Journal of Combinatorial Mathematics and Combinatorial Computing, 122: 351–359
DOI:10.61091/jcmcc122-29
http://www.combinatorialpress.com/jcmcc
Received 3 August 2024, Accepted 22 September 2024, Published 30 September 2024

Combinatorial Press

Article

On Negacyclic Codes of Length $8p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

Youssef AHENDOUZ[1,*], **and Ismail AKHARRAZ**[1]

[1] Mathematical and Informatics Engineering Laboratory Ibn Zohr University - Morocco

* **Correspondence:** youssef.ahendouz@edu.uiz.ac.ma

Abstract: In this paper, we provide a correction regarding the structure of negacyclic codes of length $8p^s$ over $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ when $p^m \equiv 3 \pmod 8$ as classified in [1]. Among other results, we determine the number of codewords and the dual of each negacyclic code.

Keywords: Negacyclic codes, Codes over Rings, Dual codes

1. Introduction

Constacyclic codes are a crucial part of error-correcting code theory because they extend cyclic codes. They are valuable in practice because they can be encoded efficiently using simple shift registers and have rich algebraic structures that improve error detection and correction. Many well-known codes, such as BCH, Kerdock, Golay, Reed-Muller, Preparata, and binary Hamming codes, either belong to or are derived from the cyclic code family. This is why constacyclic codes play a significant role in engineering.

Let's consider R to be a commutative finite ring. A code of length n over R is a nonempty subset C of $R^n = \{(r_0, r_1, \ldots, r_{n-1}) \mid r_i \in R,\ i = 0, 1, \ldots, n-1\}$, and its elements are called codewords. The code C is called linear if C forms an R-submodule of R^n. We define the standard Euclidean inner product on the space R^n as $[r, t] = \sum_{i=0}^{n-1} r_i t_i$, where $r = (r_0, r_1, \ldots, r_{n-1})$ and $t = (t_0, t_1, \ldots, t_{n-1})$ belong to R^n. The dual code is given by $C^\perp = \{r \in R^n \mid [r, t] = 0, \forall t \in C\}$.

For $\delta \in R^\times$, a linear code C of length n over R is termed a δ-constacyclic code if $(\delta r_{n-1}, r_0, r_1, \ldots, r_{n-2}) \in C$ for all $(r_0, r_1, \ldots, r_{n-1}) \in C$. Specifically, C is called a negacyclic code if $\delta = -1$, and a cyclic code if $\delta = 1$. For any $r = (r_0, r_1, \ldots, r_{n-1}) \in R^n$, let $r(x) = r_0 + r_1 x + \cdots + r_{n-1}x^{n-1} \in \frac{R[x]}{\langle x^n - \delta \rangle}$. We will identify r with $r(x)$ in this paper. It is well known that C is a δ-constacyclic code of length n over R if and only if C is an ideal of the residue class ring $\frac{R[x]}{\langle x^n - \delta \rangle}$.

Consider the finite commutative ring $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where $u^2 = 0$. The elements of $\mathcal{R}$ are linear combinations of 1 and u with coefficients in $\mathbb{F}_{p^m}$, namely of the form $\alpha + u\beta$ where $\alpha, \beta \in \mathbb{F}_{p^m}$. Furthermore, such an element is a unit if and only if $\alpha \neq 0$. This ring is commonly used for constacyclic codes. A notable example is $\mathbb{F}_2 + u\mathbb{F}_2$, positioned between $\mathbb{F}_4$ and $\mathbb{Z}_4$. It exhibits an additive resemblance with $\mathbb{F}_4$ and a multiplicative resemblance with $\mathbb{Z}_4$. Many studies focus on constacyclic codes over the ring $\mathcal{R}$.

In general, The classification of codes over $\mathcal{R}$ plays an important role in studying their structures, but in general, it is very difficult. In 2010, Dinh [2] classified constacyclic codes of

length p^s over $\mathcal{R}$. Subsequent works have extended this classification to include lengths such as $2p^s$, $3p^s$, $4p^s$, $5p^s$, and $8p^s$ [1,3–6].

In this paper, we correct the results from [1] regarding the algebraic structure of negacyclic codes of length p^s over $\mathcal{R}$, specifically when $p^m \equiv 3 \pmod 8$. Additionally, we compute the number of codewords for these codes and provide the duals for each negacyclic code under this condition.

2. Main Results

We recall that a chain commutative ring R is a ring in which all its ideals can be ordered by inclusion. Various characterizations of finite chain rings include the following.

Proposition 1. [7, Proposition 2.1] *If R is a finite commutative ring, the following conditions are equivalent:*

1. *R is a local ring with a maximal ideal $\langle r\rangle$ for some $r \in R$,*
2. *R is a local principal ideal ring,*
3. *R is a chain ring.*

In the case where R is a finite chain ring with a maximal ideal $\langle r\rangle$ and e is the nilpotency index of r, the ideals of R are of the form $\langle r^i\rangle$ where $i = 0, \ldots, e$. Moreover,

$$\forall i = 0, \ldots, e, \left|\langle r^i\rangle\right| = \left|\frac{R}{\langle r\rangle}\right|^{e-i}. \tag{1}$$

In the rest of this paper, we define $\mathcal{R} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and $\mathscr{R} = \frac{\mathcal{R}[x]}{\langle x^{8p^s}+1\rangle}$ where $u^2 = 0$. Here, p is an odd prime number such that $p^m \equiv 3 \pmod 8$. Additionally, both m and s are positive integers.

It is known that negacyclic codes of length $8p^s$ over $\mathcal{R}$ are ideals of the ring $\mathscr{R}$. As mentioned in [1], there exists $\beta \in \mathbb{F}_{p^m}^*$ such that $\beta^2 = -2$. Moreover, the following factorization into monic irreducible polynomials holds in $\mathcal{R}[x]$:

$$x^8 + 1 = \left(x^4 - \beta x^2 - 1\right)\left(x^4 + \beta x^2 - 1\right). \tag{2}$$

Theorem 1. [1, Theorem 3.3.4.] *The ring $\mathscr{R}$ is a principal ideal ring whose ideals can be expressed as*

$$\left\langle \left(x^4 - \beta x^2 - 1\right)^i \left(x^4 + \beta x^2 - 1\right)^j \right\rangle,$$

where $0 \le i, j \le p^s$.

According to this theorem, the ring $\mathscr{R}$ has two maximal ideals: $\langle x^4 - \beta x^2 - 1\rangle$ and $\langle x^4 + \beta x^2 - 1\rangle$. In addition, since the element $u \in \mathscr{R}$ is nilpotent, it is not invertible and must belong to a maximal ideal. Without loss of generality, we can assume that $u \in \langle x^4 - \beta x^2 - 1\rangle$. This assumption implies the existence of polynomials $a_0(x)$, $a_1(x)$, $b_0(x)$, and $b_1(x) \in \mathbb{F}_{p^m}[x]$ such that

$$u = (a_0(x) + ua_1(x))\left(x^4 - \beta x^2 - 1\right) + (b_0(x) + ub_1(x))\left(x^8 + 1\right)^{p^s}.$$

By isolating the terms involving u, we get

$$1 = a_1(x)\left(x^4 - \beta x^2 - 1\right) + b_1(x)\left(x^8 + 1\right)^{p^s}.$$

Hence, $(x^4 - \beta x^2 - 1)$ must divide 1 in $\mathbb{F}_{p^m}[x]$, yielding a contradiction.. Therefore, [1, Theorem 3.3.4.] is incorrect. We will correct it in the rest of this section.

Since $(x^4 - \beta x^2 - 1)^{p^s}$ and $(x^4 + \beta x^2 - 1)^{p^s}$ are coprime, By the Chinese reminder theorem:

$$\mathscr{R} = \bigoplus_{\ell \in \{\pm 1\}} \mathcal{S}_\ell,$$

where $\mathcal{S}_\ell = \frac{\mathcal{R}[x]}{\left\langle (x^4 + \ell\beta x^2 - 1)^{p^s} \right\rangle}$. Consequently, every negacyclic code C of length $8p^s$ over $\mathcal{R}$ can be expressed as $C \cong \bigoplus_{\ell \in \{\pm 1\}} C_\ell$, where C_ℓ is an ideal of $\mathcal{S}_\ell$. Thus, the negacyclic codes of length $8p^s$ over $\mathcal{R}$ are entirely determined by the ideals $\mathcal{S}_\ell$.

2.1. The Ring $\mathcal{S}_\ell$ and its Ideals

Let $b(x) \in \mathcal{S}_\ell$. It can be represented as a polynomial of degree less than $4p^s$ over $\mathcal{R}$. Thus, $b(x)$ can be uniquely expressed as

$$\begin{aligned} b(x) &= \sum_{k=0}^{p^s-1} b_{0k}(x) \left(x^4 + \ell\beta x^2 + 1\right)^k + u \sum_{k=0}^{p^s-1} b_{1k} \left(x^4 + \ell\beta x^2 + 1\right)^k \\ &= b_{00}(x) + \left(x^4 + \ell\beta x^2 + 1\right) \sum_{k=1}^{p^s-1} b_{0k} \left(x^4 + \ell\beta x^2 + 1\right)^{k-1} + u \sum_{k=0}^{p^s-1} b_{1k} \left(x^4 + \ell\beta x^2 + 1\right)^k \\ &= b_{00}(x) + c(x), \end{aligned}$$

where, for any $0 \le k \le p^s - 1$, $b_{0k}(x)$ and $b_{1k}(x)$ are polynomials in $\mathbb{F}_{p^m}[x]$ with a degree less than 4. The polynomial $c(x)$ is defined as:

$$c(x) = \left(x^4 + \ell\beta x^2 + 1\right) \sum_{k=1}^{p^s-1} b_{0k} \left(x^4 + \ell\beta x^2 + 1\right)^{k-1} + u \sum_{k=0}^{p^s-1} b_{1k} \left(x^4 + \ell\beta x^2 + 1\right)^k.$$

Given that the degree of $b_{00}(x)$ is less than the degree of $(x^4 + \ell\beta x^2 + 1)$ and $(x^4 + \ell\beta x^2 + 1)$ is irreducible, it follows that either $b_{00}(x) = 0$ or $b_{00}(x)$ is coprime with $(x^4 + \ell\beta x^2 + 1)$. This implies that either $b_{00}(x)$ is zero, or $b_{00}(x)$ is a unit in the ring $\mathcal{S}_\ell$.

Additionally, it is evident that $c(x)$ is nilpotent. Therefore, $b(x)$ is non-invertible if and only if $b_{00}(x) = 0$. This means that all non-invertible elements of $\mathcal{S}_\ell$ form the ideal $\langle x^4 + \ell\beta x^2 + 1, u\rangle$.

As a result, $\mathcal{S}_\ell$ is a local ring with the maximal ideal $\langle x^4 + \ell\beta x^2 + 1, u\rangle$. It is clear that u is not in $\langle x^4 + \ell\beta x^2 + 1\rangle$, and $x^4 + \ell\beta x^2 + 1$ is also not in $\langle u\rangle$. Therefore, $\langle x^4 + \ell\beta x^2 + 1, u\rangle$ is not a principal ideal of $\mathcal{S}_\ell$. According to Proposition 1, $\mathcal{S}_\ell$ is not a chain ring. We thus have the following Theorem.

Theorem 2. *The ring $\mathcal{S}_\ell$ is a local ring with the maximal ideal $\langle x^4 + \ell\beta x^2 + 1, u\rangle$, but it is not a chain ring.*

In the following, we provide the ideals of the ring $\mathcal{S}_\ell$.

Theorem 3. *The ideals in $\mathcal{S}_\ell$ are classified as follows:*

- *Type 1:*
$$\{\langle 0\rangle, \langle 1\rangle\}.$$
- *Type 2:*
$$\left\langle u \left(x^4 + \ell\beta x^2 + 1\right)^j \right\rangle,$$
where $0 \le j \le p^s - 1$.

- *Type 3:*

$$\left\langle \left(x^4+\ell\beta x^2+1\right)^i + u\left(x^4+\ell\beta x^2+1\right)^t b(x) \right\rangle,$$

where $1 \le i \le p^s-1$, $0 \le t < i$, *and* $b(x)$ *is either* 0 *or a unit that can be represented as*

$$b(x) = \sum_k b_k(x)\left(x^4+\ell\beta x^2+1\right)^k,$$

with $b_k(x) \in \mathbb{F}_{p^m}[x]$, $\deg b_k(x) < 4$, *and* $b_0(x) \neq 0$.

- *Type 4:*

$$\left\langle \left(x^4+\ell\beta x^2+1\right)^i + u\left(x^4+\ell\beta x^2+1\right)^t b(x), u\left(x^4+\ell\beta x^2+1\right)^j \right\rangle,$$

where $1 \le i \le p^s-1$, *and* $j < T$, $b(x)$ *as in Type 3, and* T *is the smallest integer such that*

$$u\left(x^4+\ell\beta x^2+1\right)^T \in \left\langle \left(x^4+\ell\beta x^2+1\right)^i + u\left(x^4+\ell\beta x^2+1\right)^t b(x) \right\rangle.$$

Proof. Let $\mathcal{T}_\ell = \frac{\mathbb{F}_{p^m}[x]}{\left\langle (x^4+\ell\beta x^2-1)^{p^s}\right\rangle}$ and consider the ring homomorphism $\mu : \mathcal{S}_\ell \to \mathcal{T}_\ell$ defined by $\mu(a(x)+ub(x)) = a(x)$ for any $a(x)+ub(x) \in \mathcal{S}_\ell$, where $a(x), b(x) \in \mathbb{F}_{p^m}[x]$.

Since $x^4+\ell\beta x^2-1$ is irreducible, the ring $\mathcal{T}_\ell$ is a chain ring with ideals of the form $\langle (x^4+\ell\beta x^2-1)^i\rangle$ for $0 \le i \le p^s$. Now, let C be an ideal of $\mathcal{S}_\ell$. As μ is surjective, $\mu(C)$ is an ideal of $\mathcal{T}_\ell$, and thus $\mu(C) = \langle (x^4+\ell\beta x^2-1)^i\rangle$ for some $0 \le i \le p^s$. In particular, there exists an element $b(x)$ such that $(x^4+\ell\beta x^2-1)^i + ub(x) \in C$.

If $c(x) \in C$, then there exists an $f(x) \in \mathcal{T}_\ell$ such that

$$\mu(c(x)) = f(x)(x^4+\ell\beta x^2-1)^i = \mu(g(x))\mu\left((x^4+\ell\beta x^2-1)^i + ub(x)\right),$$

where $g(x) \in \mathcal{S}_\ell$ and $\mu(g(x)) = f(x)$. This implies that

$$c(x) - g(x)\left((x^4+\ell\beta x^2-1)^i + ub(x)\right) \in \ker(\mu) \cap C = \langle u\rangle \cap C.$$

Hence,

$$C = \left\langle (x^4+\ell\beta x^2-1)^i + ub(x) \right\rangle + \langle u\rangle \cap C. \tag{3}$$

Let C' be an ideal such that $\langle u\rangle \cap C = uC'$. Applying the same procedure to C', we get

$$C' = \left\langle (x^4+\ell\beta x^2-1)^j + ue(x) \right\rangle + \langle u\rangle \cap C',$$

for $0 \le j \le p^s$ and $e(x) \in \mathcal{S}_\ell$. Substituting this expression into (3), we find

$$C = \left\langle (x^4+\ell\beta x^2-1)^i + ub(x), u(x^4+\ell\beta x^2-1)^j \right\rangle.$$

- If $i = 0$, then $(x^4+\ell\beta x^2-1)^i + ub(x)$ is a unit, hence $C = \langle 1\rangle$.
- If $i = p^s$, then by choosing $b(x) = 0$, we have $C = \langle u(x^4+\ell\beta x^2-1)^j\rangle$. Furthermore, if $j = p^s$, then $C = \langle 0\rangle$. If $0 \le j \le p^s-1$, then $C = \langle u(x^4+\ell\beta x^2-1)^j\rangle$, which is of type 2.
- If $1 \le i \le p^s-1$, write $ub(x)$ in the form

$$ub(x) = u\left(x^4+\ell\beta x^2+1\right)^t \sum_{k=0}^{p^s-t-1} b_k(x)\left(x^4+\ell\beta x^2+1\right)^k,$$

where $b_k(x)$ are polynomials of degree less than 4, and $b_0(x) \neq 0$. Then

$$C = \left\langle (x^4+\ell\beta x^2-1)^i + u\left(x^4+\ell\beta x^2+1\right)^t \right.$$

$$\sum_{k=0}^{p^s-t-1} b_k(x)\left(x^4+\ell\beta x^2+1\right)^k, u(x^4+\ell\beta x^2-1)^j\Bigg\rangle.$$

If $j \geq T$, then C is of type 3:

$$C = \left\langle (x^4+\ell\beta x^2-1)^i + u\left(x^4+\ell\beta x^2+1\right)^t \sum_{k=0}^{p^s-t-1} b_k(x)\left(x^4+\ell\beta x^2+1\right)^k \right\rangle.$$

Otherwise, C is of type 4.

□

The parameter T is crucial in the classification of Type 4 as per Theorem 3. Next, we will determine the value of T.

Proposition 2. *Let T be the smallest integer such that*

$$u\left(x^4+\ell\beta x^2+1\right)^T \in \left\langle \left(x^4+\ell\beta x^2+1\right)^i + u\left(x^4+\ell\beta x^2+1\right)^t b(x) \right\rangle.$$

Then, T is given by

$$T = \begin{cases} i, & \text{if } b(x) = 0, \\ \min\{i, p^s - i + t\}, & \text{if } b(x) \neq 0. \end{cases}$$

Proof. There exist polynomials $f(x), g(x) \in \mathbb{F}_{p^m}[x]$ such that $u\left(x^4+\ell\beta x^2-1\right)^T$ can be expressed as

$$u\left(x^4+\ell\beta x^2-1\right)^T = (f(x)+ug(x))\left(\left(x^4+\ell\beta x^2-1\right)^i + u\left(x^4+\ell\beta x^2-1\right)^t b(x)\right).$$

Simplifying the right-hand side, we obtain

$$\begin{aligned} u\left(x^4+\ell\beta x^2-1\right)^T =& f(x)\left(x^4+\ell\beta x^2-1\right)^i \\ &+ u\left(f(x)\left(x^4+\ell\beta x^2-1\right)^t b(x) + g(x)\left(x^4+\ell\beta x^2-1\right)^i\right). \end{aligned}$$

Necessarily, $(x^4+\ell\beta x^2-1)^{p^s-i}$ divides $f(x)$, so we can write

$$\left(x^4+\ell\beta x^2-1\right)^T = f'(x)\left(x^4+\ell\beta x^2-1\right)^{p^s-i+t} b(x) + g(x)\left(x^4+\ell\beta x^2-1\right)^i,$$

for some polynomial $f'(x) \in \mathbb{F}_{p^m}[x]$. Therefore:

- If $b(x) = 0$, then $T = i$.
- If $b(x) \neq 0$, then $T = \min\{i, p^s - i + t\}$.

□

For a ideal C of $\mathcal{S}_\ell$. The torsion and residue ideals of C are defined over $\mathbb{F}_{p^m}$ as follows:

$$\begin{aligned} \mathrm{Tor}(C) &= \left\{\mathbf{a} \in \mathbb{F}_{p^m}^n \mid u\mathbf{a} \in C\right\}, \\ \mathrm{Res}(C) &= \left\{\mathbf{a} \in \mathbb{F}_{p^m}^n \mid \exists \mathbf{b} \text{ such that } \mathbf{a} + u\mathbf{b} \in C\right\}. \end{aligned}$$

The reduction modulo u from C to $\mathrm{Res}(C)$ is given by:

$$\phi : C \to \mathrm{Res}(C), \quad \phi(\mathbf{a} + u\mathbf{b}) = \mathbf{a}.$$

Clearly, ϕ is well-defined and surjective, with $\mathrm{Ker}(\phi) \cong \mathrm{Tor}(C)$, and $\phi(C) \cong \mathrm{Res}(C)$. Hence, the size of $\mathrm{Res}(C)$ is related to the size of C by:

$$|\mathrm{Res}(C)| = \frac{|C|}{|\mathrm{Tor}(C)|}.$$

i.e.,

$$|C| = |\mathrm{Res}(C)||\mathrm{Tor}(C)|.$$

Through the definition and the classification provided in Theorem 3, obtaining $\mathrm{Res}(C)$ and $\mathrm{Tor}(C)$ of any ideal C of $\mathcal{S}_\ell$ is straightforward.

Theorem 4. *The torsion and residue of ideals of $\mathcal{S}_\ell$ are given by:*

- *If $C = \langle 0 \rangle$, then $\mathrm{Res}(C) = \langle 0 \rangle$ and $\mathrm{Tor}(C) = \langle 0 \rangle$.*
- *If $C = \langle 1 \rangle$, then $\mathrm{Res}(C) = \langle 1 \rangle$ and $\mathrm{Tor}(C) = \langle 1 \rangle$.*
- *If $C_2 = \left\langle u\left(x^4 + \ell\beta x^2 + 1\right)^j \right\rangle$ is an ideal of type 2, then $\mathrm{Res}(C_2) = \langle 0 \rangle$ and $\mathrm{Tor}(C_2) = \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^j \right\rangle$.*
- *If $C_3 = \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^i + u\left(x^4 + \ell\beta x^2 + 1\right)^t b(x) \right\rangle$ is an ideal of type 3, then $\mathrm{Res}(C_3) = \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^i \right\rangle$ and $\mathrm{Tor}(C_3) = \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^T \right\rangle$.*
- *If $C_4 = \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^i + u\left(x^4 + \ell\beta x^2 + 1\right)^t b(x), u\left(x^4 + \ell\beta x^2 + 1\right)^j \right\rangle$ is an ideal of type 4, then $\mathrm{Res}(C_4) = \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^i \right\rangle$ and $\mathrm{Tor}(C_4) = \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^i \right\rangle$.*

As $\mathrm{Tor}(C)$ and $\mathrm{Res}(C)$ are ideals of the ring $\frac{\mathbb{F}_{p^m}[x]}{\left\langle (x^4+\ell\beta x^2+1)^{p^s} \right\rangle}$, and this ring is a chain ring, we can calculate the sizes of $\mathrm{Res}(C)$ and $\mathrm{Tor}(C)$ using (1). By multiplying the sizes of $\mathrm{Res}(C)$ and $\mathrm{Tor}(C)$ in each case, we can then determine the number of elements in each ideal C of the ring $\mathcal{S}_\ell$.

2.2. Dual of Negacyclic Code

The reciprocal polynomial of $a(x) = a_0 + a_1 x + \cdots + a_t x^t \in \mathcal{R}[x]$ with degree t, denoted by $a^*(x)$, is defined by

$$a^*(x) = a_t + a_{t-1}x + a_{t-2}x^2 + \cdots + a_0 x^t = x^t a\left(\frac{1}{x}\right).$$

The annihilator of an ideal C of $\mathscr{R}$ is defined by

$$\mathcal{A}(C) = \{a(x) \in \mathscr{R} \mid \forall b(x) \in C, a(x) \cdot b(x) = 0\}.$$

It is well known [7] that for any negacyclic code C of length $8p^s$ over $\mathcal{R}$, i.e., an ideal of $\mathscr{R}$,

$$C^\perp = \mathcal{A}(C)^* = \{a^*(x) \mid a(x) \in \mathcal{A}(C)\}.$$

Proposition 3. *Let $C \cong \bigoplus_{\ell \in \{\pm 1\}} C_\ell$ be a negacyclic code of length $8p^s$ over $\mathcal{R}$, where C_ℓ is an ideal of $\mathcal{S}_\ell$. Then*

$$C^\perp \cong \bigoplus_{\ell \in \{\pm 1\}} \mathcal{A}\left(C_{-\ell}\right)^*.$$

Proof. It is evident that $\mathcal{A}(C) \cong \bigoplus_{\ell \in \{\pm 1\}} \mathcal{A}(C_\ell)$. Let $\mathcal{A}(C)^* \cong \bigoplus_{\ell \in \{\pm 1\}} D_\ell$, where D_ℓ is an ideal of $\mathcal{S}_\ell$.

For $\ell \in \{\pm 1\}$ and $c_\ell(x) \in \mathcal{A}(C_\ell)$, there exists $f(x) \in \mathcal{A}(C)$ such that

$$c_\ell(x) = f(x) + h(x)\left(x^4 + \ell\beta x^2 + 1\right)$$

for some polynomial $h(x)$.

As $(x^4 + \ell\beta x^2 + 1)^* = (x^4 - \ell\beta x^2 + 1)$, it implies that $c_\ell^*(x) \in D_{-\ell}$, and thus $\mathcal{A}(C_\ell) \subseteq D_{-\ell}$. Given that $|\mathcal{A}(C)| = |\mathcal{A}(C)^*|$, we obtain the desired result. □

We will now determine the annihilator for each ideal of $\mathcal{S}_\ell$. For an ideal of Type 1, it is evident that $\mathcal{A}(\langle 0\rangle) = \langle 1\rangle$ and $\mathcal{A}(\langle 1\rangle) = \langle 0\rangle$. Now, let's proceed to consider the other types.

Theorem 5. *Let* $C = \left\langle u\left(x^4 + \ell\beta x^2 + 1\right)^i \right\rangle$ *be an ideal of* $\mathcal{S}_\ell$, *then* $\mathcal{A}(C) = \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - i}, u \right\rangle$.

Proof. Let $f(x) = f_0(x) + uf_1(x)$ where $f_0(x), f_1(x) \in \mathbb{F}_{p^m}[x]$. Then

$$\begin{aligned} f(x) \in \mathcal{A}(C) &\Leftrightarrow (f_0(x) + uf_1(x))\, u\left(x^4 + \ell\beta x^2 + 1\right)^i = 0 \\ &\Leftrightarrow f_0(x)\left(x^4 + \ell\beta x^2 + 1\right)^i = 0 \\ &\Leftrightarrow \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - 1} \text{ divides } f_0(x) \\ &\Leftrightarrow f(x) \in \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - i}, u \right\rangle. \end{aligned}$$

□

Theorem 6. *Let* $C = \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^i + u\left(x^4 + \ell\beta x^2 + 1\right)^t b(x) \right\rangle$ *be an ideal of* $\mathcal{S}_\ell$, *where* $b(x)$ *is* 0 *or* $b(x)$ *is a unit. Then* $\mathcal{A}(C)$ *is determined as follows.*

1. *If* $b(x) = 0$, *then* $\mathcal{A}(C) = \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - i} \right\rangle$.
2. *If* $b(x)$ *is a unit, then* $\mathcal{A}(C) = \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T} - u\left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T + t - i} b(x), u\left(x^4 + \ell\beta x^2 + 1\right)^{p^s - i} \right\rangle$.

Proof. The proof of (1) is straightforward and will be omitted. Instead, we will focus on proving (2). Let $f(x) = f_0(x) + uf_1(x)$ where $f_0(x), f_1(x) \in \mathbb{F}_{p^m}[x]$. Since $u\left(x^4 + \ell\beta x^2 + 1\right)^T \in C$, we have that $\left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T}$ divides $f_0(x)$, so we can write $f_0(x) = \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T} f_0'(x)$. Given that $T = \min\{i, p^s - i + t\}$, it follows that

$$\begin{aligned} & f(x) \in \mathcal{A}(C) \\ & \Leftrightarrow \left(\left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T} f_0'(x) + uf_1(x)\right)\left(\left(x^4 + \ell\beta x^2 + 1\right)^i + u\left(x^4 + \ell\beta x^2 + 1\right)^t b(x)\right) = 0 \\ & \Leftrightarrow \left(x^4 + \ell\beta x^2 + 1\right)^i f_1(x) + \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T} f_0'(x)\left(x^4 + \ell\beta x^2 + 1\right)^t b(x) = 0 \\ & \Leftrightarrow \left(x^4 + \ell\beta x^2 + 1\right)^i \left(f_1(x) + \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T + t - i} f_0'(x) b(x)\right) = 0 \\ & \Leftrightarrow \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - i} \text{ divides } \left(f_1(x) + \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T + t - i} f_0'(x) b(x)\right) \\ & \Leftrightarrow f_1(x) + \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T + t - i} f_0'(x) b(x) = \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - i} f_1'(x), \end{aligned}$$

then

$$\begin{aligned} f(x) &= \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T} f_0'(x) + u\left(\left(x^4 + \ell\beta x^2 + 1\right)^{p^s - i} f_1'(x)\right. \\ &\quad \left. - \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T + t - i} f_0'(x) b(x)\right) \\ &= f_0'(x)\left(\left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T} - u\left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T + t - i} b(x)\right) \\ &\quad + f_1'(x) u\left(x^4 + \ell\beta x^2 + 1\right)^{p^s - i}. \end{aligned}$$

Thus, $\mathcal{A}(C)$ is given by:

$$\mathcal{A}(C) = \left\langle \left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T} - u\left(x^4 + \ell\beta x^2 + 1\right)^{p^s - T + t - i} b(x), u\left(x^4 + \ell\beta x^2 + 1\right)^{p^s - i} \right\rangle.$$

□

Theorem 7. *Let* $C = \left\langle (x^4+\ell\beta x^2+1)^i + u\,(x^4+\ell\beta x^2+1)^t\, b(x), u\,(x^4+\ell\beta x^2+1)^j \right\rangle$, *where* $b(x)$ *is* 0 *or* $b(x)$ *is a unit. Then* $\mathcal{A}(C)$ *is determined as follows:*

1. *If* $b(x)=0$, *then* $\mathcal{A}(C) = \left\langle (x^4+\ell\beta x^2+1)^{p^s-j}, u\,(x^4+\ell\beta x^2+1)^{p^s-i} \right\rangle$.
2. *If* $b(x)$ *is a unit, then* $\mathcal{A}\,(C) = \left\langle (x^4+\ell\beta x^2+1)^{p^s-j} - u\,(x^4+\ell\beta x^2+1)^{p^s-j+t-i}\, b(x), u\,(x^4+\ell\beta x^2+1)^{p^s-i} \right\rangle$.

Proof. Let $f(x) = f_0(x) + uf_1(x)$ where $f_0(x), f_1(x) \in \mathbb{F}_{p^m}[x]$. Since $u\,(x^4+\ell\beta x^2+1)^j \in C$, we have that $(x^4+\ell\beta x^2+1)^{p^s-j}$ divides $f_0(x)$, so we can write $f_0(x) = (x^4+\ell\beta x^2+1)^{p^s-j} f_0'(x)$. Given that $t<j<T\le i$, it follows that

$$
\begin{aligned}
& f(x) \in \mathcal{A}\,(C) \\
& \Leftrightarrow \left((x^4+\ell\beta x^2+1)^{p^s-j} f_0'(x) + uf_1(x)\right)\left((x^4+\ell\beta x^2+1)^i + u\,(x^4+\ell\beta x^2+1)^t\, b(x)\right) = 0 \\
& \Leftrightarrow (x^4+\ell\beta x^2+1)^i f_1(x) + (x^4+\ell\beta x^2+1)^{p^s-j} f_0'(x)\,(x^4+\ell\beta x^2+1)^t\, b(x) = 0 \\
& \Leftrightarrow (x^4+\ell\beta x^2+1)^i \left(f_1(x) + (x^4+\ell\beta x^2+1)^{p^s-j+t-i} f_0'(x)b(x)\right) = 0 \\
& \Leftrightarrow (x^4+\ell\beta x^2+1)^{p^s-i} \text{ divides } \left(f_1(x) + (x^4+\ell\beta x^2+1)^{p^s-j+t-i} f_0'(x)b(x)\right) \\
& \Leftrightarrow f_1(x) + (x^4+\ell\beta x^2+1)^{p^s-j+t-i} f_0'(x)b(x) = (x^4+\ell\beta x^2+1)^{p^s-i} f_1'(x) \\
& \Leftrightarrow f(x) = (x^4+\ell\beta x^2+1)^{p^s-j} f_0'(x) + u\left((x^4+\ell\beta x^2+1)^{p^s-i} f_1'(x) - (x^4+\ell\beta x^2+1)^{p^s-j+t-i} f_0'(x)b(x)\right) \\
& \Leftrightarrow f(x) = f_0'(x)\left((x^4+\ell\beta x^2+1)^{p^s-j} - u\,(x^4+\ell\beta x^2+1)^{p^s-j+t-i}\, b(x)\right) + f_1'(x)u\,(x^4+\ell\beta x^2+1)^{p^s-i}.
\end{aligned}
$$

Thus $\mathcal{A}\,(C)$ is given by:

$$\mathcal{A}\,(C) = \left\langle \left(x^4+\ell\beta x^2+1\right)^{p^s-j} - u\left(x^4+\ell\beta x^2+1\right)^{p^s-j+t-i} b(x), u\left(x^4+\ell\beta x^2+1\right)^{p^s-i} \right\rangle.$$

□

Remark 1. *1. To obtain* $\mathcal{A}(C)^*$ *from* $\mathcal{A}(C)$, *it suffices to note that:* $\langle h(x), ug(x)\rangle^* = \langle h^*(x), ug^*(x)\rangle$ *and* $(g(x)h(x))^* = g^*(x)h^*(x)$. *Additionally, if* $\deg g \ge \deg h$, *then*

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

2. By using Proposition 3, the self-dual negacyclic codes of length $8p^s$ *over* $\mathcal{R}$ *are exactly those where* $C \cong I \bigoplus \mathcal{A}(I)^*$, *with* I *being an ideal of* $\mathcal{S}_{-1}$.

References

1. Dinh, H. Q., Nguyen, B. T. and Paravee, M., 2022. Constacyclic codes of length $8p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *Advances in Mathematics of Communications, 16*(3), pp.525–570.
2. Dinh, H. Q., 2010. Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *Journal of Algebra, 324*(5), pp.940-950.
3. Dinh, H. Q., 2012. Repeated-root constacyclic codes of length $2p^s$. *Finite Fields and Their Applications, 18*, pp.133-143.
4. Dinh, H. Q., Nguyen, B. T. and Yamaka, W., 2020. Constacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and their application in various distance distributions. *IEEE Access, 8*, pp.204031-204056.

5. Dinh, H. Q., Dhompongsa, S. and Sriboonchitta, S., 2017. On constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *Discrete Mathematics, 340*, pp.832-849.

6. Dinh, H. Q., Nguyen, B. T., Thi, H. L. and Yamaka, W., 2022. On Hamming distance distributions of repeated-root cyclic codes of length $5p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *IEEE Access, 10*, pp.-119904.

7. Dinh, H. Q. and López-Permouth, S. R., 2004. Cyclic and negacyclic codes over finite chain rings.*IEEE Transactions on Information Theory, 50*(8), pp.1728-1744.

8. Dinh, H. Q., 2009. Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Transactions on Information Theory, 55*(4), pp.1730-1740.