Journal of Algebra and Its Applications
(2019) 1950023 (16 pages)

DOI: 10.1142/S0219498819500233

On $(\alpha + u\beta)$-constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*

Hai Q. Dinh[*,†,‡,††], Bac T. Nguyen[‡,§,¶,‡‡], Songsak Sriboonchitta[‖,§§] and Thang M. Vo[‡,**,¶¶]

[*]*Division of Computational Mathematics and Engineering*
Institute for Computational Science
Ton Duc Thang University, Ho Chi Minh City, Vietnam

[†]*Faculty of Mathematics and Statistics*
Ton Duc Thang University
Ho Chi Minh City, Vietnam

[‡]*Department of Mathematical Sciences*
Kent State University, 4314 Mahoning Avenue
Warren, OH 44483, USA

[§]*Department of Basic Sciences, University*
of Economics and Business Administration
Thai Nguyen University, Thai Nguyen Province, Vietnam

[¶]*Nguyen Tat Thanh University*
300 A Nguyen Tat Thanh Street
Ho Chi Minh City, Vietnam

[‖]*Faculty of Economics, Chiang Mai University*
Chiang Mai 52000, Thailand

[**]*Department of Personnel and Organization*
Vinh University of Technology Education
Vinh City Nghe An, Vietnam
[††]*dinhquanghai@tdt.edu.vn*
[‡‡]*bacnt2008@gmail.com*
[§§]*songsakecon@gmail.com*
[¶¶]*vomanhthang@vute.edu.vn*

Received 24 December 2017
Accepted 5 January 2018
Published 26 March 2018

Communicated by S. R. López-Permouth

For any odd prime p such that $p^m \equiv 3 \pmod 4$, the structures of all $(\alpha+u\beta)$-constacyclic codes of length $4p^s$ over the finite commutative chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ $(u^2 = 0)$ are established in term of their generator polynomials. When the unit $(\alpha+u\beta)$ is a square, each $(\alpha + u\beta)$-constacyclic code of length $4p^s$ is expressed as a direct sum of two constacyclic codes of length $2p^s$. In the main case that the unit $(\alpha + u\beta)$ is not a square, it is shown that the ambient ring $\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle x^{4p^s}-(\alpha+u\beta)\rangle}$ is a principal ideal ring. From that, the structure, number of codewords, duals of all such $(\alpha + u\beta)$-constacyclic codes

are obtained. As an application, we identify all self-orthogonal, dual-containing, and the unique self-dual $(\alpha + u\beta)$-constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$.

Keywords: Constacyclic codes; dual codes; repeated-root codes; codes over rings; chain rings.

Mathematics Subject Classification 2010: 94B15, 94B05, 11T71

1. Introduction

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

The class of finite commutative chain rings of the form $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where $u^2 = 0$, has been widely used as alphabets for constacyclic codes. For example, the structure of $\mathbb{F}_2 + u\mathbb{F}_2$ is interesting, it is lying between $\mathbb{F}_4$ and $\mathbb{Z}_4$ in the sense that it is additively analogous to $\mathbb{F}_4$, and multiplicatively analogous to $\mathbb{Z}_4$. It has been studied by a lot of researchers (see, for example, [1, 2, 5, 13, 17, 18]).

The classification of codes has an important role in studying their structures, but in general, it is very difficult to do so. Over the last few years, in a series of papers [3, 5–8], Dinh *et al.* have done this job of classifying classes of constacyclic codes of certain lengths over certain finite fields or finite chain rings. In 2009 [5], all constacyclic codes of length 2^s over the Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$ are classified and their detailed structures are also established. Then in 2010 [6], we classified and gave the detailed structures of all constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$; and in 2012 [7] and 2013 [8], we provided that for all constacyclic codes of length $2p^s$ and $4p^s$ over the finite field $\mathbb{F}_{p^m}$. In 2015 and 2016, the structures of negacyclic codes, and then more generally, all constacyclic codes, of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, were established in [12] and [3], respectively.

Recently, in 2017, Dinh *et al.* [9] continued this line of research to investigate constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ in the case where p is an odd prime such that $p^m \equiv 1 \pmod 4$. The key result was that, when the unit λ is not a square in $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, any nonzero polynomial of degree <4 over $\mathbb{F}_{p^m}$ is invertible in the ambient ring $\frac{(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x]}{\langle x^{4p^s} - \lambda \rangle}$ of constacyclic codes of length $4p^s$ (cf. [9, Propositions 4.1 and 5.1]). This fact was then be used to obtain the algebraic structure of all constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and their duals. However, [9, Sec. 6] explained that this fact is no longer true for the case $p^m \equiv 3 \pmod 4$.

Notice that there are two types of units of the ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, namely, $\alpha + u\beta$ and γ, where $\alpha, \beta, \gamma \in \mathbb{F}_{p^m}^*$. Motivated by that, in this paper, we study

$(\alpha + u\beta)$-constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ for the remaining case of $p^m \equiv 3 \pmod 4$, which is the hypothesis we use throughout the paper. The remaining case of γ-constacyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ for $\gamma \in \mathbb{F}_{p^m}^*$ is considered in our recent paper [11].

This paper is organized as follows. Section 2 gives preliminary concepts, including a discussion of the easier case that the unit λ is a square in the ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. In this case, each λ-constacyclic code of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ is represented as a direct sum of an $-\alpha$-constacyclic and an α-constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where the structures of such constacyclic codes were given in [3]. The rest of the paper considers the main case that the unit $(\alpha + u\beta)$ is not a square in $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. In Sec. 3, we show that $x^4 - \alpha_0$ factors into a product of two pairwise coprime irreducible quadratic factors. It then will be shown that the ambient ring $\frac{(\mathbb{F}_{p^m} + u\mathbb{F}_{p^m})[x]}{\langle x^{4p^s} - (\alpha + u\beta)\rangle}$ is a principal ideal ring, which gives the structure of all $(\alpha + u\beta)$-constacyclic codes. Using this structure, Sec. 4 establishes all duals codes, and identifies the unique self-dual $(\alpha + u\beta)$-constacyclic code, as well as all self-orthogonal and dual-containing codes.

2. Preliminaries

An ideal I of a ring R is called *principal* if it is generated by one element. A ring R is a principal ideal ring if its ideals are principal. R is called a local ring if $R/\mathrm{rad}\, R$ is a division ring, or equivalently, if R has a unique maximal right (left) ideal. Furthermore, a ring R is called a chain ring if the set of all right (left) ideals of R is linearly ordered under set-theoretic inclusion. The following equivalent conditions are known for the class of finite commutative rings (cf. [10, Proposition 2.1]).

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

(i) *R is a local ring and the maximal ideal M of R is principal, i.e. $M = \langle\gamma\rangle$ for some $\gamma \in R$,*
(ii) *R is a local principal ideal ring,*
(iii) *R is a chain ring whose ideals are $\langle\gamma^i\rangle$, $0 \le i \le N(\gamma)$, where $N(\gamma)$ is the nilpotency of γ.*

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

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

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

Each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ 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 that, the following fact is well known (cf. [14, 15]) and straightforward.

Proposition 2.2. *A linear code C of length n is λ-constacyclic over R if and only if C is an ideal of the quotient ring $\frac{R[x]}{\langle x^n-\lambda\rangle}$. (Hence, this quotient ring is referred to as the ambient ring of the code C.)*

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 as usual

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

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

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

A code C is called *self-orthogonal* if $C \subseteq C^\perp$, and it is called *self-dual* if $C = C^\perp$. The following result is well known (cf. [4, 14–16]).

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

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

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

In this paper, for any odd prime p with $p^m \equiv 3 \pmod 4$, we will consider constacyclic codes of length $4p^s$ over the ring $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. The ring R consists of all p^m-ary polynomials of degree 0 and 1 in indeterminate u, it is closed under p^m-ary polynomial addition and multiplication modulo u^2. Thus, $R = \frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle} = \{a + ub \,|\, a, b \in \mathbb{F}_{p^m}\}$ is a local ring with maximal ideal $u\mathbb{F}_{p^m}$, and hence, it is a chain ring.

Hereafter, for any unit λ of R, we denote the ambient ring of λ-constacyclic codes of length $4p^s$ over R as

$$\mathcal{R}_\lambda = \frac{R[x]}{\langle x^{4p^s} - \lambda\rangle}.$$

Then, by Proposition 2.2, constacyclic codes of length $4p^s$ over R are ideals of $\mathcal{R}_\lambda$.

Definition 2.5. If

$$f(x) = a_0 + a_1x + \cdots + a_rx^r$$

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

$$f^*(x) = a_r + a_{r-1}x + a_{r-2}x^2 + \cdots + a_0x^r.$$

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

Definition 2.6. Let I be an ideal of $\mathcal{R}_\lambda$. We define $\text{ann}(I) = \{g(x) \mid f(x)g(x) = 0, \forall f(x) \in I\}$. Then $\text{ann}(I)$ is called the annihilator of I, which is also an ideal of $\mathcal{R}_\lambda$.

From the above definition we can see that if C is a constacyclic code of length n over R with associated ideal I (which is an ideal of $\mathcal{R}_\lambda$), then the associated ideal of $C^\perp$ is $\text{ann}(I)^*$ (which is an ideal of $\mathcal{R}_{\lambda^{-1}}$.) The following lemma is easy to prove and will be used in Sec. 4.

Lemma 2.7.

(a) $(f(x)g(x))^* = f^*(x)g^*(x)$.
(b) *If* $\deg f \geq \deg g$, *then*

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

(c) *More generally, if* $\deg f \geq \deg g_i$, *for* $1 \leq i \leq k$, *then*

$$\left(f(x) + \prod_{i=1}^{k} g_i(x)\right)^* = f^*(x) + \prod_{i=1}^{k} x^{\deg f - \deg g_i} g_i^*(x).$$

(d) *Let* C *be an ideal of* $\mathcal{R}_\lambda$, *then* $C^\perp = \text{ann}(C)^*$, *which is an ideal of* $\mathcal{R}_{\lambda^{-1}}$.

An element $a + ub$ of R ($a, b \in \mathbb{F}_{p^m}$) is invertible if and only if $a \neq 0$. Hence, the ring R has $p^m(p^m - 1)$ units, and we categorize them into two types, namely, $\alpha + u\beta$, and γ, where α, β, γ are nonzero elements of the field $\mathbb{F}_{p^m}$. In this paper, unless otherwise stated, we will assume that p is a prime such that $p^m \equiv 3 \pmod 4$, and we focus on the case the unit λ is of the form $\alpha + u\beta$.

When the unit λ is a square, i.e. there exists a unit $\alpha \in R$ such that $\lambda = \alpha^2$, we have

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

And hence, by the Chinese reminder theorem,

$$\mathcal{R}_\lambda \cong \frac{R[x]}{\langle x^{2p^s} + \alpha\rangle} \oplus \frac{R[x]}{\langle x^{2p^s} - \alpha\rangle}.$$

It follows that ideals of $\mathcal{R}_\lambda$ are of the form $A \oplus B$, where A and B are ideals of $\frac{R[x]}{\langle x^{2p^s}+\alpha\rangle}$ and $\frac{R[x]}{\langle x^{2p^s}-\alpha\rangle}$, respectively, i.e. they are $-\alpha$- and α-constacyclic codes of

length $4p^s$ over R. It means that any λ-constacyclic code of length $4p^s$ over R, i.e. an ideal C of $\mathcal{R}$, is represented as a direct sum of C_+ and C_-:

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

where C_+ and C_- are ideals of $\frac{R[x]}{\langle x^{2p^s}+\alpha\rangle}$ and $\frac{R[x]}{\langle x^{2p^s}-\alpha\rangle}$, respectively. Thus, the classification, detailed structure, and number of codewords of constacyclic codes C of length $4p^s$ over R can be obtained from that of the direct summands C_+ and C_- (cf. [3]). It turns out that the dual code $C^\perp$ of C is also a direct sum of the dual codes of the direct summands $C_+^\perp$ and $C_-^\perp$.

Theorem 2.8. *Let the unit $\lambda = \alpha^2 \in R$, and $C = C_+ \oplus C_-$ be a constacyclic code of length $4p^s$ over R, where C_+, C_- are ideals of $\frac{R[x]}{\langle x^{2p^s}+\alpha\rangle}$, $\frac{R[x]}{\langle x^{2p^s}-\alpha\rangle}$, respectively. Then*

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

In particular, C is a self-dual constacyclic code of length $4p^s$ over R if and only if C_+, C_- are self-dual $-\alpha$-constacyclic code and self-dual α-constacyclic code of length $2p^s$ over R, respectively.

Proof. Clearly, $C_+^\perp \oplus C_-^\perp \subseteq C^\perp$. Now,

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

Thus, $C^\perp = C_+^\perp \oplus C_-^\perp$. □

3. Structure of $(\alpha + u\beta)$-Constacyclic Codes

In this section, we consider the case that the unit λ is of the form $\lambda = \alpha + u\beta$ for nonzero elements α, β of $\mathbb{F}_{p^m}$, and λ is not a square in R. By Proposition 2.2, the $(\alpha + u\beta)$-constacyclic codes of length $4p^s$ are ideals of the ambient ring

$$\mathcal{R}_{\alpha,\beta} = \frac{R[x]}{\langle x^{4p^s} - (\alpha + u\beta)\rangle}.$$

It is worth noting that $\alpha + u\beta$ is not a square in R if and only if α is not a square in $\mathbb{F}_{p^m}$. Otherwise, if $\alpha = \alpha'^2 \in \mathbb{F}_{p^m}$, then $\alpha + u\beta = (\alpha' + u\beta')^2$, where $\beta' = 2^{-1}\alpha'^{-1}\beta$.

Since $\alpha \in \mathbb{F}_{p^m}$, $\alpha^{p^m} = \alpha$, and so $\alpha^{p^{tm}} = \alpha$, for any positive integer t. By the Division Algorithm, there exist non-negative integers α_q, α_r such that $s = \alpha_q m + \alpha_r$, and $0 \le \alpha_r \le m-1$. Let $\alpha_0 = \alpha^{p^{(\alpha_q+1)m-s}} = \alpha^{p^{m-\alpha_r}}$. Then $\alpha_0^{p^s} = \alpha^{p^{(\alpha_q+1)m}} = \alpha$. Clearly, α is not a square if and only if α_0 is not a square. Moreover, in $\mathcal{R}_{\alpha,\beta}$, $(x^4 - \alpha_0)^{p^s} = x^{4p^s} - \alpha = u\beta$. We summarize the above discussion in the following proposition.

Proposition 3.1. *Let $\alpha_0 \in \mathbb{F}_{p^m}$ be such that $\alpha = \alpha_0^{p^s}$. In $\mathcal{R}_{\alpha,\beta}$, $\langle (x^4 - \alpha_0)^{p^s}\rangle = \langle u\rangle$. In particular, $x^4 - \alpha_0$ is nilpotent with nilpotency index $2p^s$.*

Proposition 3.2. *The following hold true*:

(i) *Any nonzero linear polynomial $cx + d \in \mathbb{F}_{p^m}[x]$ is invertible in $\mathcal{R}_{\alpha,\beta}$.*
(ii) *Any linear polynomial $cx + d \in R[x]$, which is not a multiple of u, is invertible in $\mathcal{R}_{\alpha,\beta}$.*

Proof. (i) Let $cx + d \in \mathbb{F}_{p^m}[x]$, where $c \neq 0$. In $\mathcal{R}_{\alpha,\beta}$, we have

$$(x+d)^{p^s}(x-d)^{p^s}(x^2+d^2)^{p^s} = (x^4-d^4)^{p^s} = x^{4p^s} - d^{4p^s} = (\alpha - d^{4p^s}) + u\beta.$$

Since α is not a square in $\mathbb{F}_{p^m}$, $\alpha - d^{4p^s}$ is invertible in $\mathbb{F}_{p^m}$, whence, $(\alpha - d^{4p^s}) + u\beta$ is invertible in R. Thus,

$$(x+d)^{-1} = (x+d)^{p^s-1}(x-d)^{p^s}(x^2+d^2)^{p^s}(\alpha - d^{4p^s} + u\beta)^{-1}.$$

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

$$\begin{aligned}(cx+d)^{-1} &= c^{-1}(x+c^{-1}d)^{-1} \\ &= c^{-1}(x+c^{-1}d)^{p^s-1}(x-c^{-1}d)^{p^s}(x^2+c^{-2}d^2)^{p^s} \\ &\quad \times (\alpha - c^{-4p^s}d^{4p^s} + u\beta)^{-1}.\end{aligned}$$

(ii) Let $f(x) = (c_1 + uc_2)x + d_1 + ud_2 \in R[x]$, where $c_1, c_2, d_1, d_2 \in \mathbb{F}_{p^m}$, be a linear polynomial which is not a multiple of u, i.e. c_1 and d_1 cannot be both 0. We have $f(x) = (c_1x + d_1) + u(c_2x + d_2)$. Hence,

$$f(x)((c_1x+d_1) - u(c_2x+d_2)) = (c_1x+d_1)^2,$$

which is invertible because, by part (i), $c_1x + d_1$ is invertible. That means $f(x)$ is invertible. □

Lemma 3.3. *Let $z \in \mathbb{F}_{p^m}$ be a non-square. Then*:

(i) *$-z$ is a fourth power in $\mathbb{F}_{p^m}$.*
(ii) *There is an element $z' \in \mathbb{F}_{p^m}$ such that $z = -4z'^4$.*

Proof. (i) Since $p^m \equiv 3 \pmod 4$, -1 is an odd power of ξ. As z is a non-square, z is also an odd power of ξ. Thus $-z$ is an even power of ξ, say $-z = \xi^{2k}$. If k is even, then $-z$ is a fourth power. If k is odd, then $-\xi^k$ is an even power of ξ, and hence $-z = (-\xi^k)^2$ is a fourth power.

(ii) Note that $p^m \equiv 3 \pmod 4$ means $p \equiv 3 \pmod 4$ (and m must necessarily be odd), and hence either 2 or -2 is a square in $\mathbb{F}_{p^m}$. Thus, 4 is a fourth power in $\mathbb{F}_{p^m}$. By part (i), we get $-z/4$ is a fourth power, i.e. there is an element $z' \in \mathbb{F}_{p^m}$ such that $-z/4 = z'^4$. Therefore, $z = -4z'^4$. □

Proposition 3.4. *Let $\eta \in \mathbb{F}_{p^m}$ be such that $\alpha_0 = -4\eta^4$ (such η exists by Lemma 3.3). Then $x^4 - \alpha_0$ has the following factorization into product of monic*

coprime irreducible factors:

$$x^4 - \alpha_0 = (x^2 + 2\eta x + 2\eta^2)(x^2 - 2\eta x + 2\eta^2).$$

Moreover, in $\mathcal{R}_{\alpha,\beta}$,

$$\langle (x^2 + 2\eta x + 2\eta^2)^{2p^s} \rangle = \langle (x^2 + 2\eta x + 2\eta^2)^{2p^s+k} \rangle,$$
$$\langle (x^2 - 2\eta x + 2\eta^2)^{2p^s} \rangle = \langle (x^2 - 2\eta x + 2\eta^2)^{2p^s+k} \rangle,$$

for any non-negative integer k.

Proof. We have

$$\begin{aligned} x^4 - \alpha_0 &= x^4 + 4\eta^4 \\ &= (x^4 + 4\eta^2 x^2 + 4\eta^4) - 4\eta^2 x^2 \\ &= (x^2 + 2\eta^2)^2 - (2\eta x)^2 \\ &= (x^2 + 2\eta x + 2\eta^2)(x^2 - 2\eta x + 2\eta^2). \end{aligned}$$

Since $(x^2 + 2\eta x + 2\eta^2) - (x^2 - 2\eta x + 2\eta^2) = 4\eta x$, which is invertible, $x^2 + 2\eta x + 2\eta^2$ and $x^2 - 2\eta x + 2\eta^2$ are coprime. As $x^4 - \alpha_0$ is nilpotent, they are both not invertible. Thus, by Proposition 3.2, any nonzero linear factor of $R[x]$, which is not a multiple of u, is invertible, so both $x^2 + 2\eta x + 2\eta^2$ and $x^2 - 2\eta x + 2\eta^2$ are irreducible. For the last assertion, note that, since $x^2 + 2\eta x + 2\eta^2$ and $x^2 - 2\eta x + 2\eta^2$ are coprime, $(x^2 + 2\eta x + 2\eta^2)^k$ and $(x^2 - 2\eta x + 2\eta^2)^{2p^s}$ are also coprime. Hence, there are polynomials $g, h \in \mathcal{R}_{\alpha,\beta}$ such that $(x^2 + 2\eta x + 2\eta^2)^k g + (x^2 - 2\eta x + 2\eta^2)^{2p^s} h = 1$ in $\mathcal{R}_{\alpha,\beta}$. Therefore, in $\mathcal{R}_{\alpha,\beta}$,

$$\begin{aligned} (x^2 + 2\eta x + 2\eta^2)^{2p^s+k} g &= (1 - (x^2 - 2\eta x + 2\eta^2)^{2p^s} h)(x^2 + 2\eta x + 2\eta^2)^{2p^s} \\ &= (x^2 + 2\eta x + 2\eta^2)^{2p^s} - (x^4 - \alpha_0)^{2p^s} h \\ &= (x^2 + 2\eta x + 2\eta^2)^{2p^s}, \end{aligned}$$

implying $\langle (x^2 + 2\eta x + 2\eta^2)^{2p^s} \rangle = \langle (x^2 + 2\eta x + 2\eta^2)^{2p^s+k} \rangle$. □

Theorem 3.5. *The ring* $\mathcal{R}_{\alpha,\beta}$ *is a principal ideal ring whose ideals are* $\langle (x^2 + 2\eta x + 2\eta^2)^i (x^2 - 2\eta x + 2\eta^2)^j \rangle$, *where* $0 \le i, j \le 2p^s$. *Equivalently, each* $(\alpha + u\beta)$*-constacyclic code of length* $4p^s$ *over* R *has the form*

$$C = \left\langle (x^2 + 2\eta x + 2\eta^2)^i (x^2 - 2\eta x + 2\eta^2)^j \right\rangle,$$

for $0 \le i, j \le 2p^s$. *Moreover,* C *contains* $p^{m(8p^s - 2i - 2j)}$ *codewords.*

Proof. Let C be a $(\alpha + u\beta)$-constacyclic code of length $4p^s$ over R, i.e. C is an ideal of the ring $\mathcal{R}_{\alpha,\beta}$. Let C_u be the set of elements of C reduced modulo u. Then C_u is an ideal of the ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{4p^s} - \alpha \rangle}$. As discussed above, $x^4 - \alpha_0$ factors into product

*On $(\alpha + u\beta)$-constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ **

of monic irreducible pairwise coprime polynomials in $\mathbb{F}_{p^m}[x]$ and $R[x]$ as

$$x^4 - \alpha_0 = (x^2 + 2\eta x + 2\eta^2)(x^2 - 2\eta x + 2\eta^2),$$

and $C_u = \langle (x^2 + 2\eta x + 2\eta^2)^{k_1}(x^2 - 2\eta x + 2\eta^2)^{k_2} \rangle$, where $0 \leq k_1, k_2 \leq p^s$. Thus, for any polynomial $c(x) \in C$, there exist polynomials $g(x), h(x) \in \mathcal{R}_{\alpha,\beta}$ such that

$$c(x) = g(x)(x^2 + 2\eta x + 2\eta^2)^{k_1}(x^2 - 2\eta x + 2\eta^2)^{k_2} + uh(x).$$

By Proposition 3.1, $u \in \langle (x^4 - \alpha_0)^{p^s} \rangle = \langle (x^2 + 2\eta x + 2\eta^2)^{p^s}(x^2 - 2\eta x + 2\eta^2)^{p^s} \rangle$, which implies

$$C \subseteq \left\langle (x^2 + 2\eta x + 2\eta^2)^{k_1}(x^2 - 2\eta x + 2\eta^2)^{k_2} \right\rangle.$$

Choose i, j to be the largest among those powers ℓ_1, ℓ_2 such that $C \subseteq \langle (x^2 + 2\eta x + 2\eta^2)^{\ell_1}(x^2 - 2\eta x + 2\eta^2)^{\ell_2} \rangle$. Then $0 \leq i, j \leq 2p^s$ and $C \subseteq \langle (x^2 + 2\eta x + 2\eta^2)^{i}(x^2 - 2\eta x + 2\eta^2)^{j} \rangle$. By the maximalities of i, j, there exists $d(x) \in C$ such that $d(x) = e(x)(x^2 + 2\eta x + 2\eta^2)^i(x^2 - 2\eta x + 2\eta^2)^j$, where $e(x) \in \mathcal{R}_{\alpha,\beta}$ such that $\gcd(e, x^2 + 2\eta x + 2\eta^2) = \gcd(e, x^2 - 2\eta x + 2\eta^2) = 1$. Thus,

$$\gcd(e, x^4 - \alpha_0) = \gcd(e, (x^2 + 2\eta x + 2\eta^2)(x^2 - 2\eta x + 2\eta^2)) = 1.$$

By Proposition 3.5, it follows that $e(x)$ is invertible in $\mathcal{R}_{\alpha,\beta}$. Hence,

$$(x^2 + 2\eta x + 2\eta^2)^i(x^2 - 2\eta x + 2\eta^2)^j = d(x)e(x)^{-1} \in C,$$

and hence, $C = \langle (x^2 + 2\eta x + 2\eta^2)^i(x^2 - 2\eta x + 2\eta^2)^j \rangle$. As discussed above, $0 \leq i, j \leq 2p^s$. In fact, if either i or j is greater than $2p^s$, say, $i = 2p^s + k$, then Proposition 3.4 gives

$$\begin{aligned}\langle (x^2 + 2\eta x + 2\eta^2)^i(x^2 - 2\eta x + 2\eta^2)^j \rangle &= \langle (x^2 + 2\eta x + 2\eta^2)^{2p^s + k}(x^2 - 2\eta x + 2\eta^2)^j \rangle \\ &= \langle (x^2 + 2\eta x + 2\eta^2)^{2p^s}(x^2 - 2\eta x + 2\eta^2)^j \rangle.\end{aligned}$$

□

We spend the rest of this section to provide some additional properties of the ambient ring $\mathcal{R}_{\alpha,\beta}$. Any element $f(x)$ of $\mathcal{R}_{\alpha,\beta}$ can be viewed as a polynomial of degree up to $4p^s - 1$ of $R[x]$, and so $f(x) = f_1(x) + uf_2(x)$, where $f_1(x), f_2(x)$ are polynomials of degrees up to $4p^s - 1$ of $\mathbb{F}_{p^m}[x]$. Thus, $f(x)$ can be uniquely expressed as

$$\begin{aligned}f(x) = &\sum_{i=0}^{p^s-1} (a_{0i}x^3 + b_{0i}x^2 + c_{0i}x + d_{0i})(x^4 - \alpha_0)^i \\ &+ u \sum_{i=0}^{p^s-1} (a_{1i}x^3 + b_{1i}x^2 + c_{1i}x + d_{1i})(x^4 - \alpha_0)^i\end{aligned}$$

$$= (a_{00}x^3 + b_{00}x^2 + c_{00}x + d_{00}) + (x^4 - \alpha_0)\sum_{i=1}^{p^s-1}(a_{0i}x^3 + b_{0i}x^2 + c_{0i}x + d_{0i})(x^4 - \alpha_0)^{i-1} + u\sum_{i=0}^{p^s-1}(a_{1i}x^3 + b_{1i}x^2 + c_{1i}x + d_{1i})(x^4 - \alpha_0)^i,$$

where $a_{0i}, a_{1i}, b_{0i}, b_{1i}, c_{0i}, c_{1i}, d_{0i}, d_{1i} \in \mathbb{F}_{p^m}$. By Proposition 3.1, $u \in \langle x^4 - \alpha_0\rangle$, and so $f(x)$ can be expressed as $f(x) = (a_{00}x^3 + b_{00}x^2 + c_{00}x + d_{00}) + (x^4 - \alpha_0)g(x)$. Thus, $f(x)$ is nilpotent if and only if $a_{00} = b_{00} = c_{00} = d_{00} = 0$, i.e. $f(x) \in \langle x^4 - \alpha_0\rangle$. It means that $\langle x^4 - \alpha_0\rangle$ is the set of all nilpotent elements of $\mathcal{R}_{\alpha,\beta}$, which is the so-called nil radical of $\mathcal{R}_{\alpha,\beta}$. On the other hand, $f(x)$ is invertible if and only if $a_{00}x^3 + b_{00}x^2 + c_{00}x + d_{00}$ is invertible, which is equivalent to $a_{00}x^3 + b_{00}x^2 + c_{00}x + d_{00} \notin \langle x^2 + 2\eta x + 2\eta^2\rangle$ and $a_{00}x^3 + b_{00}x^2 + c_{00}x + d_{00} \notin \langle x^2 - 2\eta x + 2\eta^2\rangle$, i.e. $a_{00}x^3 + b_{00}x^2 + c_{00}x + d_{00} \notin \langle x^2 + 2\eta x + 2\eta^2\rangle \cup \langle x^2 - 2\eta x + 2\eta^2\rangle$. That means $\langle x^2 + 2\eta x + 2\eta^2\rangle \cup \langle x^2 - 2\eta x + 2\eta^2\rangle$ is the set of all non-invertible elements of $\mathcal{R}_{\alpha,\beta}$. Moreover, it is easy to see that $\langle x^2 + 2\eta x + 2\eta^2\rangle$ and $\langle x^2 - 2\eta x + 2\eta^2\rangle$ are maximal ideals of $\mathcal{R}_{\alpha,\beta}$. We summarize those in the following proposition for future use.

Proposition 3.6. *The following hold true for the ambient ring $\mathcal{R}_{\alpha,\beta}$:*

(i) *$\mathcal{R}_{\alpha,\beta}$ is a principal ideal ring with maximal ideals $\langle x^2 + 2\eta x + 2\eta^2\rangle$ and $\langle x^2 - 2\eta x + 2\eta^2\rangle$.*
(ii) *The ideal $\langle x^4 - \alpha_0\rangle$ is the nil radical of $\mathcal{R}_{\alpha,\beta}$.*
(iii) *The set $\langle x^2 + 2\eta x + 2\eta^2\rangle \cup \langle x^2 - 2\eta x + 2\eta^2\rangle$ is the set of all non-invertible elements of $\mathcal{R}_{\alpha,\beta}$.*

4. Duals of $(\alpha + u\beta)$-Constacyclic Codes

For an $(\alpha + u\beta)$-constacyclic code $C \subseteq \mathcal{R}_{\alpha,\beta}$ of length $4p^s$ over R, by Proposition 2.4, its dual $C^\perp$ is an $(\alpha+u\beta)^{-1}$ of length $4p^s$ over R. Since $(\alpha+u\beta)(\alpha-u\beta) = \alpha^2$, it follows that $(\alpha + u\beta)^{-1} = (\alpha - u\beta)\alpha^{-2} = \alpha^{-1} - u\alpha^{-2}\beta$. It means

$$C^\perp \subseteq \mathcal{R}_{\alpha^{-1},-\alpha^{-2}\beta} = \frac{R[x]}{\langle x^{4p^s} - (\alpha^{-1} - u\alpha^{-2}\beta)\rangle}.$$

Since $\alpha_0^{p^s} = \alpha$, $(\alpha_0^{-1})^{p^s} = \alpha^{-1}$, and α_0^{-1} is not a square. As in Lemma 3.3 and Proposition 3.4, there exists $\eta \in \mathbb{F}_{p^m}$ such that $\alpha_0 = -4\eta^4$, or equivalently, $\alpha_0^{-1} = -\frac{\eta^{-4}}{4}$. Hence, $x^4 - \alpha_0^{-1}$ factors into product of monic coprime irreducible divisors as follows:

$$x^4 - \alpha_0^{-1} = x^4 + \frac{\eta^{-4}}{4} = \left(x^4 + \eta^{-2}x^2 + \frac{\eta^{-4}}{4}\right) - \eta^{-2}x^2$$

$$= \left(x^2+\frac{\eta^{-2}}{2}\right)^2 - \left(\eta^{-1}x\right)^2$$
$$= \left(x^2+\eta^{-1}x+\frac{\eta^{-2}}{2}\right)\left(x^2-\eta^{-1}x+\frac{\eta^{-2}}{2}\right).$$

Hence, our arguments for $\mathcal{R}_{\alpha,\beta}$ in Sec. 3 work the same way for $\mathcal{R}_{\alpha^{-1},-\alpha^{-2}\beta}$, and we have the following results.

Theorem 4.1. *In $\mathcal{R}_{\alpha^{-1},-\alpha^{-2}\beta}$, $\langle (x^4-\alpha_0^{-1})^{p^s}\rangle = \langle u\rangle$. In particular, $x^4-\alpha_0^{-1}$ is nilpotent with nilpotency index $2p^s$. The ambient ring $\mathcal{R}_{\alpha^{-1},-\alpha^{-2}\beta}$ is a principal ideal ring, whose ideals are*

$$\left\langle \left(x^2+\eta^{-1}x+\frac{\eta^{-2}}{2}\right)^i \left(x^2-\eta^{-1}x+\frac{\eta^{-2}}{2}\right)^j \right\rangle,$$

where $0\le i,j\le 2p^s$. Equivalently, the $(\alpha^{-1}-u\alpha^{-2}\beta)$-constacyclic codes of length $4p^s$ over R are precisely the ideals

$$\left\langle \left(x^2+\eta^{-1}x+\frac{\eta^{-2}}{2}\right)^i \left(x^2-\eta^{-1}x+\frac{\eta^{-2}}{2}\right)^j \right\rangle,$$

where $0\le i,j\le 2p^s$. Each $(\alpha^{-1}-u\alpha^{-2}\beta)$-constacyclic code $\langle \left(x^2+\eta^{-1}x+\frac{\eta^{-2}}{2}\right)^i \left(x^2-\eta^{-1}x+\frac{\eta^{-2}}{2}\right)^j\rangle \subseteq \mathcal{R}_{\alpha^{-1},-\alpha^{-2}\beta}$ has $p^{m(8p^s-2i-2j)}$ codewords.

Note that

$$(x^2+2\eta x+2\eta^2)^* = 2\eta^2x^2+2\eta x+1 = 2\eta^2\left(x^2+\eta^{-1}x+\frac{\eta^{-2}}{2}\right),$$

and

$$\left(x^2-2\eta x+2\eta^2\right)^* = 2\eta^2x^2-2\eta x+1 = 2\eta^2\left(x^2-\eta^{-1}x+\frac{\eta^{-2}}{2}\right).$$

Therefore,

$$\begin{aligned}
&\langle (x^2+2\eta x+2\eta^2)^i(x^2-2\eta x+2\eta^2)^j\rangle^\perp \\
&= (\mathrm{ann}\langle (x^2+2\eta x+2\eta^2)^i(x^2-2\eta x+2\eta^2)^j\rangle)^* \\
&= (\langle (x^2+2\eta x+2\eta^2)^{2p^s-i}(x^2-2\eta x+2\eta^2)^{2p^s-j}\rangle)^* \\
&= \langle ((x^2+2\eta x+2\eta^2)^*)^{2p^s-i}((x^2-2\eta x+2\eta^2)^*)^{2p^s-j}\rangle \\
&= \left\langle \left(x^2+\eta^{-1}x+\frac{\eta^{-2}}{2}\right)^{2p^s-i} \left(x^2-\eta^{-1}x+\frac{\eta^{-2}}{2}\right)^{2p^s-j} \right\rangle.
\end{aligned}$$

Hence, we now have a description of the duals of $(\alpha+u\beta)$-constacyclic codes.

Theorem 4.2. *Let C be an $(\alpha+u\beta)$-constacyclic code of length $4p^s$ over R. Then*

$$C = \langle (x^2+2\eta x+2\eta^2)^i(x^2-2\eta x+2\eta^2)^j\rangle \subseteq \mathcal{R}_{\alpha,\beta},$$

for some $i, j \in \{0, 1, \ldots, 2p^s\}$, *and its dual* $C^\perp$ *is the* $(\alpha^{-1} - u\alpha^{-2}\beta)$*-constacyclic code*

$$C^\perp = \left\langle \left(x^2 + \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{2p^s - i} \left(x^2 - \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{2p^s - j} \right\rangle \subseteq \mathcal{R}_{\alpha^{-1}, -\alpha^{-2}\beta},$$

which contains $p^{m(2i+2j)}$ *codewords.*

It is readily to see that the ideal $\langle u \rangle \subseteq \mathcal{R}_{\alpha,\beta}$ is a self-dual $(\alpha + u\beta)$-constacyclic code of length $4p^s$ over R. We now show that it is the only self-dual code.

Theorem 4.3. *The ideal* $\langle u \rangle \subseteq \mathcal{R}_{\alpha,\beta}$ *is the unique self-dual* $(\alpha + u\beta)$*-constacyclic code of length* $4p^s$ *over* R.

Proof. We only need to show the uniqueness. Let C be an $(\alpha + u\beta)$-constacyclic code of length $4p^s$ over R. From Theorems 3.5 and 4.2,

$$C = \left\langle (x^2 + 2\eta x + 2\eta^2)^i (x^2 - 2\eta x + 2\eta^2)^j \right\rangle \subseteq \mathcal{R}_{\alpha,\beta},$$

for some $i, j \in \{0, 1, \ldots, 2p^s\}$, its dual $C^\perp$ is the $(\alpha^{-1} - u\alpha^{-2}\beta)$-constacyclic code

$$C^\perp = \left\langle \left(x^2 + \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{2p^s - i} \left(x^2 - \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{2p^s - j} \right\rangle \subseteq \mathcal{R}_{\alpha^{-1}, -\alpha^{-2}\beta},$$

and $|C| = p^{m(8p^s - 2i - 2j)}$, $|C^\perp| = p^{m(2i+2j)}$. Thus, in order for C to be self-dual, we must have $|C| = |C^\perp|$, i.e. $i + j = 2p^s$. At this point, we consider two cases, namely, $i = j$ and $i \neq j$.

Case 1: $i = j$. That means $i = j = p^s$. Then,

$$C = \langle (x^2 + 2\eta x + 2\eta^2)^{p^s} (x^2 - 2\eta x + 2\eta^2)^{p^s} \rangle = \langle (x^4 - \alpha_0)^{p^s} t \rangle = \langle u \rangle.$$

Case 2: $i \neq j$, say $i < j$. Since $i + j = 2p^s$, it follows that $0 \leq i < p^s < j \leq 2p^s$. Because $\langle u \rangle = \langle (x^2 + 2\eta x + 2\eta^2)^{p^s} (x^2 - 2\eta x + 2\eta^2)^{p^s} \rangle$, it implies that $C \not\subseteq \langle u \rangle$. Thus, C contains a codeword with an invertible entry. Without loss of generality, we can assume that there exists a codeword $(c_0, c_1, \ldots, c_{4p^s - 1}) \in C$ such that $c_{4p^s - 1}$ is invertible. As $C = C^\perp$, C is both $(\alpha + u\beta)$- and $(\alpha^{-1} - u\alpha^{-2}\beta)$-constacyclic, hence,

$$((\alpha + u\beta)c_{4p^s - 1}, c_0, \ldots, c_{4p^s - 2}) \in C,$$
$$((\alpha^{-1} - u\alpha^{-2}\beta)c_{4p^s - 1}, c_0, \ldots, c_{4p^s - 2}) \in C.$$

Thus,

$$\big(((\alpha - \alpha^{-1}) + u(\beta + \alpha^{-2}\beta))c_{4p^s - 1}, 0, \ldots, 0\big) \in C.$$

*On $(\alpha + u\beta)$-constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ **

Now, since α is not a square, $\alpha - \alpha^{-1} \neq 0$, implying $(\alpha - \alpha^{-1}) + u(\beta + \alpha^{-2}\beta)$ is invertible in R. Therefore,

$$(1, 0, \ldots, 0) = ((\alpha - \alpha^{-1}) + u(\beta + \alpha^{-2}\beta))^{-1} c_{4p^s-1}^{-1}$$
$$(((\alpha - \alpha^{-1}) + u(\beta + \alpha^{-2}\beta))c_{4p^s-1}, 0, \ldots, 0) \in C.$$

As $(1, 0, \ldots, 0)$ and all its cyclic shift give a basis for R^{4p^s}, it follows that $C = R^{4p^s}$, and so $C^\perp = \{\mathbf{0}\}$, a contradiction to the assumption that C is self-dual. □

Proposition 4.4. *Let C be an $(\alpha + u\beta)$-constacyclic code of length $4p^s$ over R. Then $C \cap C^\perp \subseteq u\mathbb{F}_{p^m}^{4p^s}$.*

Proof. Suppose to the contrary that $C \cap C^\perp \not\subseteq u\mathbb{F}_{p^m}^{4p^s}$, that means $C \cap C^\perp$ contains a codeword with an invertible entry. Thus, without loss of generality, we can assume that there is a codeword $c = (c_0, c_1, \ldots, c_{4p^s-1}) \in C \cap C^\perp$, where c_{4p^s-1} is invertible in R. Since C is $(\alpha + u\beta)$-constacyclic and $C^\perp$ is $(\alpha^{-1} - u\alpha^{-2}\beta)$-constacyclic, we get

$$((\alpha + u\beta)c_{4p^s-1}, c_0, \ldots, c_{4p^s-2}) \in C,$$
$$((\alpha^{-1} - u\alpha^{-2}\beta)c_{4p^s-1}, c_0, \ldots, c_{4p^s-2}) \in C^\perp.$$

Thus,

$$(\alpha + u\beta)c_{4p^s-1}c_0 + c_0c_1 + \cdots + c_{4p^s-2}c_{4p^s-1} = 0,$$
$$(\alpha^{-1} - u\alpha^{-2}\beta)c_{4p^s-1}c_0 + c_0c_1 + \cdots + c_{4p^s-2}c_{4p^s-1} = 0,$$

which implies

$$\big((\alpha - \alpha^{-1}) + u(\beta - \alpha^{-2}\beta)\big)c_{4p^s-1}c_0 = 0.$$

Since α is not a square, $\alpha \neq \alpha^{-1}$, hence, $(\alpha - \alpha^{-1}) + u(\beta - \alpha^{-2}\beta)$ is invertible in R. Therefore, $c_0 = 0$, i.e. the codeword $c = (0, c_1, \ldots, c_{4p^s-1})$. Continuing this process, we have

$$((\alpha + u\beta)c_{4p^s-2}, (\alpha + u\beta)c_{4p^s-1}, 0, c_1 \ldots, c_{4p^s-3}) \in C,$$
$$((\alpha^{-1} - u\alpha^{-2}\beta)c_{4p^s-2}, (\alpha^{-1} - u\alpha^{-2}\beta)c_{4p^s-1}, 0, c_1, \ldots, c_{4p^s-3}) \in C^\perp,$$
$$(\alpha + u\beta)c_{4p^s-1}c_1 + c_1c_3 + \cdots + c_{4p^s-3}c_{4p^s-1} = 0,$$
$$(\alpha^{-1} - u\alpha^{-2}\beta)c_{4p^s-1}c_1 + c_1c_3 + \cdots + c_{4p^s-3}c_{4p^s-1} = 0,$$

implying

$$((\alpha - \alpha^{-1}) + u(\beta - \alpha^{-2}\beta))c_{4p^s-1}c_1 = 0,$$

so $c_1 = 0$. Keep repeating this process, we have $c_0 = c_1 = \cdots = c_{4p^s-2} = c_{4p^s-1} = 0$, which is a contradiction. Therefore, $C \cap C^\perp \subseteq u\mathbb{F}_{p^m}^{4p^s}$. □

Recall that a code C is called *self-orthogonal* if $C \subseteq C^{\perp}$, and C is *dual-containing* if $C^{\perp} \subseteq C$. We conclude this section by identifying self-orthogonal and dual-containing $(\alpha + u\beta)$-constacyclic codes over R.

Corollary 4.5. *Let C be an $(\alpha+u\beta)$-constacyclic code of length $4p^s$ over R. That means*

$$C = \langle (x^2 + 2\eta x + 2\eta^2)^i (x^2 - 2\eta x + 2\eta^2)^j \rangle \subseteq \mathcal{R}_{\alpha,\beta},$$

for some $i, j \in \{0, 1, \ldots, 2p^s\}$, and its dual $C^{\perp}$ is the $(\alpha^{-1} - u\alpha^{-2}\beta)$-constacyclic code

$$C^{\perp} = \left\langle \left(x^2 + \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{2p^s - i} \left(x^2 - \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{2p^s - j} \right\rangle \subseteq \mathcal{R}_{\alpha^{-1}, -\alpha^{-2}\beta}.$$

Then C is self-orthogonal if $p^s \leq i, j \leq 2p^s$, and C is dual-containing if $0 \leq i, j \leq p^s$.

Proof. If $p^s \leq i, j \leq 2p^s$, then

$$\begin{aligned}
C &= \langle (x^2 + 2\eta x + 2\eta^2)^i (x^2 - 2\eta x + 2\eta^2)^j \rangle_{\mathcal{R}_{\alpha,\beta}} \\
&\subseteq \langle (x^2 + 2\eta x + 2\eta^2)^{p^s} (x^2 - 2\eta x + 2\eta^2)^{p^s} \rangle_{\mathcal{R}_{\alpha,\beta}} \\
&= \langle (x^4 - \alpha_0)^{p^s} \rangle_{\mathcal{R}_{\alpha,\beta}} \\
&= \langle u \rangle_{\mathcal{R}_{\alpha,\beta}} \\
&= u\mathbb{F}_{p^m}^{4p^s} \\
&= \langle u \rangle_{\mathcal{R}_{\alpha^{-1}, -\alpha^{-2}\beta}} \\
&= \langle (x^4 - \alpha_0^{-1})^{p^s} \rangle_{\mathcal{R}_{\alpha^{-1}, -\alpha^{-2}\beta}} \\
&= \left\langle \left(x^2 + \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{p^s} \left(x^2 - \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{p^s} \right\rangle_{\mathcal{R}_{\alpha^{-1}, -\alpha^{-2}\beta}} \\
&\subseteq \left\langle \left(x^2 + \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{2p^s - i} \left(x^2 - \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{2p^s - j} \right\rangle_{\mathcal{R}_{\alpha^{-1}, -\alpha^{-2}\beta}} \\
&= C^{\perp}.
\end{aligned}$$

Similarly, if $0 \leq i, j \leq p^s$, then

$$\begin{aligned}
C &= \langle (x^2 + 2\eta x + 2\eta^2)^i (x^2 - 2\eta x + 2\eta^2)^j \rangle_{\mathcal{R}_{\alpha,\beta}} \\
&\supseteq \langle (x^2 + 2\eta x + 2\eta^2)^{p^s} (x^2 - 2\eta x + 2\eta^2)^{p^s} \rangle_{\mathcal{R}_{\alpha,\beta}} \\
&= \langle (x^4 - \alpha_0)^{p^s} \rangle_{\mathcal{R}_{\alpha,\beta}}
\end{aligned}$$

*On $(\alpha + u\beta)$-constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ **

$$
\begin{aligned}
&= \langle u \rangle_{\mathcal{R}_{\alpha,\beta}} \\
&= u\mathbb{F}_{p^m}^{4p^s} \\
&= \langle u \rangle_{\mathcal{R}_{\alpha^{-1},-\alpha^{-2}\beta}} \\
&= \left\langle (x^4 - \alpha_0^{-1})^{p^s} \right\rangle_{\mathcal{R}_{\alpha^{-1},-\alpha^{-2}\beta}} \\
&= \left\langle \left(x^2 + \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{p^s} \left(x^2 - \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{p^s} \right\rangle_{\mathcal{R}_{\alpha^{-1},-\alpha^{-2}\beta}} \\
&\supseteq \left\langle \left(x^2 + \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{2p^s-i} \left(x^2 - \eta^{-1}x + \frac{\eta^{-2}}{2}\right)^{2p^s-j} \right\rangle_{\mathcal{R}_{\alpha^{-1},-\alpha^{-2}\beta}} \\
&= C^{\perp}. \qquad \square
\end{aligned}
$$

Acknowledgments

H. Q. Dinh and S. Sriboonchitta are grateful to the Central of Excellence in Econometrics of the Faculty of Economics, Chiang Mai University, for partial financial support. This paper was done during the visit of B. T. Nguyen and T. M. Vo to H. Q. Dinh at the Department of Mathematical Sciences, Kent State University, Ohio, USA, in November 2017 to January 2018. B. T. Nguyen and T. M. Vo are thankful for the hospitality and support of the Department of Mathematical Sciences, Kent State University. This work was also partially supported by a grant from the Simons Foundation. B. T. Nguyen is grateful to the Foundation for Science and Technology Development, Nguyen Tat Thanh University, for partial financial support.

References

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

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

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

[5] 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.

[6] 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.

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

[8] H. Q. Dinh, On repeated-root constacyclic codes of length $4p^s$, *Asian European J. Math.* **6** (2013) 1–25.
[9] H. Q. Dinh, S. Dhompongsa and S. Sriboonchitta, On constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *Discrete Math.* **340** (2017) 832–849.
[10] H. Q. Dinh and S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inform. Theory* **50** (2004) 1728–1744.
[11] H. Q. Dinh, B. T. Nguyen, S. Sriboonchitta and T. M. Vo, On a class of constacyclic codes length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, *J. Algebra Appl.* (2018), accepted for publication.
[12] 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.
[13] W. C. Huffman, On the decomposition of self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ with an automorphism of odd prime order, *Finite Fields Appl.* **13** (2007) 681–712.
[14] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes* (Cambridge University Press, Cambridge, 2003).
[15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 10th impression (North-Holland, Amsterdam, 1998).
[16] V. Pless and W. C. Huffman, *Handbook of Coding Theory* (Elsevier, Amsterdam, 1998).
[17] I. Siap, Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and their complete weight enumerators, in *Codes and Designs*, *Ohio State University Mathematical Research Institute Publications*, Vol. 10 (de Gruyter, Berlin, 2002), pp. 259–271.
[18] P. Udaya and A. Bonnecaze, Decoding of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inform. Theory* **45** (1999) 2148–2157.