Southeast-Asian J. of Sciences Vol. 5, No. 1 (2017)pp. 22-31

$\Lambda + u^2\Lambda_2$ - CONSTACYCLIC CODES OF LENGTH $2 \cdot 5^s$ OVER $\mathbb{F}_{5^m} + u\mathbb{F}_{5^m} + u^2\mathbb{F}_{5^m}$

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 the class of Λ-constacyclic codes of length $2\cdot 5^s$ over the finite commutative chain ring $\mathcal{R}_3 = \frac{\mathbb{F}_{5^m}[u]}{\langle u^3\rangle} = \mathbb{F}_{5^m} + u\mathbb{F}_{5^m} + u^2\mathbb{F}_{5^m}$, for all units Λ of $\mathcal{R}_3$ that have the form $\Lambda = \Lambda_0 + u^2\Lambda_2$, where $\Lambda_0, \Lambda_2 \in \mathbb{F}_{5^m}$, $\Lambda_0 \neq 0$, $\Lambda_2 \neq 0$. The algebraic structures and duals of all Λ-constacyclic codes of length $2\cdot 5^s$ over $\mathcal{R}_3$ are established.

1. Introduction

The classes of cyclic and negacyclic codes in particular, and constacyclic codes in general, play a very significant role in the theory of error-correcting codes. Let $\mathbb{F}$ be a finite field of characteristic p and λ be a nonzero element of $\mathbb{F}$. λ-constacyclic codes of length n over $\mathbb{F}$ are classified as the ideals $\langle g(x)\rangle$ of the quotient ring $\mathbb{F}[x]/\langle x^n - \lambda\rangle$, where the generator polynomial $g(x)$ is the unique monic polynimial of minimum degree in the code, which is a divisor of $x^n - \lambda$.

In fact, cyclic codes are the most studied of all codes. Many well known codes, such as BCH, Kerdock, Golay, Reed-Muller, Preparata, Justesen, and binary Hamming codes, are either cyclic codes or constructed from cyclic codes. Cyclic codes over finite fields were first studied in the late 1950s by Prange [33], while negacyclic codes over finite fields were initiated by Berlekamp in the late 1960s [4], [5]. 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

Key words: Constacyclic codes, dual codes, chain rings.

since 1967 by Berman [6], and then in the 1970s and 1980s by several authors such as Massey et al. [28], Falkner *et al.* [23], Roth and Seroussi [38]. However, repeated-root codes were investigated in the most generality in the 1990's by Castagnoli *et al.* [10], and van Lint [42], 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.

After the realization in the 1990's [9, 24, 30] by Nechaev and Hammons *et al.*, codes over $\mathbb{Z}_4$ in particular, and codes over finite rings in general, has developed rapidly in recent decade years. Constacyclic codes over a finite commutative chain ring have been studied by many authors (see, for example, [1], [7], [31], and [39]). The structure of constacyclic codes is also investigated over a special family of finite chain rings of the form $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. For example, the structure of $\frac{\mathbb{F}_2[u]}{\langle u^2\rangle}$ is interesting, because this ring lies between $\mathbb{F}_4$ and $\mathbb{Z}_4$ in the sense that it is additively analogous to $\mathbb{F}_4$, and multiplicatively analogous to $\mathbb{Z}_4$. Codes over $\frac{\mathbb{F}_2[u]}{\langle u^2\rangle}$ have been extensively studied by many researchers, whose work includes cyclic and self-dual codes [2], decoding of cyclic codes [3], Type II codes [20], duadic codes [27], repeated-root constacyclic codes [13].

2. Preliminaries

Let R be a finite commutative ring. An ideal I of 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 has a unique maximal ideal. Furthermore, a ring R is called a *chain ring* if the set of all ideals of R is a chain under set-theoretic inclusion. The following equivalent conditions are well-known for the class of finite commutative chain rings (cf. [18, Proposition 2.1]).

The following equivalent conditions are well-known for the class of finite commutative chain rings.

Proposition 2.1. (cf. [18, Proposition 2.1]) *For a finite commutative ring R the following conditions are equivalent:*
(i) R is a local ring and the maximal ideal M of R is principal;
(ii) R is a local principal ideal ring;
(iii) R is a chain ring.

The following result is a well-known fact about finite commutative chain rings.

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

(i) For some prime p and positive integers $k, l (k \geq l), |R| = p^k, |\bar{R}| = p^l$, and the characteristic of R and $\bar{R}$ are powers of p;
(ii) For $i = 0, 1, \ldots, t, |\langle a^i \rangle| = |\bar{R}|^{t-i}$. In particular, $|R| = |\bar{R}|^t$, i.e., $k = lt$.

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

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

evaluated in R. Two words 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 said to be *self-orthogonal* if $C \subseteq C^\perp$, and it is said to be *self-dual* if $C = C^\perp$. The following result is appeared in [18].

Proposition 2.3. *Let 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, $0 \leq k \leq \alpha n$. Moreover, the dual code $C^\perp$ has $p^{\alpha n - k}$ codewords, so that $|C| \cdot |C^\perp| = |R|^n$.*

Given an n-tuple $(x_0, x_1, \ldots, x_{n-1}) \in R^n$, the *cyclic shift* τ and *negashift* ν on R^n are defined as usual, i.e.,

$$\tau(x_0, x_1, \ldots, x_{n-1}) = (x_{n-1}, x_0, x_1, \cdots, x_{n-2}),$$

and

$$\nu(x_0, x_1, \ldots, x_{n-1}) = (-x_{n-1}, x_0, x_1, \cdots, x_{n-2}).$$

A code C is called *cyclic* if $\tau(C) = C$, and C is called *negacyclic* if $\nu(C) = C$. More generally, if λ is a unit of the ring R, then the λ-*constacyclic* (λ-twisted) *shift* τ_λ on R^n is the shift

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

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. From this definition, when $\lambda = 1$, λ-constacyclic codes are cyclic codes, and when $\lambda = -1$, λ-constacyclic codes are just negacyclic codes.

Each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, 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 this, the following fact is straightforward:

Proposition 2.4. *A linear code C of length n is λ-constacyclic over R if and only if C is an ideal of $\frac{R[x]}{\langle x^n-\lambda\rangle}$.*

We knew that the dual of a cyclic code is a cyclic code, and the dual of a negacyclic code is a negacyclic code. In general, the dual of a λ-constacyclic code is a λ^{-1}-constacyclic code. (see, for example, [14], [16]).

The following result is also a fact appeared in [14].

Proposition 2.5. *Let R be a finite commutative ring, λ be a unit of R and*

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

Then $a(x)b(x) = 0$ in $\frac{R[x]}{\langle x^n-\lambda\rangle}$ 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 λ^{-1}-constacyclic shifts.

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

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

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

For a polynomial f of degree k, the polynomial $x^k f(x^{-1})$ is called a *reciprocal polynomial* of polynomial f. The reciprocal polynomial of f will be denoted by f^*. Suppose that $f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + a_kx^k$. Then $f^*(x) = x^k(a_0+a_1x^{-1}+\cdots+a_{k-1}x^{-(k-1)}+a_kx^{-k}) = a_k+a_{k-1}x+\cdots+a_1x^{k-1}+a_0x^k$. Note that $(f^*)^* = f$ 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. Since the dual of a λ-constacyclic code is a λ^{-1}-constacyclic code, $C^\perp$ is a λ^{-1}-constacyclic codes of length n over R, and hence, $C^\perp$ is an ideal of the ring $\frac{R[x]}{\langle x^n-\lambda^{-1}\rangle}$, by Proposition 2.4. It is clear that $\operatorname{ann}^*(C)$ is also an ideal of $\frac{R[x]}{\langle x^n-\lambda^{-1}\rangle}$. Therefore, applying Proposition 2.5, we can conclude that $g(x) \in \operatorname{ann}^*(C)$ if and only if $g(x) = f^*(x)$ for some $f(x) \in \operatorname{ann}(C)$, if and only if $g(x) \in C^\perp$. Then, we have a following result.

Proposition 2.6. *Let R be a finite commutative ring, and λ be a unit of R. Assume that C is a λ-constacyclic code of length n over R. Then the dual $C^\perp$ of C is $\operatorname{ann}^*(C)$.*

3. $\Lambda + u^2\Lambda_2$-constacyclic codes of length $2 \cdot 5^s$ over $\mathbb{F}_{5^m} + u\mathbb{F}_{5^m} + u^2\mathbb{F}_{5^m}$

In this paper, we study $\Lambda + u^2\Lambda_2$-constacyclic codes of length $2 \cdot 5^s$ over $\mathbb{F}_{5^m} + u\mathbb{F}_{5^m} + u^2\mathbb{F}_{5^m}$ and its dual, where $\Lambda = \Lambda_0 + u^2\Lambda_2$ is a unit of $\mathbb{F}_{5^m} + u\mathbb{F}_{5^m} + u^2\mathbb{F}_{5^m}$. By Proposition 2.4, we know that these codes are ideals of the ring

$$\mathcal{S}_a(s, \Lambda) = \frac{\mathcal{R}_a[x]}{\langle x^{2\cdot 5^s} - \Lambda \rangle}.$$

We can see that $(\Lambda_0 + u^2\Lambda_2)^{5^m} = \Lambda_0^{5^m} + u^{2\cdot 5^m}\Lambda_2^{5^m} = \Lambda_0^{5^m} = \Lambda_0$. This follows that $\Lambda^{5^m}\Lambda_0^{-1} = 1$. Hence, $\Lambda^{-1} = \Lambda^{5^m-1}\Lambda_0^{-1}$. We have $\Lambda^{5^m-1} = (\Lambda_0 + u^2\Lambda_2)^{5^m-1} = \Lambda_0^{5^m-1} + u^2\Lambda_2(5^m - 1) = 1 + u^2\Lambda_2(5^m - 1)$, implying that $\Lambda^{-1} = \Lambda_0^{-1} + u^2\Lambda_2'$.

If the unit Λ is a square in $\mathbb{F}_{5^m} + u\mathbb{F}_{5^m} + u^2\mathbb{F}_{5^m}$, i.e., there exists a unit $\beta \in \mathbb{F}_{5^m} + u\mathbb{F}_{5^m} + u^2\mathbb{F}_{5^m}$ such that $\Lambda = \beta^2$. Then we have

$$x^{2\cdot 5^s} - \Lambda = x^{2\cdot 5^s} - \beta^2 = (x^{5^s} + \beta)(x^{5^s} - \beta).$$

Applying the Chinese remainder theorem, we can see that

$$\mathcal{S}_3(s, \Lambda) = \frac{\mathcal{R}_3[x]}{\langle x^{5^s} + \beta \rangle} \oplus \frac{\mathcal{R}_3[x]}{\langle x^{5^s} - \beta \rangle}.$$

This follows that all ideals of $\mathcal{S}_3(s, \Lambda)$ are of the form $A \oplus B$, where A and B are ideals of $\frac{\mathcal{R}_a[x]}{\langle x^{5^s} + \beta \rangle}$ and $\frac{\mathcal{R}_3[x]}{\langle x^{5^s} - \beta \rangle}$, respectively, i.e., they are $-\beta$- and β-constacyclic codes of length 5^s over $\mathcal{R}_3$. Hence, if Λ is a square in $\mathcal{R}_3$, a $\Lambda_0 + u^2\Lambda_2$-constacyclic code of length $2 \cdot 5^s$ over $\mathcal{R}_3$ is expressed as a direct sum of C_+ and C_-:

$$C = C_+ \oplus C_-,$$

where C_+ and C_- are ideals of $\frac{\mathcal{R}_3[x]}{\langle x^{5^s} + \beta \rangle}$ and $\frac{\mathcal{R}_3[x]}{\langle x^{5^s} - \beta \rangle}$, respectively. The classification, detailed structure, and number of codewords of α and $-\alpha$ constacyclic codes length 5^k were investigated in [40]. Thus, when Λ is a square in $\mathcal{R}_3$, we can obtain Λ-constacyclic codes C of length $2 \cdot 5^s$ over $\mathcal{R}_3$ from that of the direct summands C_+ and C_- (cf. [40]). Hence, we can prove that the dual code $C^\perp$ of C is also a direct sum of the dual codes of the direct summand $C_+^\perp$ and $C_-^\perp$.

Theorem 3.1. *Let the unit $\Lambda = \beta^2 \in \mathbb{F}_{5^m} + u\mathbb{F}_{5^m} + u^2\mathbb{F}_{5^m}$, and $C = C_+ \oplus C_-$ be a constacyclic code of length $2 \cdot 5^s$ over $\mathbb{F}_{5^m} + u\mathbb{F}_{5^m} + u^2\mathbb{F}_{5^m}$, where C_+, C_- are ideals of $\frac{\mathcal{R}_3[x]}{\langle x^{5^s} + \beta \rangle}$, $\frac{\mathcal{R}_3[x]}{\langle x^{5^s} - \beta \rangle}$, respectively. Then*

$$C^\perp = C_+^\perp \oplus C_-^\perp.$$

In particular, C is a self-dual constacyclic code of length $2\cdot 5^s$ over $\mathbb{F}_{5^m}+u\mathbb{F}_{5^m}+u^2\mathbb{F}_{5^m}$ if and only if C_+, C_- are self-dual $-\beta$-constacyclic code and self-dual β-constacyclic code of length 5^s over $\mathbb{F}_{5^m}+u\mathbb{F}_{5^m}+u^2\mathbb{F}_{5^m}$, respectively.

Proof. It is easy to verify that $C_+^\perp \oplus C_-^\perp \subseteq C^\perp$. On the other hand,

$$|C_+^\perp \oplus C_-^\perp| = |C_+^\perp|\cdot|C_-^\perp| = \frac{|\mathcal{R}_3|^{5^s}}{|C_+|}\cdot\frac{|\mathcal{R}_3|^{p^s}}{|C_-|} = \frac{|\mathcal{R}_3|^{5^s}}{|C_+|\cdot|C_-|} = \frac{|\mathcal{R}_3|^{5^s}}{|C|} = |C^\perp|.$$

This implies that $C^\perp = C_+^\perp \oplus C_-^\perp$. □

Therefore, we only need to concentrate on the main case where Λ is not a square in $\mathbb{F}_{5^m}+u\mathbb{F}_{5^m}+u^2\mathbb{F}_{5^m}$. We first start by characterizing this condition.

Proposition 3.2. *Let $\Lambda = \Lambda_0 + u^2\Lambda_2$, $\Lambda_0, \Lambda_2 \in \mathbb{F}_{5^m}$, $\Lambda_0 \neq 0$, $\Lambda_2 \neq 0$, be a unit of $\Lambda_0 + u^2\Lambda_2$ of $\mathbb{F}_{5^m}+u\mathbb{F}_{5^m}+u^2\mathbb{F}_{5^m}$. Then Λ is not a square if and only if Λ_0 is not a square.*

Proof. Suppose that $\Lambda_0'^2 = \Lambda_0$, we consider $(\Lambda_0' + u\Lambda_1' + u^2\Lambda_2')^2$, where $\Lambda_i' \in \mathbb{F}_{p^m}$. Assume that $(\Lambda_0' + u\Lambda_1' + u^2\Lambda_2')^2 = \Lambda_0 + u^2\Lambda_2$. Then we have $\Lambda_0'^2 + 2\Lambda_0'\Lambda_1'u + 2\Lambda_0'\Lambda_2' + u^2\Lambda_1'^2 + 2u^3\Lambda_1'\Lambda_2'^4\Lambda_2'^2 = \Lambda_0 + u^2\Lambda_2$. Comparing coefficients, we have

$$\Lambda_0 = \Lambda_0'^2, 2\Lambda_0'\Lambda_1' = 0, \Lambda_2 = \Lambda_1'^2 + 2\Lambda_0'\Lambda_2'.$$

Since $\Lambda_0' \neq 0$, we must have $\Lambda_1' = 0$. By hypothesis, $\Lambda_0'^{-1}$ exists, we can compute $\Lambda_2' = 2^{-1}\Lambda_0'^{-1}\Lambda_2$.

From this, we can prove the following result.

Proposition 3.3. *Any nonzero linear polynomial $cx+d \in \mathbb{F}_{5^m}[x]$ is invertible in $\mathcal{S}_3(s,\Lambda)$.*

Proof. In $\mathcal{S}_3(s,\Lambda)$, we have

$$(x+d)^{5^s}(x-d)^{5^s} = (x^2-d^2)^{5^s} = x^{2\cdot 5^s} - d^{2\cdot 5^s} = (\Lambda_0 - d^{2\cdot 5^s}) + u^2\Lambda_2.$$

Since Λ_0 is not a square in $\mathbb{F}_{5^m}$, $\Lambda_0 - d^{2\cdot 5^s}$ is invertible in $\mathbb{F}_{5^m}$. This follows that $(\Lambda_0 - d^{2\cdot 5^s}) + u^2\Lambda_2$ is invertible in $\mathcal{S}_3(s,\Lambda)$. Thus,

$$(x+d)^{-1} = (x+d)^{5^s-1}(x-d)^{5^s}(\Lambda_0 - d^{2\cdot 5^s} + u^2\Lambda_2)^{-1}.$$

Therefore, for any $c \neq 0$ in $\mathbb{F}_{5^m}$,

$$(cx+d)^{-1} = c^{-1}(x+c^{-1}d)^{-1} = (x+c^{-1}d)^{5^s-1}(x-c^{-1}d)^{5^s}(\Lambda_0 - c^{-2\cdot 5^s}d^{2\cdot 5^s} + u^2\Lambda_2)^{-1}. \square$$

Since $\Lambda_0 \in \mathbb{F}_{5^m}$, we have $\Lambda_0^{5^{tm}} = \Lambda_0$, for any positive integer t. By the Division Algorithm, there exist nonnegative integers α_q, α_r such that $s = \alpha_q m + \alpha_r$, and $0 \leq \alpha_r \leq m-1$. Let $\alpha_0 = \Lambda_0^{5^{(\alpha_q+1)m-s}} = \Lambda_0^{5^{m-\alpha_r}}$. Then

$\alpha_0^{5^s} = \Lambda_0^{5^{(\alpha_q+1)m}} = \Lambda_0$. The following provides the key to prove that the ring $\mathcal{S}_3(s, \Lambda)$ is a chain ring.

Lemma 3.4. *In $\mathcal{S}_3(s, \Lambda)$, we have $\langle (x^2 - \alpha_0)^{5^s} \rangle = \langle u \rangle$. In particular, $x^2 - \alpha_0$ is nilpotent with nipotency index $3 \cdot 5^s$.*

Proof. The results follow from the fact that in $\mathcal{S}_3(s, \Lambda)$, $(x^2 - \alpha_0)^{5^s} = x^{2\cdot 5^s} - \Lambda_0 = u\Lambda_1 + u^2\Lambda_2$. □

Any element $f(x)$ of $\mathcal{S}_3(s, \Lambda)$ can be expressed as a polynomial of degree up to $2 \cdot 5^s - 1$ of $\mathcal{R}_3[x]$, and so $f(x) = f_1(x) + uf_2(x) + u^2 f_3(x)$, where $f_1(x), f_2(x), f_3(x)$ are polynomials of degrees up to $2 \cdot 5^s - 1$ of $\mathbb{F}_{5^m}[x]$. Thus, $f(x)$ can be uniquely represented as

$$\begin{aligned} f(x) &= \sum_{i=0}^{5^s-1} (c_{0i}x + d_{0i})(x^2 - \alpha_0)^i + u \sum_{i=0}^{5^s-1} (c_{1i}x + d_{1i})(x^2 - \alpha_0)^i \\ &\qquad + u^2 \sum_{i=0}^{5^s-1} (c_{3i}x + d_{3i})(x^2 - \alpha_0)^i \\ &= (c_{00}x + d_{00}) + (x^2 - \alpha_0) \sum_{i=1}^{5^s-1} (c_{0i}x + d_{0i})(x^2 - \alpha_0)^{i-1} \\ &\qquad + u \sum_{i=0}^{5^s-1} (a_{1i}x + b_{1i})(x^2 - \alpha_0)^i + u^2 \sum_{i=0}^{5^s-1} (c_{3i}x + d_{3i})(x^2 - \alpha_0)^i, \end{aligned}$$

where $c_{0i}, d_{1i}, c_{0i}, d_{1i} \in \mathbb{F}_{5^m}$. By Lemma 3.4, $u \in \langle x^2 - \alpha_0 \rangle$, and so $f(x)$ can be written as

$$f(x) = (c_{00}x + d_{00}) + (x^2 - \alpha_0)g(x).$$

Thus, $f(x)$ is non-invertible if and only if $c_{00} = d_{00} = 0$, i.e., $f(x) \in \langle x^2 - \alpha_0 \rangle$. It means that $\langle x^2 - \alpha_0 \rangle$ forms the set of all non-invertible elements of $\mathcal{R}_a$. Thus, $\mathcal{S}_3(s, \Lambda)$ is a local ring with maximal ideal $\langle x^2 - \alpha_0 \rangle$, hence, by Proposition 2.1, $\mathcal{S}_3(s, \Lambda)$ is a chain ring. We summarize the discussion above in the following theorem.

Theorem 3.5. *The ring $\mathcal{S}_3(s, \Lambda)$ is a chain ring with maximal ideal $\langle x^2 - \alpha_0 \rangle$, whose ideals are*

$$\mathcal{S}_3(s, \Lambda) = \langle 1 \rangle \supsetneq \langle x^2 - \alpha_0 \rangle \supsetneq \cdots \supsetneq \langle (x^2 - \alpha_0)^{3\cdot 5^s - 1} \rangle \supsetneq \langle (x^2 - \alpha_0)^{3\cdot 5^s} \rangle = \langle 0 \rangle.$$

From Theorem 3.5, we now can give the structure of $\Lambda_0 + u^2\Lambda_2$-constacyclic codes of length $2 \cdot 5^s$ over $\mathcal{R}_3$, and their sizes as follows.

Theorem 3.6. *$\Lambda_0 + u^2\Lambda_2$-constacyclic codes of length $2 \cdot 5^s$ over $\mathcal{R}_3$ are precisely the ideals $\langle (x^2 - \alpha_0)^i \rangle \subseteq \mathcal{R}_3$, where $0 \le i \le 3 \cdot 5^s$. Each $\Lambda_0 + u^2\Lambda_2$-constacyclic code $\langle (x^2 - \alpha_0)^i \rangle$ has $5^{2m(3\cdot 5^s - i)}$ codewords.*

For a $\Lambda_0 + u^2\Lambda_2$-constacyclic code $C = \langle (x^2 - \alpha_0)^i \rangle \subseteq \mathcal{R}_3$ of length $2 \cdot 5^s$ over $\mathcal{R}_3$, by Proposition 2.5 and Proposition 2.10, its dual $C^\perp$ is a $\Lambda_0 + u^2\Lambda_2$-constacyclic code of length $2 \cdot 5^s$ over $\mathcal{R}_3$. This means

$$C^\perp \subseteq \mathcal{S}_3(s, \Lambda^{-1}) = \frac{\mathcal{R}_3[x]}{\langle x^{2\cdot 5^s} - \Lambda^{-1} \rangle}.$$

Hence, Lemma 3.4 and Theorem 3.5 are applicable for $C^\perp$ and $\mathcal{S}_3(s, \Lambda^{-1})$. Therefore, similar to the case of $\mathcal{S}_3(s, \Lambda)$, we can prove that $\mathcal{S}_3(s, \Lambda^{-1})$ is a chain ring.

Theorem 3.7. *The ring $\mathcal{S}_3(s, \Lambda^{-1})$ is a chain ring with maximal ideal $\langle x^2 - \alpha_0^{-1} \rangle$, whose ideals are*

$$\mathcal{S}_3(s, \Lambda^{-1}) = \langle 1 \rangle \supsetneq \langle x^2 - \alpha_0^{-1} \rangle \supsetneq \cdots \supsetneq \langle (x^2 - \alpha_0^{-1})^{3\cdot 5^s - 1} \rangle \supsetneq \langle (x^2 - \alpha_0^{-1})^{3\cdot 5^s} \rangle = \langle 0 \rangle.$$

In other words, Λ^{-1}-constacyclic codes of length $2 \cdot 5^s$ over $\mathcal{R}_3$ are precisely the ideals $\langle (x^2 - \alpha_0^{-1})^i \rangle \subseteq \mathcal{S}_3(s, \Lambda^{-1})$, where $0 \leq i \leq 3 \cdot 5^s$. Each Λ^{-1}-constacyclic code $\langle (x^2 - \alpha_0^{-1})^i \rangle \subseteq \mathcal{S}_3(s, \Lambda^{-1})$ has 5^{2mi} codewords.

Applying Theorem 3.7, we now can describe the duals of Λ-constacyclic codes in the following corollary.

Corollary 3.8. *Let C be a Λ-constacyclic code of length $2 \cdot 5^s$ over $\mathcal{R}_3$. Then $C = \langle (x^2 - \alpha_0)^i \rangle \subseteq \mathcal{R}_3$, for some $i \in \{0, 1, \ldots, 3 \cdot 5^s\}$, and its dual $C^\perp$ is the Λ^{-1}-constacyclic code*

$$C^\perp = \left\langle (x^2 - \alpha_0^{-1})^{3\cdot 5^s - i} \right\rangle \subseteq \mathcal{R}_3.$$

Proof. Let $C = \langle (x^2 - \alpha_0)^i \rangle \subseteq \mathcal{S}_3(s, \Lambda)$ be a Λ-constacyclic code of length $2 \cdot 5^s$ over $\mathcal{R}_3$. Then, $C^\perp$ is an ideal of $\mathcal{S}_3(s, \Lambda^{-1})$. By Theorem 3.7, $|C| = 5^{2m(3\cdot 5^s - i)}$, and hence, by Proposition 2.3,

$$|C^\perp| = \frac{|\mathcal{R}_3|^{2\cdot 5^s}}{|C|} = \frac{5^{6m5^s}}{p^{2m(3\cdot 5^s - i)}} = 5^{2mi}.$$

From Theorem 3.7, we have $C^\perp = \left\langle (x^2 - \alpha_0^{-1})^{5^s - i} \right\rangle \subseteq \mathcal{S}_3(s, \Lambda^{-1})$. $\square$

References

[1] M.C.V. Amarra and F. R. Nemenzo, On $(1-u)$- cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, Applied Mathematics Letters, 21 (2008), 1129-1133.

[2] 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.

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

[4] E.R. Berlekamp, Algebraic Coding Theory, revised 1984 edition, Aegean Park Press, 1984.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] B. Chen, L. Lin, and H. Liu, *Matrix product codes with Rosenbloom-Tsfasma metric*, Acta Math. Sci. **33B** (2013), 687-700.

[12] H.Q. Dinh, *On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions*, Finite Fields & Appl. **14** (2008), 22-40.

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

[19] H.Q. Dinh, S. Dhompongsa and S. Sriboonchitta, *Repeated-root constacyclic codes of prime power length over* $\frac{\mathbb{F}_{p^m}[u]}{\langle u^a \rangle}$ *and their duals*, Discrete Math. to appear.

[20] S. Dougherty, P. Gaborit, M. Harada, and P. Sole, *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory **45** (1999), 32-45.

[21] S.T. Dougherty and M.M. Skriganov, *Macwilliams duality and Rosenbloom-Tsfasman metric*, Moscow Math. J., **2** (2002), 81-97.

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

[23] 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.

[24] 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.

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

[26] K. Lee, *Automorphism group of the Rosenbloom-Tsfasman space*, Eur. J. Combin. **24** (2003), 607-612.

[27] S. Ling and P. Solé, *Duadic codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, Appl. Algebra Engrg. Comm. Comput. **12** (2001), 365-379.

[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] 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.

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

[33] E. Prange, *Cyclic Error-Correcting Codes in Two Symbols*, (September 1957), TN-57-103.

[34] E. Prange, *Some cyclic error-correcting codes with simple decoding algorithms*, (April 1958), TN-58-156.

[35] E. Prange, *The use of coset equivalence in the analysis and decoding of group codes*, (1959), TN-59-164.

[36] E. Prange, *An algorithm for factoring $x^n - 1$ over a finite field*, (October 1959), TN-59-175.

[37] M.Y. Rosenbloom and M. A. Tsfasman, *Codes for the m-metric*, Problems Inf. Trans. **33** (1997), 45-52.

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

[39] R. Sobhani, and M. Esmaeili, Cyclic and negacyclic codes over the Galois ring $GR(p^2, m)$ Discrete Applied Mathematics, 157 (2009), 2892-2903.

[40] R. Sobhani, Complete classification of $(\delta + u^2\gamma)$-constacyclic codes of length p^k over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$, FFA, **34** (2015), 123-138.

[41] M.M. Skriganov, *On linear codes with large weights simultaneously for the Rosenbloom-Tsfasman and Hamming metrics*, J. of Complexity **23** (2007), 926-936.

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