Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2019) 43: 561 – 578
© TÜBİTAK
doi:10.3906/mat-1808-108

RT distance and weight distributions of Type 1 constacyclic codes of length $4p^s$ over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^a\rangle}$

Hai Q. DINH[1,2]*, **Bac Trong NGUYEN**[3,4]†, **Songsak SRIBOONCHITTA**[5]

[1]Division of Computational Mathematics and Engineering, Institute for Computational Science,
Ton Duc Thang University, Ho Chi Minh City, Vietnam
[2]Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[3]Nguyen Tat Thanh University, Ho Chi Minh city, Vietnam
[4]Department of Basic Sciences, Thai Nguyen University of Economics and Business Administration,
Thai Nguyen Province, Vietnam
[5]Faculty of Economics, Chiang Mai University, Chiang Mai, Thailand

Received: 23.08.2018 • **Accepted/Published Online:** 03.12.2018 • **Final Version:** 27.03.2019

Abstract: For any odd prime p such that $p^m \equiv 1 \pmod 4$, the class of Λ-constacyclic codes of length $4p^s$ over the finite commutative chain ring $\mathcal{R}_a = \frac{\mathbb{F}_{p^m}[u]}{\langle u^a\rangle} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{a-1}\mathbb{F}_{p^m}$, for all units Λ of $\mathcal{R}_a$ that have the form $\Lambda = \Lambda_0 + u\Lambda_1 + \cdots + u^{a-1}\Lambda_{a-1}$, where $\Lambda_0, \Lambda_1, \ldots, \Lambda_{a-1} \in \mathbb{F}_{p^m}$, $\Lambda_0 \neq 0$, $\Lambda_1 \neq 0$, is investigated. If the unit Λ is a square, each Λ-constacyclic code of length $4p^s$ is expressed as a direct sum of a $-\lambda$-constacyclic code and a λ-constacyclic code of length $2p^s$. In the main case that the unit Λ is not a square, we show that any nonzero polynomial of degree < 4 over $\mathbb{F}_{p^m}$ is invertible in the ambient ring $\frac{\mathcal{R}_a[x]}{\langle x^{4p^s} - \Lambda\rangle}$ and use it to prove that the ambient ring $\frac{\mathcal{R}_a[x]}{\langle x^{4p^s} - \Lambda\rangle}$ is a chain ring with maximal ideal $\langle x^4 - \lambda_0\rangle$, where $\lambda_0^{p^s} = \Lambda_0$. As an application, the number of codewords and the dual of each λ-constacyclic code are provided. Furthermore, we get the Rosenbloom–Tsfasman (RT) distance and weight distributions of such codes. Using these results, the unique MDS code with respect to the RT distance is identified.

Key words: RT distance, constacyclic codes, dual codes, chain rings

1. Introduction

Let p be a prime number and $\mathbb{F}_{p^m}$ the finite field. An [n,k] linear code C over $\mathbb{F}_{p^m}$ is a k-dimensional subspace of $\mathbb{F}_{p^m}^n$. A linear code C of length n over $\mathbb{F}_{p^m}$ is called a λ-*constacyclic code* if it is an ideal of the quotient ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n-\lambda\rangle}$, where the generator polynomial $g(x)$ is the unique monic polynomial of minimum degree in the code, which is a divisor of $x^n - \lambda$. In the case of $\lambda = 1$, those λ-constacyclic codes are called *cyclic codes*, and when $\lambda = -1$, such λ-constacyclic codes are called *negacyclic codes*. Cyclic and negacyclic codes are interesting from both theoretical and practical perspectives, which have been well studied since the late 1960s.

When the code of length n is relatively prime to the characteristic of the field $\mathbb{F}$, these codes are said to be *simple root codes*; otherwise, they are called *repeated-root codes*, which were first studied in 1967 by Berman [5]. Many authors studied repeated-root codes over finite fields ([28, 33, 44]). However, repeated-root codes were

*dinhquanghai@tdtu.edu.vn

†Correspondence: bacnt2008@gmail.com

2010 *AMS Mathematics Subject Classification:* Primary 94B15, 94B05; Secondary 11T71 investigated in the most generality in the 1990s by Castagnoli et al. [11] and van Lint [47], 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, which motivates researchers to further study this class of codes (see, for example, [36]).

Codes over finite rings have been intensively studied since the 1990s because of their new role in algebraic coding theory and their successful applications. In an important paper [29], Hammons et al. proved that certain good nonlinear codes such as Kerdock and Preparata codes can be constructed from linear codes over $\mathbb{Z}_4$ via the Gray map. Since then, codes over finite chain rings have received attention. Since 2003, special classes of repeated-root codes over certain classes of finite chain rings have been studied by numerous other authors (see, for example, [1, 6, 22]).

After the realization in the 1990s [10, 29, 35] that many important yet seemingly nonlinear codes over finite fields are actually closely related to linear codes over the ring of integers modulo four, codes over $\mathbb{Z}_4$ in particular and codes over finite commutative chain rings in general have developed rapidly in recent decade years. Constacyclic codes over a finite commutative chain ring have been studied by many authors (see, for example, [2, 9, 37, 46]). 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 works include cyclic and self-dual codes [7], decoding of cyclic codes [8], type II codes [26], duadic codes [32], and repeated-root constacyclic codes [15].

Recently, Dinh, in a series of papers ([17–19]), 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. Therefore, certain classes of repeated-root constacyclic codes over finite chain rings are studied in some of our papers. For example, Dinh [16] classified all constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Moreover, in 2015, Dinh et al. [25] studied negacyclic codes of length $2p^s$ over the ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Recently, Chen et al. [12] determined the algebraic structures of all λ-constacyclic codes of length $2p^s$ over the finite commutative chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and provided the number of codewords and the dual of every λ-constacyclic code. As a generalization of finite chain rings $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ $(u^2 = 0)$, finite chain rings of the form $\mathcal{R}_a = \frac{\mathbb{F}_{p^m}[u]}{\langle u^a \rangle} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{a-1}\mathbb{F}_{p^m}$ $(u^a = 0)$ have been developed as code alphabet as well. In [20], we partitioned the units of the chain ring $\mathcal{R}_a$ into a distinct types and studied Type 1 constacyclic codes of length p^s over $\mathcal{R}_a$ in detail. From this, we showed that self-dual Λ-constacyclic codes of length p^s over $\mathcal{R}_a$ exist if and only if a is even, and in such case, it is unique.

In a recent paper [23], we studied the algebraic structures of Type 1 Λ-constacyclic codes of length $2p^s$ over $\mathcal{R}_a$. Moreover, Rosenbloom–Tsfasman distances and weight distributions of these codes were considered. The aim of this paper is to generalize the study in [23] of codes of length $2p^s$ to the case of codes of length $4p^s$ over $\mathcal{R}_a = \frac{\mathbb{F}_{p^m}[u]}{\langle u^a \rangle} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{a-1}\mathbb{F}_{p^m}$ $(u^a = 0)$. We can show that any nonzero polynomial of degree < 4 over $\mathbb{F}_{p^m}$ is invertible in the ambient ring $\frac{\mathcal{R}}{\langle x^{4p^s} - \Lambda \rangle}$. Using this important result, the ambient ring $\frac{\mathcal{R}}{\langle x^{4p^s} - \Lambda \rangle}$ will be proven to be a chain ring, whose maximal ideal is $\langle x^4 - \lambda_0 \rangle$, and the nilpotency of $(x^4 - \lambda_0)$ is ap^s.

In 1997, Rosenbloom and Tsfasman [43] introduced a new metric, which was later named after them as the RT metric, for vectors over a finite field as a generalization of the classical Hamming metric. Therefore, the study of this RT metric is very significant from both a theoretical and a practical viewpoint. In recent decades, the RT metric received the attention of many researchers. The codes on this metric were considered with various bounds, weight distributions, MacWilliams identities, maximum distance separability, and groups of automorphisms. In this paper, as an application, the structure of Type 1 Λ-constacyclic codes is used to determine the RT distance and weight distributions of all such codes. From this, the unique MDS code with respect to the RT distance is also obtained.

The rest of this paper is organized as follows. Preliminary concepts and some properties of constacyclic codes over finite commutative rings are shown in Section 2. We introduce some results about the rings $\mathcal{R}_a = \frac{\mathbb{F}_{p^m}[u]}{\langle u^a \rangle}$ and their units studied in [20] in this section. We provide the algebraic structures of Type 1 Λ-constacyclic codes of length $4p^s$ over $\mathcal{R}_a$ and their duals in Section 3. In Section 4, these structures are used to obtain the RT distance and weight distributions of all such codes. The only MDS code, with respect to the RT distance, among these constacyclic codes is also identified.

2. Constacyclic codes over finite commutative rings

An ideal I of a ring R is called *principal* if there is an element a of R such that $I = aR = \{ar : r \in R\}$. A ring R is a *principal ideal ring* if its ideals are principal. A commutative ring with identity is called a *chain ring* if all its ideals form a chain under inclusion. By [22, Proposition 2.1], we have some characterizations of chain rings as follows.

Proposition 2.1 [22, 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.

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.

The codeword $c = (c_0, c_1, \dots, c_{n-1})$ is represented by its polynomial representation $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, using the obvious one-to-one correspondence, so multiplication by x in the ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n - \lambda \rangle}$ corresponds to a λ-constacyclic shift of $c(x)$. From this, we have the following result that appeared in [30].

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

The inner product of vectors $x = (x_0, x_1, \dots, x_{n-1}), y = (y_0, y_1, \dots, y_{n-1}) \in R^n$ is defined by

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

Once we have specified a family of codes called the dual of a code C to be

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

a code C is called *self-orthogonal* if $C \subseteq C^{\perp}$, and it is called *self-dual* if $C = C^{\perp}$. An important result is cited here to use later on.

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

The *Hamming weight* of x is the number of nonzero components of x denoted by $\mathrm{wt_H}(x)$ for every word $x = (x_0, x_1, \ldots, x_{n-1}) \in R^n$. The Hamming distance $d(x, y)$ of two words x, y is the number of components in which they differ, which is the Hamming weight $\mathrm{wt_H}(x - y)$ of $x - y$. For a nonzero linear code C, the Hamming weight and the Hamming distance $d(C)$ are the same. They are defined as the smallest Hamming weight of nonzero codewords of C:

$$d(C) = \min\{\mathrm{wt_H}(x) \mid x \neq \mathbf{0},\ x \in C\}.$$

The zero code is conventionally said to have Hamming distance 0.

For a unit λ of R, the λ-constacyclic (λ-twisted) shift τ_λ on R^n is the shift

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

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 the case of $\lambda = 1$, those λ-constacyclic codes are called cyclic codes, and when $\lambda = -1$, such λ-constacyclic codes are called negacyclic codes.

Each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ 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 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 know 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, [16, 18]).

The following result is also a fact that appeared in [16, 18].

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

$$a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},\ b(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \in R[x].$$

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 $\mathrm{ann}(S)$, is the set

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

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

For a polynomial f of degree k, the polynomial $x^k f(x^{-1})$ is called the *reciprocal polynomial* of polynomial f, and it is denoted by f^*. Suppose that $f(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + a_k x^k$. 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 code 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 $\mathrm{ann}^*(C)$ is also an ideal of $\frac{R[x]}{\langle x^n - \lambda^{-1}\rangle}$. Therefore, applying Proposition 2.5, we can conclude that $g(x) \in \mathrm{ann}^*(C)$ if and only if $g(x) = f^*(x)$ for some $f(x) \in \mathrm{ann}(C)$, if and only if $g(x) \in C^\perp$. Then we have the 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 $\mathrm{ann}^*(C)$.*

In [20], the units of $\mathcal{R}_a$ are separated into a distinct types. A unit $\lambda = \lambda_0 + u\lambda_1 + \cdots + u^{a-1}\lambda_{a-1}$ of $\mathcal{R}_a$ is said to be of type k if k is the smallest index such that $\lambda_k \neq 0$ for an integer $k \in \{1, \ldots, a-1\}$. Moreover, if $\lambda_0 = 1$, then $1 + u\lambda_1 + \cdots + u^{a-1}\lambda_{a-1}$ is said to be of type k^*. If $\lambda_i = 0$ for all $1 \le i \le a-1$, i.e. the unit is of the form $\lambda = \lambda_0 \in \mathbb{F}_{p^m}$, we say that λ is of type 0 (or type 0^* if $\lambda_0 = 1$). $\mathcal{R}_a$ has $p^m - 1$ units of type 0 and $(p^m-1)^2p^{m(a-k-1)}$ units of type k, showing that $\mathcal{R}_a$ has $p^m - 1$ type 0 constacyclic codes and $(p^m-1)^2p^{m(a-k-1)}$ type k constacyclic codes.

We now suppose that Λ is a unit of type k of $\mathcal{R}_a$. Then Λ can be expressed as follows:

$$\Lambda = \Lambda_0 + u^k\Lambda_k + \cdots + u^{a-1}\Lambda_{a-1},$$

where $\Lambda_0, \Lambda_k, \ldots, \Lambda_{a-1} \in \mathbb{F}_{p^m}$, $\Lambda_0 \neq 0, \Lambda_k \neq 0$, and $1 \le k \le a-1$. Let $\lambda = 1 + u^k\lambda_k + \cdots + u^{a-1}\lambda_{a-1}$, for $k \le i \le a-1$, $\lambda_i = \Lambda_i\Lambda_0^{-1} \in \mathbb{F}_{p^m}$. Then we can see that λ is a unit of type k^* such that $\Lambda = \Lambda_0\lambda$. It is easy to verify that in the case of Λ being a unit of type 0 and λ of type 0^*, we also have $\Lambda = \Lambda_0\lambda$. The unit of Λ is determined in the following proposition.

Proposition 2.7 [20] *Let $\Lambda = \Lambda_0 + u\Lambda_1 + \cdots + u^{a-1}\Lambda_{a-1}$ be a unit of $\mathcal{R}_a$ and t be the smallest positive integer such that $p^{tm} \ge a$. Then:*

(a) $\Lambda^{-1} = \Lambda^{p^{tm}-1}\Lambda_0^{-1}$.

(b) If Λ is of type k, for $1 \le k \le a-1$, i.e. $\Lambda = \Lambda_0 + u^k\Lambda_k + \cdots + u^{a-1}\Lambda_{a-1}$, where $\Lambda_0 \neq 0, \Lambda_k \neq 0$, then Λ^{-1} is also of type k. More precisely,

$$\Lambda^{-1} = \Lambda_0^{-1} + u^k\Lambda'_k + \cdots + u^{a-1}\Lambda'_{a-1},$$

where $\Lambda'_k \neq 0$. If Λ is of type 0, i.e. $\Lambda = \Lambda_0$, then $\Lambda^{-1} = \Lambda_0^{-1}$, which is of type 0. In particular, for $0 \le \ell \le a-1$, Λ is of type ℓ (resp. type ℓ^*) if and only if Λ^{-1} is of type ℓ (resp. type ℓ^*).

(c) Let Λ be of type k for $1 \le k \le a-1$. If $\Lambda = \Lambda^{-1}$ then $p = 2$, and $k \ge a/2$ (if a is even) or $k \ge \lfloor a/2 \rfloor + 1$ (if a is odd). More precisely, in such a case, the units Λ such that $\Lambda = \Lambda^{-1}$ are precisely units of the form

$$\Lambda = 1 + \sum_{i=a/2}^{a-1} u^i\Lambda_i^i \qquad \textit{if } a \textit{ is even, or}$$

$$\Lambda = 1 + \sum_{i=\lfloor a/2\rfloor+1}^{a-1} u^i \Lambda_i^i \qquad \textit{if } a \textit{ is odd,}$$

where $\Lambda_i \in \mathbb{F}_{2^m}$

3. Type 1 Λ-constacyclic codes of length $4p^s$ over $\mathcal{R}_a$

In this paper, we study Λ-constacyclic codes of length $4p^s$ over $\mathcal{R}_a$ and its dual, where Λ is a unit of Type 1 of $\mathcal{R}_a$, i.e. Λ has the following form:

$$\Lambda = \Lambda_0 + u\Lambda_1 + \cdots + u^{a-1}\Lambda_{a-1},$$

where $\Lambda_0, \Lambda_1, \ldots, \Lambda_{a-1} \in \mathbb{F}_{p^m}$, $\Lambda_0 \neq 0$, $\Lambda_1 \neq 0$. It is well known from Proposition 2.4 that these codes are ideals of the ring

$$\mathcal{S}_a(s,\Lambda) = \frac{\mathcal{R}_a[x]}{\langle x^{4p^s} - \Lambda\rangle}.$$

Applying Proposition 2.7, if Λ is a unit of Type 1, then Λ^{-1} is also a unit of Type 1. Hence, Λ^{-1} can be expressed as follows:

$$\Lambda^{-1} = \Lambda_0^{-1} + u\Lambda_1' + \cdots + u^{a-1}\Lambda_{a-1}',$$

where $\Lambda_1' \neq 0$.

Suppose that unit Λ is a square in $\mathcal{R}_a$. It implies that there exists a unit $\lambda \in \mathcal{R}_a$ such that $\Lambda = \lambda^2$, i.e. $\Lambda = (\lambda_0 + u\lambda_1 + \cdots + u^{a-1}\lambda_{a-1})^2$. Since $\Lambda_0 \neq 0$ and $\Lambda_1 \neq 0$, it is easy to see that $\lambda_0 \neq 0$ and $\lambda_1 \neq 0$. This means that λ is also a unit of Type 1. Then we have

$$x^{4p^s} - \Lambda = x^{4p^s} - \lambda^2 = (x^{2p^s} + \lambda)(x^{2p^s} - \lambda).$$

Hence, by the Chinese remainder theorem, we can express $\mathcal{S}_a(s,\Lambda)$ as follows:

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

This shows that all ideals of $\mathcal{S}_a(s,\Lambda)$ are of the form $A \oplus B$, where A and B are ideals of $\frac{\mathcal{R}_a[x]}{\langle x^{2p^s}+\lambda\rangle}$ and $\frac{\mathcal{R}_a[x]}{\langle x^{2p^s}-\lambda\rangle}$, respectively. It is clear that they are $-\lambda$- and λ-constacyclic codes of length $2p^s$ over $\mathcal{R}_a$. Therefore, a Type 1 Λ-constacyclic code of length $4p^s$ over $\mathcal{R}_a$ can be written as a direct sum of C_+ and C_-:

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

where C_+ and C_- are ideals of $\frac{\mathcal{R}_a[x]}{\langle x^{2p^s}+\lambda\rangle}$ and $\frac{\mathcal{R}_a[x]}{\langle x^{2p^s}-\lambda\rangle}$, respectively. Hence, we can obtain Λ-constacyclic codes C of length $4p^s$ over $\mathcal{R}_a$ from that of the direct summands C_+ and C_- because the classification, detailed structure, and number of codewords of λ and $-\lambda$ constacyclic codes of length $2p^s$ were investigated in [23]. This implies that the dual code $C^\perp$ of C is also a direct sum of the dual codes of the direct summand $C_+^\perp$ and $C_-^\perp$. The following results allow us to determine the dual code $C^\perp$ of C when Λ is a square in $\mathcal{R}_a$:

Theorem 3.1 *Let the unit $\Lambda = \lambda^2 \in \mathcal{R}_a$, and let $C = C_+ \oplus C_-$ be a constacyclic code of length $4p^s$ over $\mathcal{R}_a$, where C_+, C_- are ideals of $\frac{\mathcal{R}_a[x]}{\langle x^{2p^s}+\lambda\rangle}$, $\frac{\mathcal{R}_a[x]}{\langle x^{2p^s}-\lambda\rangle}$, respectively. Then*

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

In particular, C is a self-dual constacyclic code of length $4p^s$ over $\mathcal{R}_a$ if and only if C_+, C_- are a self-dual $-\lambda$-constacyclic code and self-dual λ-constacyclic code of length $2p^s$ over $\mathcal{R}_a$, respectively.

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

$$|C_+^\perp \oplus C_-^\perp| = |C_+^\perp| \cdot |C_-^\perp| = \frac{|\mathcal{R}_a|^{2p^s}}{|C_+|} \cdot \frac{|\mathcal{R}_a|^{2p^s}}{|C_-|} = \frac{|\mathcal{R}_a|^{4p^s}}{|C_+| \cdot |C_-|} = \frac{|\mathcal{R}_a|^{4p^s}}{|C|} = |C^\perp|.$$

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

We consider on the main case where Λ is not a square in $\mathcal{R}_a$. We need an important observation given in [23].

Proposition 3.2 [23, Proposition 3.2] *Let $\Lambda = \Lambda_0 + u\Lambda_1 + \cdots + u^{a-1}\Lambda_{a-1}$, $\Lambda_0, \Lambda_1, \ldots, \Lambda_{a-1} \in \mathbb{F}_{p^m}$, $\Lambda_0 \neq 0$, $\Lambda_1 \neq 0$, be a unit of Type 1 of $\mathcal{R}_a$. Then Λ is not a square if and only if Λ_0 is not a square.*

Applying this, we have the following result.

Theorem 3.3 *If Λ is not a square, then any nonzero polynomial of degree less than 4 in $\mathbb{F}_{p^m}[x]$ is invertible in $\mathcal{S}_a(a, \Lambda)$.*

Proof Let $f(x) = ax^3 + bx^2 + cx + d$ be a nonzero polynomial in $\mathbb{F}_{p^m}[x]$, i.e. $a, b, c, d \in \mathbb{F}_{p^m}$ such that not all of them are 0. We must show that $f(x)$ is invertible in $\mathcal{S}_a(s, \Lambda)$. It is easy to see that if $a = b = c = 0$, then $f(x) = d \neq 0$, which is invertible. We need to consider three cases where $\deg(f) = 1, 2,$ and 3.

Case 1: $\deg(f) = 1$, i.e. $a = b = 0$, $c \neq 0$, and $f(x) = cx + d$.

In $\mathcal{S}_a(s, \Lambda)$, we can see that

$$(x+d)^{p^s}(x-d)^{p^s}(x^2+d^2)^{p^s} = (x^4 - d^4)^{p^s} = x^{4p^s} - d^{4p^s} = (\Lambda_0 - d^{4p^s}) + u\Lambda_1 + \cdots + u^{a-1}\Lambda_{a-1}.$$

Since Λ_0 is not a square in $\mathbb{F}_{p^m}$, $\Lambda_0 - d^{4p^s}$ is invertible in $\mathbb{F}_{p^m}$. This implies that $(\Lambda_0 - d^{4p^s}) + u\Lambda_1 + \cdots + u^{a-1}\Lambda_{a-1}$ is invertible in R. Hence,

$$(x+d)^{-1} = (x+d)^{p^s-1}(x-d)^{p^s}(x^2+d^2)^{p^s}(\Lambda_0 - d^{4p^s} + u\Lambda_1 + \cdots + u^{a-1}\Lambda_{a-1})^{-1}.$$

From this, for any $c \neq 0$ in $\mathbb{F}_{p^m}$, $x + c^{-1}d$ is invertible, and

$$\begin{aligned}(cx+d)^{-1} &= c^{-1}(x + c^{-1}d)^{-1} \\ &= c^{-1}(x + c^{-1}d)^{p^s-1}(x - c^{-1}d)^{p^s}(x^2 + c^{-2}d^2)^{p^s}(\Lambda_0 - c^{-4p^s}d^{4p^s} + u\Lambda_1 + \cdots + u^{a-1}\Lambda_{a-1})^{-1}.\end{aligned}$$

Case 2: $\deg(f) = 2$, i.e. $a = 0$, $b \neq 0$, and $f(x) = bx^2 + cx + d$. Since $\Lambda_0 \in \mathbb{F}_{p^m}$, $\Lambda_0^{p^m} = \Lambda_0$, and so $\Lambda_0^{p^{tm}} = \Lambda_0$, for any positive integer t. By the division algorithm, there exist nonnegative integers

Λ_q, Λ_r such that $s = \Lambda_0 m + \Lambda_r$, and $0 \leq \Lambda_r \leq m-1$. Let $\lambda_0 = \Lambda_0^{p^{(\Lambda+1)m-s}} = \Lambda_0^{p^{m-\Lambda_r}}$. Then $\lambda_0^{p^s} = \Lambda_0^{p^{(\Lambda_q+1)m}} = \Lambda_0$. Clearly, Λ_0 is not a square if and only if λ_0 is not a square. In $\mathcal{S}_a(s,\Lambda)$, $f(x)^{-1}$ can be expressed as follows:

$$\begin{aligned}
f(x)^{-1} &= (bx^2+cx+d)^{-1} = b^{-1}(x^2+b^{-1}cx+b^{-1}d)^{-1}\\
&= b^{-1}(x^2+c_2x+d_2)^{-1}, \qquad \text{where } c_2 = b^{-1}c, d_2 = b^{-1}d,\\
&= b^{-1}(g(x))^{p^s-1}(g(x))^{-p^s}(x^2-c_2x-d_2+c_2^2)^{-p^s}(x^2-c_2x-d_2+c_2^2)^{p^s}, \qquad \text{where } g(x) = x^2+c_2x+d_2,\\
&= b^{-1}(g(x))^{p^s-1}(x^2-c_2x-d_2+c_2^2)^{p^s}\left[(g(x))(x^2-c_2x-d_2+c_2^2)\right]^{-p^s}\\
&= b^{-1}(g(x))^{p^s-1}(x^2-c_2x-d_2+c_2^2)^{p^s}\left[x^4+(c_2^3-2c_2d_2)x+(c_2^2d_2-d_2^2)\right]^{-p^s}\\
&= b^{-1}(g(x))^{p^s-1}(x^2-c_2x-d_2+c_2^2)^{p^s}\left[x^{4p^s}+(c_2^3-2c_2d_2)^{p^s}x^{p^s}+(c_2^2d_2-d_2^2)^{p^s}\right]^{-1}\\
&= b^{-1}(g(x))^{p^s-1}(x^2-c_2x-d_2+c_2^2)^{p^s}\left[\Lambda_0+u\Lambda_1+\cdots+u^{a-1}\Lambda_{a-1}+(c_2^3-2c_2d_2)^{p^s}x^{p^s}+(c_2^2d_2-d_2^2)^{p^s}\right]^{-1}\\
&= b^{-1}(g(x))^{p^s-1}(x^2-c_2x-d_2+c_2^2)^{p^s}\left[\left(\lambda_0+c_2^2d_2-d_2^2+(c_2^3-2c_2d_2)x\right)^{p^s}+u\Lambda_1+\cdots+u^{a-1}\Lambda_{a-1}\right]^{-1}.
\end{aligned}$$

This shows that $f(x)$ is invertible if and only if $\lambda_0+c_2^2d_2-d_2^2+(c_2^3-2c_2d_2)x$ is invertible. By Case 1, it is equivalent to $\lambda_0+c_2^2d_2-d_2^2+(c_2^3-2c_2d_2)x \neq 0$. It is routine to check that $c_2^3-2c_2d_2=0$ if and only if $c_2=0$ or $c_2^2=2d_2$. This implies that $\lambda_0+c_2^2d_2-d_2^2=0$ if and only if $\lambda_0 = d_2^2-c_2^2d_2$, i.e. $\lambda_0 = d_2^2$ (if $c_2=0$), or $\lambda_0 = -d_2^2$ (if $c_2^2=2d_2$). This is a contradiction because -1 is a square and λ_0 is not a square. Therefore, $f(x)$ is invertible.

Case 3: $\deg(f)=3$, i.e. $a\neq 0$, and $f(x)=ax^3+bx^2+cx+d$.

In $\mathcal{S}_a(s,\Lambda)$, $f(x)$ being invertible means

$$\begin{aligned}
f(x)^{-1} &= (ax^3+bx^2+cx+d)^{-1} = a^{-1}(x^3+a^{-1}bx^2+a^{-1}cx+a^{-1}d)^{-1}\\
&= a^{-1}(x^3+b_3x^2+c_3x+d_3)^{-1}, \qquad \text{where } b_3=a^{-1}b, c_3=a^{-1}c, d_3=a^{-1}d,\\
&= a^{-1}(h(x))^{p^s-1}(h(x))^{-p^s}(x-b_3)^{p^s}(x-b_3)^{-p^s}, \qquad \text{where } h(x)=x^3+b_3x^2+c_3x+d_3,\\
&= a^{-1}(h(x))^{p^s-1}(x-b_3)^{p^s}\left[(h(x))(x-b_3)\right]^{-p^s}\\
&= a^{-1}(h(x))^{p^s-1}(x-b_3)^{p^s}\left[x^4+(c_3-b_3^2)x^2+(d_3-b_3c_3)x-b_3d_3\right]^{-p^s}\\
&= a^{-1}(h(x))^{p^s-1}(x-b_3)^{p^s}\left[x^{4p^s}+(c_3-b_3^2)^{p^s}x^{2p^s}+(d_3-b_3c_3)^{p^s}x^{p^s}-b_3^{p^s}d_3^{p^s}\right]^{-1}\\
&= a^{-1}(h(x))^{p^s-1}(x-b_3)^{p^s}\left[\Lambda_0+u\Lambda_1+\cdots+u^{a-1}\Lambda_{a-1}+(c_3-b_3^2)^{p^s}x^{2p^s}+(d_3-b_3c_3)^{p^s}x^{p^s}-b_3^{p^s}d_3^{p^s}\right]^{-1}\\
&= a^{-1}(h(x))^{p^s-1}(x-b_3)^{p^s}\left[\left((c_3-b_3^2)x^2+(d_3-b_3c_3)x+(\lambda_0-b_3d_3)\right)^{p^s}+u\Lambda_1+\cdots+u^{a-1}\Lambda_{a-1}\right]^{-1}.
\end{aligned}$$

Therefore, $f(x)$ is invertible if and only if $(c_3-b_3^2)x^2+(d_3-b_3c_3)x+(\lambda_0-b_3d_3)$ is invertible, which is, by Case 2, equivalent to

$$(c_3-b_3^2)x^2+(d_3-b_3c_3)x+(\lambda_0-b_3d_3) \neq 0.$$

In order for $(c_3-b_3^2)x^2+(d_3-b_3c_3)x+(\lambda_0-b_3d_3)=0$, we must have $c_3-b_3^2=d_3-b_3c_3=\lambda_0-b_3d_3=0$, i.e. $c_3=b_3^2$, $d_3=b_3c_3$, and $\lambda_0=b_3d_3$. It follows that $\lambda_0=b_3d_3=b_3^2c_3=b_3^4$, which is impossible since λ_0 is not a square. Hence, $f(x)$ is invertible.

□

Note that in $\mathcal{S}_a(s,\Lambda)$, $(x^4-\lambda_0)^{p^s}=x^{4p^s}-\Lambda_0=u\Lambda_1+\cdots+u^{a-1}\Lambda_{a-1}$, and hence we get:

Lemma 3.4 *In $\mathcal{S}_a(s,\Lambda)$, we have $\langle (x^4-\lambda_0)^{p^s}\rangle=\langle u\rangle$. In particular, $x^4-\lambda_0$ is nilpotent with nilpotency index ap^s.*

Any element $f(x)$ of $\mathcal{R}_{\lambda,\beta}$ can be viewed as a polynomial of degree up to $4p^s-1$ of $R[x]$, and so $f(x)=f_1(x)+uf_2(x)+\cdots+u^{a-1}f_a(x)$, where $f_1(x),f_2(x),\ldots,f_a(x)$ are polynomials of degrees up to $4p^s-1$ of $\mathbb{F}_{p^m}[x]$. Thus, $f(x)$ can be uniquely expressed as

$$\begin{aligned}
f(x)&=\sum_{i=0}^{p^s-1}(a_{0i}x^3+b_{0i}x^2+c_{0i}x+d_{0i})(x^4-\lambda_0)^i+u\sum_{i=0}^{p^s-1}(a_{1i}x^3+b_{1i}x^2+c_{1i}x+d_{1i})(x^4-\lambda_0)^i+\ldots\\
&\quad+u^{a-1}\sum_{i=0}^{p^s-1}(a_{(a-1)i}x^3+b_{(a-1)i}x^2+c_{(a-1)i}x+d_{(a-1)i})(x^4-\lambda_0)^i\\
&=(a_{00}x^3+b_{00}x^2+c_{00}x+d_{00})+(x^4-\lambda_0)\sum_{i=1}^{p^s-1}(a_{0i}x^3+b_{0i}x^2+c_{0i}x+d_{0i})(x^4-\lambda_0)^{i-1}+\\
&\quad+u\sum_{i=0}^{p^s-1}(a_{1i}x^3+b_{1i}x^2+c_{1i}x+d_{1i})(x^4-\lambda_0)^i+\cdots+\\
&\quad+u^{a-1}\sum_{i=0}^{p^s-1}(a_{(a-1)i}x^3+b_{(a-1)i}x^2+c_{(a-1)i}x+d_{(a-1)i})(x^4-\lambda_0)^i,
\end{aligned}$$

where $a_{ji},b_{ji},c_{ji},d_{ji}\in\mathbb{F}_{p^m}$ for all $j=0,\ldots,a-1$.

By Lemma 3.4, $u\in\langle x^4-\lambda_0\rangle$, and so $f(x)$ can be written as

$$f(x)=(a_{00}x^3+b_{00}x^2+c_{00}x+d_{00})+(x^4-\lambda_0)g(x).$$

Thus, $f(x)$ is noninvertible if and only if $a_{00}=b_{00}=c_{00}=d_{00}=0$, i.e. $f(x)\in\langle x^4-\lambda_0\rangle$. It means that $\langle x^4-\lambda_0\rangle$ forms the set of all noninvertible elements of $\mathcal{R}_a$. Thus, $\mathcal{S}_a(s,\Lambda)$ is a local ring with maximal ideal $\langle x^4-\lambda_0\rangle$, and hence, by Proposition 2.1, $\mathcal{S}_a(s,\Lambda)$ is a chain ring. We summarize the discussion above in the following theorem.

Theorem 3.5 *The ring $\mathcal{S}_a(s,\Lambda)$ is a chain ring with maximal ideal $\langle x^4-\lambda_0\rangle$, whose ideals are*

$$\mathcal{S}_a(s,\Lambda)=\langle 1\rangle\supsetneq\langle x^4-\lambda_0\rangle\supsetneq\cdots\supsetneq\langle (x^4-\lambda_0)^{ap^s-1}\rangle\supsetneq\langle (x^4-\lambda_0)^{ap^s}\rangle=\langle 0\rangle.$$

By using Theorem 3.5, we can now give the structure of Type 1 Λ-constacyclic codes of length $4p^s$ over $\mathcal{R}_a$ and their sizes as follows.

Theorem 3.6 *Type* 1 Λ*-constacyclic codes of length* $4p^s$ *over* $\mathcal{R}_a$ *are precisely the ideals* $\langle (x^4-\lambda_0)^i\rangle \subseteq \mathcal{R}_a$*, where* $0 \le i \le ap^s$*. Each Type* 1 Λ*-constacyclic code* $\langle (x^4-\lambda_0)^i\rangle$ *has* $p^{4m(ap^s-i)}$ *codewords.*

For a Type 1 Λ-constacyclic code $C = \langle (x^4-\lambda_0)^i\rangle \subseteq \mathcal{R}_a$ of length $4p^s$ over $\mathcal{R}_a$, by Proposition 2.5 and Proposition 2.7, its dual $C^\perp$ is a Type 1 Λ^{-1}-constacyclic code of length $4p^s$ over $\mathcal{R}_a$. This means

$$C^\perp \subseteq \mathcal{S}_a(s,\Lambda^{-1}) = \frac{\mathcal{R}_a[x]}{\langle x^{4p^s} - \Lambda^{-1}\rangle}.$$

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

Theorem 3.7 *The ring* $\mathcal{S}_a(s,\Lambda^{-1})$ *is a chain ring with maximal ideal* $\langle x^4-\lambda_0^{-1}\rangle$*, whose ideals are*

$$\mathcal{S}_a(s,\Lambda^{-1}) = \langle 1\rangle \supsetneq \langle x^4-\lambda_0^{-1}\rangle \supsetneq \cdots \supsetneq \langle (x^4-\lambda_0^{-1})^{ap^s-1}\rangle \supsetneq \langle (x^4-\lambda_0^{-1})^{ap^s}\rangle = \langle 0\rangle.$$

In other words, Type 1 Λ^{-1}*-constacyclic codes of length* $4p^s$ *over* $\mathcal{R}_a$ *are precisely the ideals* $\langle (x^4-\lambda_0^{-1})^i\rangle \subseteq \mathcal{S}_a(s,\Lambda^{-1})$*, where* $0 \le i \le ap^s$*. Each Type* 1 Λ^{-1}*-constacyclic code* $\langle (x^4-\lambda_0^{-1})^i\rangle \subseteq \mathcal{S}_a(s,\Lambda^{-1})$ *has* p^{4mi} *codewords.*

Applying Theorem 3.7, we now can describe the duals of Type 1 Λ-constacyclic codes.

Corollary 3.8 *Let* C *be a Type* 1 Λ*-constacyclic code of length* $4p^s$ *over* $\mathcal{R}_a$*. Then* $C = \langle (x^4-\lambda_0)^i\rangle \subseteq \mathcal{R}_a$*, for some* $i \in \{0,1,\dots,ap^s\}$*, and its dual* $C^\perp$ *is the Type* 1 Λ^{-1}*-constacyclic code*

$$C^\perp = \left\langle (x^4-\lambda_0^{-1})^{ap^s-i}\right\rangle \subseteq \mathcal{R}_a.$$

Proof Let $C = \langle (x^4-\lambda_0)^i\rangle \subseteq \mathcal{S}_a(s,\Lambda)$ be a Type 1 Λ-constacyclic code of length $4p^s$ over $\mathcal{R}_a$. Then $C^\perp$ is an ideal of $\mathcal{S}_a(s,\Lambda^{-1})$. By Theorem 3.7, $|C| = p^{4m(ap^s-i)}$, and hence, by Proposition 2.3,

$$|C^\perp| = \frac{|\mathcal{R}_a|^{4p^s}}{|C|} = \frac{p^{4map^s}}{p^{4m(ap^s-i)}} = p^{4mi}.$$

From Theorem 3.7, we have $C^\perp = \left\langle (x^4-\lambda_0^{-1})^{4p^s-i}\right\rangle \subseteq \mathcal{S}_a(s,\Lambda^{-1})$. □

4. Rosenbloom–Tsfasman distance

The RT distance was first introduced in 1997 by Rosenbloom and Tsfasman. The RT distance gives a new distance on linear spaces over finite fields in coding theory. Well-known bounds for distances such as the Singleton bound, the Plotkin bound, the Hamming bound, and the Gilbert bound were derived for the RT distance. Recently, many authors have studied codes with respect to this RT metric (see, for example, [13, 27, 31, 45]).

Let R be a finite commutative ring. Then the *Rosenbloom-Tsfasman weight* (RT weight) (see [43]) of an n-tuple $\mathbf{x} = (x_0, x_1, \dots, x_{n-1}) \in R^n$ is defined as follows:

$$\mathrm{wt}_{\mathrm{HRT}}(\mathbf{x}) = \begin{cases} 1 + \max\{j \mid x_j \neq 0\}, & \text{if } \mathbf{x} \neq \mathbf{0}; \\ 0, & \text{if } \mathbf{x} = \mathbf{0}. \end{cases}$$

The *RT distance* of any two n-tuples $\mathbf{x}, \mathbf{y}$ of R^n is defined as:

$$d_{\mathrm{RT}}(\mathbf{x}, \mathbf{y}) = \mathrm{wt}_{\mathrm{HRT}}(\mathbf{x} - \mathbf{y}).$$

Suppose that C is a code of length n over R. Then we have

$$d_{\mathrm{RT}}(C) = \min\{d_{\mathrm{RT}}(\mathbf{c}, \mathbf{c}') \,|\, \mathbf{c} \neq \mathbf{c}' \in C\},$$

which is called the *RT distance* of C.

In this section the RT distances of all Λ-constacyclic codes of length $4p^s$ over the ring $\mathcal{R}_a$ for any unit Λ of Type 1 of $\mathcal{R}_a$ are investigated when Λ is not a square. The following result is straightforward from the definition of the RT weight.

Proposition 4.1 *Let $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in R^n$ be a word of length n over R, and let $c(x)$ be its polynomial presentation. Then*

$$\mathrm{wt}_{\mathrm{HRT}}(\mathbf{c}) = \begin{cases} 1 + \deg(c(x)), & \text{if } \mathbf{c} \neq \mathbf{0}; \\ 0, & \text{if } \mathbf{c} = \mathbf{0}. \end{cases}$$

The RT distances of Type 1 Λ-constacyclic codes of length $4p^s$ over $\mathcal{R}_a$ can be completely determined.

Theorem 4.2 *Let Λ be a unit of Type 1 of $\mathcal{R}_a$ such that Λ is not a square. Assume that C is a Λ-constacyclic code of length $4p^s$ over $\mathcal{R}_a$, i.e. $C = \langle (x^4 - \lambda_0)^i \rangle \subseteq \mathcal{S}_a(s, \Lambda)$, for some $i \in \{0, 1, \dots, ap^s\}$. Then the RT distance $d_{\mathrm{RT}}(C)$ of C is completely determined as follows:*

$$d_{\mathrm{RT}}(C) = \begin{cases} 0 & \text{if } i = ap^s \\ 1 & \text{if } 0 \leq i \leq (a-1)p^s \\ 4i - 4(a-1)p^s + 1 & \text{if } (a-1)p^s + 1 \leq i \leq ap^s - 1. \end{cases}$$

Proof If $i = ap^s$, it is clear that the code C is the zero code. From the definition of RT distance, we have $d_{RT}(C) = 0$. Using Lemma 3.4 and Theorem 3.5, when $0 \leq i \leq (a-1)p^s$, we have

$$\left\langle (x^4 - \lambda_0)^i \right\rangle \supseteq \left\langle (x^4 - \lambda_0)^{(a-1)p^s} \right\rangle = \left\langle u^{a-1} \right\rangle.$$

This shows that the RT distance of the code $\langle (x^4 - \lambda_0)^i \rangle$ is 1. We now consider the case $(a-1)p^s + 1 \leq i \leq ap^s - 1$. By simple calculation, we have

$$\left\langle (x^4 - \lambda_0)^i \right\rangle = \left\langle (x^4 - \lambda_0)^{(a-1)p^s} (x^4 - \lambda_0)^{i-(a-1)p^s} \right\rangle = \left\langle u^{a-1} (x^4 - \lambda_0)^{i-(a-1)p^s} \right\rangle.$$

To prove $d_{RT}(C) = 4i - 4(a-1)p^s + 1$ if $(a-1)p^s + 1 \leq i \leq ap^s - 1$, we must prove that, in each ideal $\left\langle u^{a-1}(x^4 - \lambda_0)^{i-(a-1)p^s} \right\rangle$, the generator polynomial $u^{a-1}(x^4 - \lambda_0)^{i-(a-1)p^s}$ is of smallest degree, which is $4i - 4(a-1)p^s$. By applying Proposition 4.1, its RT distance is $4i - 4(a-1)p^s + 1$. Assume that $f(x)$ is a nonzero polynomial in $\left\langle u^{a-1}(x^4 - \lambda_0)^{i-(a-1)p^s} \right\rangle$ of degree $0 \leq k < 4i - 4(a-1)p^s$. From this, $f(x)$ can be expressed as

$$f(x) = \sum_{j=0}^{k} (a_j x^3 + b_j x^2 + c_j x + d_j)(x^4 - \lambda_0)^j,$$

where $a_j, b_j, c_j, d_j \in \mathcal{R}_a$. Let ℓ $(0 \leq \ell \leq k)$ be the smallest index such that $a_jx^3 + b_jx^2 + c_jx + d_j \neq 0$. Then

$$f(x) = (x^4-\lambda_0)^\ell \sum_{j=\ell}^{k}(a_jx^3+b_jx^2+c_jx+d_j)(x^4-\lambda_0)^{j-\ell} = (x^4-\lambda_0)^\ell(a_\ell x^3+b_\ell x^2+c_\ell x+d_\ell)\left[1+(x^4-\lambda_0)g(x)\right],$$

where

$$g(x) = \begin{cases} 0, & \text{if } \ell = k, \\ (a_\ell x^3 + b_\ell x^2 + c_\ell x + d_\ell)^{-1} \sum\limits_{j=\ell+1}^{k} (a_jx^3 + b_jx^2 + c_jx + d_j)(x^4 - \lambda_0)^{j-\ell-1}, & \text{if } 0 \leq \ell < k, \end{cases} \in \mathcal{S}_a(s, \Lambda).$$

Using Lemma 3.4 again, $x^4 - \lambda_0$ is nilpotent in $\mathcal{S}_a(s, \Lambda)$, and then there is an odd integer t such that $(x^4 - \lambda_0)^t = 0$. From this, we have

$$\begin{aligned} 1 &= 1 + \left[(x^4 - \lambda_0)g(x)\right]^t \\ &= \left[1 + (x^4 - \lambda_0)g(x)\right]\left[1 - (x^4 - \lambda_0)g(x) + (x^4 - \lambda_0)^2 g(x)^2 - \cdots + (x^4 - \lambda_0)^{t-1}g(x)^{t-1}\right]. \end{aligned}$$

This means that $1+(x^4-\lambda_0)g(x)$ is invertible in $\mathcal{S}_a(s, \Lambda)$. Hence, $f(x) = (x^4-\lambda_0)^\ell h(x)$ for some unit $h(x)$ of $\mathcal{S}_a(s, \Lambda)$. It is equivalent to the statement that $f(x) \in \langle (x^4-\lambda_0)^\ell \rangle$, but $f(x) \notin \langle (x^4-\lambda_0)^{\ell+1} \rangle$, and in particular, $f(x) \notin C$. This proves that any nonzero polynomial of degree less than $4i - 4(a-1)p^s$ is not in C, i.e. the smallest degree of nonzero polynomials in C is $4i - 4(a-1)p^s$, as desired. □

We can determine the RT weight distributions of the Type 1 Λ-constacyclic code.

Proposition 4.3 *For $(a-1)p^s+1 \leq i \leq ap^s-1$, we get the RT weight distribution of the Type 1 Λ-constacyclic code $\langle (x^4 - \lambda_0)^i \rangle \subseteq \mathcal{S}_a(s, \Lambda)$:*

$$A_j = \begin{cases} 1 & \text{if } j = 0 \\ 0 & \text{if } 1 \leq j \leq 4i - 4(a-1)p^s \\ (p^m - 1)p^{mk} & \text{if } j = 4i - 4(a-1)p^s + 1 + k, \text{ for } 0 \leq k \leq 4ap^s - 4i - 1, \end{cases}$$

where A_j is the number of codewords of RT weight j of $\langle (x^4 - \lambda_0)^i \rangle$.

Proof Similar to the proof of Theorem 4.2, if $(a-1)p^s + 1 \leq i \leq ap^s - 1$, then $\left\langle (x^4 - \lambda_0)^i \right\rangle = \left\langle u^{a-1}(x^4 - \lambda_0)^{i-(a-1)p^s} \right\rangle$. It follows that $A_j = 0$ for $1 \leq j \leq 4i-4(a-1)p^s$. When $4i-4(a-1)p^s+1 \leq j \leq 4p^s$, say, $j = 4i - 4(a-1)p^s + 1 + k$, for $0 \leq k \leq 4ap^s - 4i - 1$, we can see that A_j is the number of distinct polynomials of degree k in $\mathbb{F}_{p^m}[x]$. Therefore, $A_j = (p^m - 1)p^{mk}$. □

When $i = p^s t$, $0 \leq t \leq a-1$, by Lemma 3.4, the ideals $\langle (x^4 - \lambda_0)^i \rangle = \langle u^t \rangle \subseteq \mathcal{S}_a(s, \Lambda)$. Then the weight distributions of such codes are given in the following proposition.

Proposition 4.4 *For $i = p^s t$, $0 \leq t \leq a-1$, the RT weight distribution of the Λ-constacyclic code $\langle (x^4 - \lambda_0)^i \rangle \subseteq \mathcal{S}_a(s, \Lambda)$ is as follows:*

$$A_j = \begin{cases} 1 & \text{if } j = 0 \\ \left(p^{m(a-t)} - 1\right) p^{m(a-t)(j-1)} & \text{if } 1 \leq j \leq 4p^s, \end{cases}$$

where A_j is the number of codewords of RT weight j of $\langle (x^4 - \lambda_0)^i \rangle$.

Proposition 4.5 *Let $1 \leq b \leq a-1$. For $(b-1)p^s+1 \leq i \leq bp^s-1$, we can determine the RT weight distribution of the Λ-constacyclic code $\langle (x^4-\lambda_0)^i\rangle \subseteq \mathcal{S}_a(s,\Lambda)$ as follows:*

$$A_j = \begin{cases} 1 & \textit{if } \ j=0 \\ \left(p^{m(a-b)}-1\right)p^{m(a-b)(j-1)} & \textit{if } \ 1 \leq j \leq 4i-4(b-1)p^s \\ p^{4m(a-b)p^s}(p^m-1)p^{mk} + \left(p^{m(a-b)}-1\right)p^{m(a-b)(j-1)} & \textit{if } \ j = 4i-4(b-1)p^s+1+k, \\ & \quad \textit{for } 0 \leq k \leq 4bp^s-4i-1, \end{cases}$$

where A_j is the number of codewords of RT weight j of $\langle (x^4-\lambda_0)^i\rangle$.

Proof By assumption, we have $(b-1)p^s+1 \leq i \leq (b-1)p^s+p^s-1$, i.e. $1 \leq i-(b-1)p^s \leq p^s-1$. Applying Lemma 3.4 again, we have

$$\left\langle u^{b-1}(x^4-\lambda_0)\right\rangle \supseteq \left\langle (x^4-\lambda_0)^i\right\rangle = \left\langle u^{b-1}(x^4-\lambda_0)^{i-p^s(b-1)}\right\rangle \supseteq \left\langle u^{b-1}(x^4-\lambda_0)^{p^s-1}\right\rangle \supsetneq \left\langle u^b\right\rangle.$$

Let B_j be the number of codewords of RT weight j of $\langle (x^4-\lambda_0)^i\rangle$, which are not in $\langle u^b\rangle$, and B'_j be the number of codewords of RT weight j of $\langle u^b\rangle$. Then, for all j, $A_j = B_j + B'_j$. Similar to Proposition 4.3, we get

$$B_j = \begin{cases} 0 & \text{if } \ j=0 \\ 0 & \text{if } \ 1 \leq j \leq 4i-4(b-1)p^s \\ p^{4m(a-b)p^s}(p^m-1)p^{mk} & \text{if } \ j = 4i-4(b-1)p^s+1+k, \\ & \quad \text{for } 0 \leq k \leq 4bp^s-4i-1. \end{cases}$$

From Proposition 4.4, it is easy to see that

$$B'_j = \begin{cases} 1 & \text{if } \ j=0 \\ \left(p^{m(a-b)}-1\right)p^{m(a-b)(j-1)} & \text{if } \ 1 \leq j \leq 4p^s. \end{cases}$$

This implies that

$$A_j = \begin{cases} 1 & \text{if } \ j=0 \\ \left(p^{m(a-b)}-1\right)p^{m(a-b)(j-1)} & \text{if } \ 1 \leq j \leq 4i-4(b-1)p^s \\ p^{4m(a-b)p^s}(p^m-1)p^{mk} + \left(p^{m(a-b)}-1\right)p^{m(a-b)(j-1)} & \text{if } \ j = 4i-4(b-1)p^s+1+k, \\ & \quad \text{for } 0 \leq k \leq 4bp^s-4i-1. \end{cases}$$ □

Remark 4.6 Propositions 4.3, 4.4, and 4.5 give us the RT weight distributions for all λ-constacyclic codes $C_i = \langle (x^4-\lambda_0)^i\rangle \subseteq \mathcal{S}_a(s,\Lambda)$ of length $4p^s$ over $\mathcal{R}_a$. By Theorem 3.5, $|C_i| = p^{4m(ap^s-i)}$. Since $|C_i| = \sum_{j=0}^{4p^s} A_j$, we can see that these RT weight distributions can be used to verify the size $|C_i|$ of such codes.

- If $(a-1)p^s+1 \leq i \leq ap^s-1$, then

$$\begin{aligned}|C_i| &= \sum_{j=0}^{4p^s} A_j \\ &= 1 + \sum_{k=0}^{4ap^s-4i-1} (p^m-1)p^{mk} \\ &= 1 + (p^m-1)\sum_{k=0}^{4ap^s-4i-1} (p^m)^k \\ &= 1 + (p^m-1)\frac{p^{m(4ap^s-4i)}-1}{p^m-1} \\ &= p^{4m(ap^s-i)}.\end{aligned}$$

- If $i = p^s t,\ 0 \leq t \leq a-1$, then

$$\begin{aligned}|C_i| &= \sum_{j=0}^{4p^s} A_j \\ &= 1 + \sum_{j=1}^{4p^s} \left(p^{m(a-t)}-1\right) p^{m(a-t)(j-1)} \\ &= 1 + \left(p^{m(a-t)}-1\right) \sum_{j=0}^{4p^s-1} p^{m(a-t)j} \\ &= 1 + \left(p^{m(a-t)}-1\right) \frac{p^{m(a-t)4p^s}-1}{p^{m(a-t)}-1} \\ &= p^{4m(a-t)p^s} \\ &= p^{4m(ap^s-i)}.\end{aligned}$$

- If $(b-1)p^s+1 \leq i \leq bp^s-1$, where $1 \leq b \leq a-1$, then

$$\begin{aligned}|C_i| &= \sum_{j=0}^{4p^s} A_j \\ &= 1 + \sum_{j=1}^{4i-4(b-1)p^s} \left(p^{m(a-b)}-1\right) p^{m(a-b)(j-1)} + \\ &\quad + \sum_{k=0}^{4bp^s-4i-1} p^{4m(a-b)p^s}(p^m-1)p^{mk} + \sum_{j=4i-4(b-1)p^s+1}^{4p^s} \left(p^{m(a-b)}-1\right) p^{m(a-b)(j-1)} \\ &= 1 + \left(p^{m(a-b)}-1\right) \sum_{j=0}^{4p^s-1} p^{m(a-b)j} + p^{4m(a-b)p^s}(p^m-1) \sum_{k=0}^{4bp^s-4i-1} p^{mk}\end{aligned}$$

$$
\begin{aligned}
&= 1 + \left(p^{m(a-b)} - 1\right) \frac{p^{m(a-b)4p^s} - 1}{p^{m(a-b)} - 1} + p^{4m(a-b)p^s} (p^m - 1) \frac{p^{m(4bp^s-4i)} - 1}{p^m - 1} \\
&= 1 + \left(p^{m(a-b)4p^s} - 1\right) + p^{4m(a-b)p^s} \left(p^{m(4bp^s-4i)} - 1\right) \\
&= p^{4m(ap^s-i)}.
\end{aligned}
$$

Maximum distance separable (MDS) codes form an optimal class of codes. A MDS code has a very strong error correction capability, especially when the code length is not very long. To determine a MDS code with respect to RT distance, we need to give the Singleton bound of the RT distance first. Let C be a linear code of length n over $\mathcal{R}_a$ with RT distance $d_{\mathrm{RT}}(C)$. Mark the first $d_{\mathrm{RT}}(C)-1$ entries of each codeword of C, and then two different codewords of C cannot coincide in all other $n - d_{\mathrm{RT}}(C) + 1$ entries. Otherwise, C would have a nonzero codeword of RT weight less than or equal to $d_{\mathrm{RT}}(C) - 1$. Therefore, C can contain at most $p^{am(n-d_{\mathrm{RT}}(C)+1)}$ codewords. Then the Singleton bound for the RT distance is given by the following result.

Theorem 4.7 (Singleton bound for RT distance) *Let C be a linear code of length n over $\mathbb{F}_{p^m}$ with RT distance $d_{\mathrm{RT}}(C)$. Then $|C| \leq p^{am(n-d_{\mathrm{RT}}(C)+1)}$.*

When a code C attains this Singleton bound, i.e. $|C| = p^{am(n-d_{\mathrm{RT}}+1)}$, it is said to be a MDS code (with respect to the RT distance). We now point out the unique MDS Type 1 constacyclic codes of length $4p^s$ over $\mathcal{R}_a$ with respect to the RT distance.

Theorem 4.8 *The only MDS Type 1 Λ-constacyclic code of length $4p^s$ over $\mathcal{R}_a$, with respect to the RT distance, is the whole ambient ring $\mathcal{S}_a(s,\Lambda)$.*

Proof Let C be a nonzero Type 1 Λ-constacyclic code of length $4p^s$ over $\mathcal{R}_a$. By Theorem 3.5, $C = \langle (x^4 - \lambda_0)^i \rangle \subseteq \mathcal{S}_a(s,\Lambda)$, for some integer $i \in \{0, 1, \ldots, ap^s - 1\}$, and $|C| = p^{4m(ap^s-i)}$. Applying Theorem 4.2, we can see that if $0 \leq i \leq (a-1)p^s$, then $d_{\mathrm{RT}}(C) = 1$, and $4p^s - d_{\mathrm{RT}}(C) + 1 = 4p^s$. This shows that

$$
\begin{aligned}
C \text{ is MDS} \quad &\leftrightarrow \quad |C| = p^{am(4p^s - d_{\mathrm{RT}}(C)+1)} \\
&\leftrightarrow \quad p^{4m(ap^s-i)} = p^{4amp^s} \\
&\leftrightarrow \quad ap^s - i = ap^s \\
&\leftrightarrow \quad i = 0.
\end{aligned}
$$

If $(a-1)p^s + 1 \leq i \leq ap^s - 1$, then, using Theorem 4.2 again, we get $d_{\mathrm{RT}}(C) = 4i - 4(a-1)p^s + 1$, and $4p^s - d_{\mathrm{RT}}(C) + 1 = 4ap^s - 4i$. Therefore,

$$
\begin{aligned}
C \text{ is MDS} \quad &\leftrightarrow \quad |C| = p^{am(4p^s - d_{\mathrm{RT}}(C)+1)} \\
&\leftrightarrow \quad p^{4m(ap^s-i)} = p^{am(4ap^s-4i)} \\
&\leftrightarrow \quad ap^s - i = a^4 p^s - ai \\
&\leftrightarrow \quad (a-1)i = (a^4 - a)p^s \\
&\leftrightarrow \quad i = ap^s,
\end{aligned}
$$

which is impossible since $(a-1)p^s + 1 \leq i \leq ap^s - 1$.

Therefore, the code $C = \langle (x^4 - \lambda_0)^i \rangle \subseteq \mathcal{S}_a(s,\Lambda)$ is MDS if and only if $i = 0$, i.e., $C = \mathcal{S}_a(s,\Lambda)$. □

5. Conclusion

In this paper, assuming $p^m \equiv 1 \pmod 4$, we investigate Type 1 Λ-constacyclic codes of length $4p^s$ over the $\mathcal{R}_a$, i.e. the unit Λ has the form

$$\Lambda = \Lambda_0 + u\Lambda_1 + \cdots + u^{a-1}\Lambda_{a-1},$$

where $\Lambda_0, \Lambda_1, \ldots, \Lambda_{a-1} \in \mathbb{F}_{p^m}$, $\Lambda_0 \neq 0$, $\Lambda_1 \neq 0$. If Λ is a square, each Λ-constacyclic code of length $4p^s$ is expressed as a direct sum of a -λ-constacyclic code and a λ-constacyclic code of length $2p^s$. In the main consideration when Λ is not a square, we first prove an important observation that any nonzero polynomial of degree less than 4 in $\mathbb{F}_{p^m}[x]$ is invertible in $\mathcal{S}_a(a, \Lambda)$. This key result is then used to obtain that the ambient ring $\mathcal{S}_a(a, \Lambda)$ is a chain ring with maximal ideal $\langle x^4 - \lambda_0 \rangle$. From this, we give the number of codewords and the dual of each Λ-constacyclic code. In addition, the RT distances and weight distributions of such codes are also determined. These results allow us to provide the only MDS Type 1 Λ-constacyclic code of length $4p^s$ over $\mathcal{R}_a$, with respect to the RT distance.

The condition that $p^m \equiv 1 \pmod 4$ is critical in our consideration. In fact, if $p^m \equiv 3 \pmod 4$, the key result that all nonzero polynomials of degree less than 4 in $\mathbb{F}_{p^m}[x]$ are invertible in $\mathcal{S}_a(a, \Lambda)$ is no longer true. It can be shown that, in that case, the polynomial $x^4 - \lambda_0$ can be decomposed as a product of 2 quadratic irreducible factors. We illustrate that in the following example.

Example 5.1 *We consider the finite commutative chain ring* $\mathcal{R}_4 = \mathbb{F}_{11} + u\mathbb{F}_{11} + u^2\mathbb{F}_{11} + u^3\mathbb{F}_{11} (u^4 = 0)$ *and* $\Lambda = 7 + u$. *It is clear that* $\Lambda_0 = 7$ *is not a square in* $\mathbb{F}_{11}$, *and by applying Proposition 3.2,* $7 + u$ *is not a square. The ambient ring of the* $(7+u)$*-constacyclic codes of length* $4 \cdot 11^2$ *over* $\mathbb{F}_{11} + u\mathbb{F}_{11} + u^2\mathbb{F}_{11} + u^3\mathbb{F}_{11}$ *is*

$$\mathcal{S}_4(4, 7+u) = \frac{(\mathbb{F}_{11} + u\mathbb{F}_{11} + u^2\mathbb{F}_{11} + u^3\mathbb{F}_{11})[x]}{\langle x^{4\cdot 11^2} - (7+u)\rangle}.$$

Observe that $7^5 \equiv (-1) \pmod{11}$, *and hence* $7^{10} \equiv 1 \pmod{11}$. *This implies that* $7^{11^2} = 7^{121} \equiv 7 \pmod{11}$. *Therefore, in* $\mathcal{S}_4(4, 7+u)$, *we have*

$$0 = x^{4\cdot 11^2} - (7+u) = x^{4\cdot 11^2} - 7^{11^2} - u = (x^4 - 7)^{11^2} - u,$$

i.e. $(x^4 - 7)^{11^2} = u$, *implying* $x^4 - 7$ *is nilpotent. However,* $x^4 - 7$ *can be decomposed as a product of* 2 *quadratic irreducible factors as follows:*

$$\begin{aligned} x^4 - 7 &= x^4 + 4 \\ &= (x^4 + 4x^2 + 4) - 4x^2 \\ &= (x^2 + 2)^2 - (2x)^2 \\ &= (x^2 + 2x + 2)(x^2 - 2x + 2). \end{aligned}$$

In fact, suppose that $(x^2 + 2x + 2)$ *and* $(x^2 - 2x + 2)$ *are reducible polynomials. Then* $(x^2 + 2x + 2)$ *and* $(x^2 - 2x + 2)$ *can be expressed as a product of* 2 *nonzero linear polynomials. Because any nonzero linear polynomial is invertible in* $\mathcal{S}_4(4, 7+u)$, *we conclude that* $x^4 - 7$ *is invertible in* $\mathcal{S}_4(4, 7+u)$, *which is a contradiction. This implies that* $(x^2 + 2x + 2)$ *and* $(x^2 - 2x + 2)$ *are irreducible polynomials in* $\mathcal{S}_4(4, 7+u)$. *Thus, Theorem 3.3 is not true when* $p^m \ \equiv 3 \pmod 4$.

This paper considered the Type 1 Λ-constacyclic codes of length $4p^s$ over $\mathcal{R}$, where $p^m \equiv 1 \pmod 4$. The class of Type 1 Λ-constacyclic codes of length $4p^s$ over $\mathcal{R}$, where $p^m \equiv 3 \pmod 4$ is investigated in our other paper [24].

Acknowledgments

We would like to thank the referees for their comments and suggestions on the manuscript. This work was partially supported by a grant from the Niels Hendrik Abel Board.

H.Q. Dinh and S. Sriboonchitta are grateful to the Centre of Excellence in Econometrics, Chiang Mai University, for partial financial support. This research is partially supported by the Research Administration Centre, Chaing Mai University. The second author is grateful to the Foundation for Science and Technology Development, Nguyen Tat Thanh University, for partial financial support.

References

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

[2] Amarra MCV, Nemenzo FR. On $(1-u)$-cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$. Applied Mathematics Letters 2008; 21: 1129-1133.

[3] Berlekamp ER. Algebraic Coding Theory, Revised 1984 Edition. Walnut Creek, CA, USA: Aegean Park Press, 1984.

[4] Berlekamp ER. Negacyclic codes for the Lee metric. In: Proceedings of the Conference on Combinatorial Mathematics and Its Application. Chapel Hill, NC, USA, 1968, pp. 298-316.

[5] Berman SD. Semisimple cyclic and Abelian codes. II. Kibernetika (Kiev) 1967; 3: 21-30 (in Russian).

[6] Blackford T. Cyclic codes over $\mathbb{Z}_4$ of oddly even length. Appl Discr Math 2003; 128: 27-46.

[7] Bonnecaze A, Udaya P. Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE T Inform Theory 1999; 45: 1250-1255.

[8] Bonnecaze A, Udaya P. Decoding of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE T Inform Theory 1999; 45: 2148-2157.

[9] Bonnecaze A, Udaya P. Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE T Inform Theory 1999; 45: 1250-1255.

[10] Calderbank AR, Hammons AR, Kumar PV, Sloane NJA, Solé P. A linear construction for certain Kerdock and Preparata codes. B Am Math Soc 1993; 29: 218-222.

[11] Castagnoli G, Massey JL, Schoeller PA, von Seemann N. On repeated-root cyclic codes. IEEE T Inform Theory 1991; 37: 337-342.

[12] Chen B, Dinh HQ, Liu H, Wang L. Constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Finite Fields and Their Applications 2016; 36: 108-130.

[13] Chen B, Lin L, Liu H. Matrix product codes with Rosenbloom-Tsfasma metric. Acta Math Sci 2013; 33B: 687-700.

[14] Dinh HQ. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. Finite Fields Appl 2008; 14: 22-40.

[15] Dinh HQ. Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE T Inform Theory 2009; 55: 1730-1740.

[16] Dinh HQ. Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. J Algebra 2010; 324: 940-950.

[17] Dinh HQ. Repeated-root constacyclic codes of length $2p^s$. Finite Fields Appl 2012; 18: 133-143.

[18] Dinh HQ. Structure of repeated-root constacyclic codes of length $3p^s$ and their duals. Discrete Math 2013; 313: 983-991.

[19] Dinh HQ. Structure of repeated-root cyclic and negacyclic codes of length $6p^s$ and their duals. AMS Contemporary Mathematics 2014; 339: 69-87.

[20] Dinh HQ, Dhompongsa S, Sriboonchitta S. Repeated-root constacyclic codes of prime power length over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^a \rangle}$ and their duals. Discrete Math 2016; 339: 1706-1715.

[21] Dinh HQ, Dhompongsa S, Sriboonchitta S. On constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Discrete Math 2017; 340: 832-849.

[22] Dinh HQ, López-Permouth SR. Cyclic and negacyclic codes over finite chain rings. IEEE T Inform Theory 2004; 50: 1728-1744.

[23] Dinh HQ, Nguyen BT, Sriboonchitta S. On a class of constacyclic codes of length $2p^s$ over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^a \rangle}$. Bulletin of the Korean Mathematical Society, 2018; 4: 1189-1208.

[24] Dinh HQ, Nguyen BT, Sriboonchitta S. On A Class Of Constacyclic Codes Of Length 4p s Over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^a \rangle}$. Algebra Colloquium. (accepted).

[25] Dinh HQ, Wang L, Zhu S. Negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Finite Fields Appl 2015; 31: 178-201.

[26] Dougherty S, Gaborit P, Harada M, Sole P. Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE T Inform Theory 1999; 45: 32-45.

[27] Dougherty ST, Skriganov MM. Macwilliams duality and Rosenbloom-Tsfasman metric. Moscow Math J 2002; 2: 81-97.

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

[29] Hammons AR, Kumar PV, Calderbank AR, Sloane NJA, Solé P. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE T Inform Theory 1994; 40: 301-319.

[30] Huffman WC, Pless V. Fundamentals of Error-Correcting Codes. Cambridge, UK: Cambridge University Press, 2003.

[31] Lee K. Automorphism group of the Rosenbloom-Tsfasman space. Eur J Combin 2003; 24: 607-612.

[32] Ling S, Solé P. Duadic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. Appl Algebra Engrg Comm Comput 2001; 12: 365-379.

[33] Massey JL, Costello DJ, Justesen J. Polynomial weights and code constructions. IEEE T Inform Theory 1973; 19: 101-110.

[34] McDonald BR. Finite Rings with Identity. Pure and Applied Mathematics. New York, NY, USA: Marcel Dekker, 1974.

[35] Nechaev AA. Kerdock code in a cyclic form. Diskr Math (USSR) 1989; 1: 123-139 (in Russian).

[36] Nedeloaia CS. Weight distributions of cyclic self-dual codes. IEEE T Inform Theory 2003; 49: 1582-1591.

[37] Norton G, Sălăgean-Mandache A. On the structure of linear cyclic codes over finite chain rings. Appl Algebra Engrg Comm Comput 2000; 10: 489-506.

[38] Pless V, Huffman WC. Handbook of Coding Theory. Amsterdam, the Netherlands: Elsevier, 1998.

[39] Prange E. Cyclic error-correcting codes in two symbols. TN 1957; 57-103.

[40] Prange E. Some cyclic error-correcting codes with simple decoding algorithms. TN 1958; 58-156.

[41] Prange E. The use of coset equivalence in the analysis and decoding of group codes. TN 1959; 59-164.

[42] Prange E. An algorithm for factoring $x^n - 1$ over a finite field. TN 1959; 59-175.

[43] Rosenbloom MY, Tsfasman MA. Codes for the m-metric. Problems Inf Trans 1997; 33: 45-52.

[44] Roth RM, Seroussi G. On cyclic MDS codes of length q over $\mathrm{GF}(q)$. IEEE T Inform Theory 1986; 32: 284-285.

[45] Skriganov MM. On linear codes with large weights simultaneously for the Rosenbloom-Tsfasman and Hamming metrics. J Complexity 2007; 23: 926-936.

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

[47] van Lint JH. Repeated-root cyclic codes. IEEE T Inform Theory 1991; 37: 343-345.