\lambda_0)^{i-1}\lambda_0^{p^s-i}.
\end{aligned}$$

Note that p is nilpotent in the chain ring R, we have p must be in the maximal ideal $\langle z\rangle$. Then, $p = tz$ for some $t \in R$. Thus,

$$\begin{aligned}(x^2-\lambda_0)^{p^s} &= z\omega - p(x^2-\lambda_0)\sum_{i=1}^{p^s-1}\frac{\binom{p^s}{i}}{p}(x^2-\lambda_0)^{i-1}\lambda_0^{p^s-i}\\ &= z\left[\omega - t(x^2-\lambda_0)\sum_{i=1}^{p^s-1}\frac{\binom{p^s}{i}}{p}(x^2-\lambda_0)^{i-1}\lambda_0^{p^s-i}\right].\end{aligned}$$

Since ω is invertible and $x^2-\lambda_0$ is nilpotent in R_λ, $\omega - t(x^2-\lambda_0)\sum\limits_{i=1}^{p^s-1}\frac{\binom{p^s}{i}}{p}(x^2-\lambda_0)^{i-1}\lambda_0^{p^s-i}$ is invertible in $\mathcal{R}_\lambda$. Therefore, $\langle (x^2-\lambda_0)^{p^s}\rangle = \langle z\rangle$, implying the nilpotency index of $x^2-\lambda_0$ is p^sN_z. Moreover, since $z \in \langle z\rangle = \langle (x^2-\lambda_0)^{p^s}\rangle \subseteq \langle x^2-\lambda_0\rangle$, the maximal ideal $\langle x^2-\lambda_0, z\rangle$ is in fact $\langle x^2-\lambda_0\rangle$. Therefore, by Proposition 2.1, $\mathcal{R}_\lambda$ is a chain ring with maximal ideal $\langle x^2-\lambda_0\rangle$. □

Now, we can list all λ-constacyclic codes of length $2p^s$ over R and their sizes.

Proposition 3.17. *Let R be a finite chain ring of characteristic p^a with maximal ideal $\langle z\rangle$, and λ be a unit of R of the form $\lambda = \lambda_0^{p^s} + z\omega$, where λ_0 and ω are units of R. There are p^sN_z+1 λ-constacyclic codes of length $2p^s$ over R, they are precisely the ideal $\langle (x^2-\lambda_0)^i\rangle$, where $0 \le i \le p^sN_z$, of the chain ring R_λ. Each λ-constacyclic code $\langle (x^2-\lambda_0)^i\rangle$ contains $|\bar{R}|^{p^sN_z-i}$ codewords, where $\bar{R} = \frac{R}{\langle z\rangle}$ is the residue field of R.*

By Proposition 2.4, the dual of a λ-constacyclic code is a λ^{-1}-constacyclic code. So, we want to determine the duals of λ-constacyclic codes. Firstly, we must obtain λ^{-1} for $\lambda = \lambda_0^{p^s} + z\omega$, where λ_0 and ω are units of R. Let k be the integer such that $2^k < N_z \le 2^{k+1}$, we have

$$\begin{aligned}&(\lambda_0^{p^s}+z\omega)(\lambda_0^{p^s}-z\omega)((\lambda_0^{p^s})^2+(z\omega)^2)((\lambda_0^{p^s})^{2^2}+(z\omega))^{2^2}\cdots((\lambda_0^{p^s})^{2^k}+(z\omega)^{2^k})\\ &= ((\lambda_0^{p^s})^2-(z\omega)^2)((\lambda_0^{p^s})^2+(z\omega)^2)((\lambda_0^{p^s})^{2^2}+(z\omega))^{2^2}\cdots((\lambda_0^{p^s})^{2^k}+(z\omega)^{2^k})\\ &\ \vdots\\ &= ((\lambda_0^{p^s})^{2^k}-(z\omega)^{2^k})((\lambda_0^{p^s})^{2^k}+(z\omega)^{2^k})\\ &= ((\lambda_0^{p^s})^{2^{k+1}}-(z\omega)^{2^{k+1}})\\ &= (\lambda_0^{p^s})^{2^{k+1}}.\end{aligned}$$

That means,

$$\lambda(\lambda_0^{p^s}-z\omega)\prod_{i=1}^{k}(\lambda_0^{2^ip^s}+z^{2^i}\omega^{2^i}) = \lambda_0^{2^{k+1}p^s}.$$

Thus,

$$\lambda^{-1} = \lambda_0^{-2^{k+1}p^s}(\lambda_0^{p^s}-z\omega)\prod_{i=1}^{k}(\lambda_0^{2^ip^s}+z^{2^i}\omega^{2^i}).$$

Viewing λ^{-1} as a polynomial of z, say $\lambda^{-1} = g(z) = g_0 + g_1 z + g_2 z^2 + \cdots$, we have

$$\begin{aligned} g_0 &= \lambda_0^{-2^{k+1}p^s} \prod_{i=1}^{k} \lambda_0^{2^i p^s} \\ &= \lambda_0^{-2^{k+1}p^s} \lambda_0^{p^s \sum_{i=0}^{k} 2^i} \\ &= \lambda_0^{-2^{k+1}p^s} \lambda^{p^s(2^{k+1}-1)} \\ &= \lambda_0^{-p^s}, \end{aligned}$$

and

$$\begin{aligned} g_1 &= -\omega\lambda_0^{-2^{k+1}p^s} \prod_{i=1}^{k} \lambda_0^{2^i p^s} \\ &= \lambda_0^{-2^{k+1}p^s} \lambda_0^{p^s \sum_{i=0}^{k} 2^i} \\ &= \lambda_0^{-2^{k+1}p^s} \lambda^{p^s(2^{k+1}-2)} \\ &= -\omega\lambda_0^{-2p^s}. \end{aligned}$$

We can see that g_1 is invertible, and so, λ^{-1} can be expressed as $\lambda^{-1} = (\lambda_0^{-1})^{p^s} + z\omega'$, for some unit ω' of R. By Theorem 3.16 and Proposition 3.17, the following results about λ^{-1}-constacyclic codes of length $2p^s$ over R are obtained.

Theorem 3.18. *Let R be a finite chain ring of characteristic p^a with maximal ideal $\langle z\rangle$ and λ be a unit of R of the form $\lambda = \lambda_0^{p^s} + z\omega$, where λ_0 and ω are units of R. Then*

- (*a*) $\lambda^{-1} = (\lambda_0^{-1})^{p^s} + z\omega'$ *of R.*
- (*b*) *In $R_{\lambda^{-1}}, \langle (x^2 - \lambda_0^{-1})^{p^s}\rangle = \langle z\rangle$, and the ambient ring $R_{\lambda^{-1}}$ is a chain ring with maximal ideals $\langle (x^2 - \lambda_0^{-1})^{p^s}\rangle$, where the nilpotency index of $x^2 - \lambda_0^{-1}$ is $p^s N_z$.*
- (*c*) *There are $p^s N_z + 1$ λ^{-1}-constacyclic codes of length $2p^s$ over R, they are precisely the ideals $\langle (x^2 - \lambda_0^{-1})^i\rangle$, where $0 \leq i \leq p^s N_z$, of the chain ring $R_{\lambda^{-1}}$. Each λ^{-1}-constacyclic code $\langle (x^2 - \lambda_0^{-1})^i\rangle \subseteq R_{\lambda^{-1}}$ contains $|\bar{R}|^{p^s N_z - i}$ codewords, where $\bar{R} = \frac{R}{\langle z\rangle}$ is the residue field of R.*

For a λ-constacyclic code of legnth $2p^s$ over R, $C = \langle (x^2 - \lambda_0)^i\rangle \subseteq \mathcal{R}_\lambda$, by Proposition 3.17, $|C| = |\bar{R}|^{p^s N_z - i}$. By Proposition 2.5, the number of codewords in the dual $C^\perp$ is

$$|C^\perp| = \frac{|\bar{R}|^{p^s}}{|C|} = \frac{|\bar{R}|^{p^s N_z}}{|\bar{R}|^{p^s N_z - i}} = |\bar{R}|^i.$$

On the other hand, since $C^\perp$ is a λ^{-1}-constacyclic code of length $2p^s$ over R, by Theorem 3.18, $C^\perp$ is an ideal of the chain ring $R_{\lambda^{-1}}$, of the form $C^\perp = \langle (x^2 - \lambda_0^{-1})^i\rangle \subseteq R_{\lambda^{-1}}$ which contains $|\bar{R}|^{p^s N_z - j}$ codewords. Hence, $p^s N_z - j = i$, i.e., $j = p^s N_z - i$. Therefore, $C^\perp = \langle (x^2 - \lambda_0)^{p^s N_z - i}\rangle \subseteq R_{\lambda^{-1}}$. Thus, we have the following result.

Corollary 3.19. *Let R be a finite chain ring of characterstic p^a with maximal ideal $\langle z\rangle$, residue field $\bar{R} = \frac{R}{\langle z\rangle}$, and λ be a unit of the form $\lambda = \lambda_0^{p^s} + z\omega$, where λ_0 and ω are units of R. Let C be a λ-constacyclic code of length $2p^s$ over R, then $C = \langle (x^2 - \lambda_0)^i\rangle \subseteq R_\lambda$, where $0 \leq i \leq p^sN_z$, that contains $|\bar{R}|^{p^sN_z - i}$ codewords. The dual $C^\perp$ is the λ^{-1}-constacyclic code $C^\perp = \langle (x^2 - \lambda_0^{-1})^{p^sN_z - i}\rangle \subseteq R_{\lambda^{-1}}$, which contains $|\bar{R}|^i$ codewords.*

Comparing the sizes of C and $C^\perp$, we have $|C| = |C^\perp|$ if and only if $p^sN_z = 2i$. So if N_z and p are odd, $C \neq C^\perp$. If N_z is even, $|C| = |C^\perp|$ if and only if $i = p^sN_z/2$, and thus,

$$C = \langle (x^2 - \lambda_0)^{p^sN_z/2}\rangle = \langle z^{N_z/2}\rangle \subseteq R_\lambda,$$
$$C^\perp = \langle (x^2 - \lambda_0^{-1})^{p^sN_z/2}\rangle = \langle z^{N_z/2}\rangle \subseteq R_{\lambda^{-1}}.$$

As both $\langle z^{N_z/2}\rangle \subseteq R_\lambda$ and $\langle z^{N_z/2}\rangle \subseteq R_{\lambda^{-1}}$ are in fact $\langle z^{N_z/2}\rangle^{p^s} \subset R^{p^s}$, it follows that, in this case

$$C = C^\perp = \langle z^{N_z/2}\rangle^{p^s} \subset R^{p^s}.$$

We summarize this result about self-dual codes, as follows.

Corollary 3.20. *Let R be a finite chain ring of characteristic p^a with maximal ideal $\langle z\rangle$, and λ be a unit of R of the form $\lambda = \lambda_0^{p^s} + z\omega$, where λ_0 and ω are units of R. If N_z and p are odd, then self-dual λ-constacyclic codes of length $2p^s$ over R do not exist. If N_z is even, then $\langle z^{N_z/2}\rangle \subset R^{p^s}$ is the unique self-dual λ-constacyclic codes of length $2p^s$ over R.*

4 Conclusion

We study λ-constacyclic codes of length $2p^s$ over a finite commutative chain ring R. If the unit λ is a square in R, i.e., $\lambda = \alpha^2$, for some unit α of R, then every λ-constacyclic codes of length $2p^s$ over R can be represented as a direct sum of an $(-\alpha)$-constacyclic code and an α-constacyclic code of length p^s over R. In the main case, the unit λ is not a square, the rings $\mathcal{R}_\lambda = \frac{R[x]}{\langle x^{2p^s} - \lambda\rangle}$ is a local ring with maximal ideal $\langle x^2 - r, z\rangle$, where $r \in R$ such that $\lambda - r^{p^s}$ is not invertible. When there exists a unit λ_0 of R such that $\lambda = \lambda_0^{p^s}$, we prove that $x^2 - \lambda_0$ is nilpotent with nilpotency index $ap^s - (a-1)p^{s-1}$. When $\lambda = \lambda_0^{p^s} + z\omega$, for some unit ω of R, we show that $\mathcal{R}_\lambda$ is also a chain ring with maximal ideals $\langle x^2 - \lambda_0\rangle$. Furthermore, the algebraic structure and dual of all λ-constacyclic codes are obtained. It is interesting to see other type of a unit λ and study all λ-constacyclic code of np^s over finite commutative chian ring R with identity.

Acknowledgements : The authors have greatly benefited from the referees report and would like to thank referees for their valuable comments and kindly suggestion, which have considerably contributed to the improvement of this work. Furthermore, the authors would like to thank Science Achievement Scholarship of Thailand, which provides supporting for research.

References

[1] S.D. Berman, Semisimple cyclic and Abelian codes. II, Kibernetika (Kiev) 3 (1967) 21-30 (Russian). English translation: Cybernetics 3 (1967) 17-23.

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

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

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

[5] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, 2010.

[6] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, 10th Impression, North-Holland, Amsterdam, 1998.

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

[8] T. Abualrub, A. Ghrayeb, R. Oehmke, A mass formula and rank of $\mathbb{Z}_4$ cyclic codes of length 2^e, IEEE Trans. Inf. Theory 50 (2004) 3306-3312.

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

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

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

[12] H.Q. Dinh, Complete distances of all negacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$, IEEE Trans. Inf. Theory 53 (2007) 147-161.

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

[14] H.Q. Dinh, On some classes of repeated-root constacyclic codes of length a power of 2 over Galois rings, Trends Math. (2010) 131-147.

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

[16] H.M. Kiah, K.H. Leung, S. Ling, Cyclic codes over $\mathrm{GR}(p^2, m)$ of length p^k, Finite Fields Appl. 14 (2008) 834-846.

[17] E. Kleinfeld, Finite Hjelmslev planes, Ill. J. Math. 3 (1959) 403-407.

[18] G. Norton, A. Sălăgean-Mandache, On the structure of linear cyclic codes over finite chain rings, Appl. Algebra Eng. Commun. Comput. 10 (2000) 489-506.

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

[20] H.Q. Dinh, H.D. Nguyen, S. Sriboonchitta, T.M. Vo, Repeated-root constacyclic codes of prime power lengths finite chain rings, Finite Feilds Appl. 43 (2017) 22-47.

[21] H.Q. Dinh, S.R. López-Permouth, Cyclic and Negacyclic Codes over Finite Chain Rings, IEEE Trans. Inform. Theory 50 (2004) 1728-1744.

[22] B.R. McDonald, Finite Rings with Identity, Marcel Dekker Incorporated, 1974.

[23] V. Pless, W.C. Huffman, Handbook of Coding Theory, Elsevier, Amsterdam, 1998.

[24] B. Chen, H.Q. Dinh, H. Liu, L. Wang, Constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, Finite Fields Appl. 37 (2016) 108-130.

(Received 23 December 2017)
(Accepted 3 June 2019)