Math. Commun. **27**(2022), 127–135

The cyclic codes of length $5p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and their dual codes

Brahim Boudine*, Jamal Laaouine and Mohammed Elhassani Charkani

Department of Mathematics, Sidi Mohamed Ben Abdellah University, Faculty of Sciences Dhar El Mahraz, Fez, 30 003, Morocco

Received September 2, 2021; accepted March 28, 2022

Abstract. Let p be a prime integer and m an integer such that $p \equiv 2 \pmod 5$ or $p \equiv$ (mod 5), and let m be odd. We classify explicitly the cyclic codes of length $5p^s$ over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ with $u^2 = 0$ and compute completely their dual codes.

AMS subject classifications: 94B15 , 11T71, 11T22, 11T06

Key words: cyclic code, cyclotomic polynomial, error-correcting codes

1. Introduction

Linear codes have been widely studied due to their algebraic structure which simplifies study, and they even have many applications in storage and communication systems as they have efficient encoding and decoding algorithms [18]. For the sake of easy encoding and decoding, one naturally requires a cyclic shift of a codeword in a code $\mathcal{C}$ to be still a codeword of $\mathcal{C}$. This yields cyclic codes [13]. Namely, the codes $\mathcal{C}$ such that: $(c_0, \ldots, c_n)$ is a codeword in $\mathcal{C}$ implies that $(c_n, c_0, c_1, \ldots, c_{n-1})$ is a codeword in $\mathcal{C}$. Formally, cyclic codes of length p over a field k are defined as the ideals of the ring $k[X]/\langle X^p - 1\rangle$ [10].

In 1957, Prange [17] have been the first to study the cyclic codes. Since then, cyclic codes over $\mathbb{F}_{p^m}$ was completely classified (see [12, 11, 7, 8, 9, 5]). After that, cyclic codes have been generalized over finite rings instead of fields only. Classifications of cyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ for some lengths are known, e.g. for length p^s in 2010 by Dinh [6], for length $2p^s$ in 2014 by Liu and Xu [14], and for length $3p^s$ in 2020 by Phuto and Klin-eam [16].

Our aim in this paper is to classify the cyclic codes of length $5p^s$ over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ when $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$ and m is odd, and to give their dual codes. We propose a method of the ideals classification inspired by the number theory techniques based on the valuation language (see [15]). This new method allows to simplify proofs and calculations, and it strengthens the algebraic coding vocabulary. Moreover, our classification is characterized by an important parameter L which allows the avoidance of the repetition of some codes in different given types or classes.

Let p be a prime integer such that $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$ and m is odd. The decomposition of the cyclic codes of length $5p^s$ yields a class of codes that we

*Corresponding author. *Email addresses:* `brahimboudine.bb@gmail.com` (B. Boudine), `laaouine.jamal@gmail.com` (J. Laaouine), `mcharkani@gmail.com` (M. E. Charkani)

call the $n-$cyclotomic codes. So we define the $n-$cyclotomic codes and recall some results about their factorization in preliminaries. Then, in Section 3, we classify the cyclic codes of length $5p^s$ over R by giving a classification of 5-cyclotomic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Finally, the last section will be devoted to computing all the dual codes for each given type.

2. Preliminaries

Let $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ with $u^2 = 0$. Every element x of R is of the form $x = x_0 + ux_1$ with x_i in $\mathbb{F}_{p^m}$. We put $\nu(x) = \min\{i \in \{0,1\} \mid x_i \neq 0\}$. Likewise, if I is an ideal of R, then we put $\nu(I) = \max\{i \in \{0,1\} \mid I \subseteq u^i R\}$. In $R[X]$, a polynomial $f(X)$ is of the form $f(X) = f_0(X) + uf_1(X)$ with $f_i(X) \in \mathbb{F}_{p^m}[X]$. So we put $\nu(f) = \min\{i \in \{0,1\} \mid f_i \neq 0\}$, and for any ideal I in $R[X]$, $\nu(I) = \max\{i \in \{0,1\} \mid I \subseteq u^i R[X]\}$.
On the other hand, cyclotomic polynomials denoted by $\Phi_n(X)$ are defined as special divisors of polynomials of the form $X^n - 1$. When n is prime [1], we get

$$\Phi_n(X) = X^{n-1} + X^{n-2} + \cdots + X + 1.$$

Lemma 1. *[20] $\Phi_n(X)$ is irreducible in $\mathbb{F}_q[X]$ if and only if q is a primitive root modulo n and n is equal to 2, 4, r^k or $2r^k$, where r is an odd prime and k is a positive integer.*

Definition 1. *Let R be a commutative ring. We define a n-cyclotomic code of length $d_n k$ over R as an ideal of the ring $R[X]/\langle \Phi_n(X)^k \rangle$ where $d_n = \deg(\Phi_n)$.*

n-cyclotomic codes generalize cyclic and negacyclic codes; indeed, 1-cyclotomic codes of length p^s are exactly the negacyclic codes of length p^s, and 2-cyclotomic codes of length p^s are the cyclic codes of length p^s [1]:

$$\Phi_1(X) = 1 + X,$$
$$\Phi_2(X) = 1 - X.$$

Proposition 1. *$\Phi_5(X)$ is irreducible in $\mathbb{F}_{p^m}$ if and only if $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$ and m is odd.*

Proof. If $p \equiv 0 \pmod 5$ or $p \equiv 1 \pmod 5$ or $p \equiv 4 \pmod 5$, then clearly p^m is not a primitive root modulo 5.
If $p \equiv 2 \pmod 5$, then when $m = 2k$ we get $p^m \equiv 4 \pmod 3$ that is not a primitive root modulo 5, and when m is odd, we get $p^m \equiv 2 \pmod 5$ or $p^m \equiv 3 \pmod 5$, which are primitive root modulo 5. Likewise, we get that p^m is a primitive root modulo 5 when $p \equiv 3 \pmod 5$ and m is odd.
Therefore, $\Phi_5(X)$ is irreducible in $\mathbb{F}_{p^m}$ if and only if $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$ and m is odd. □

Proposition 2. *Let $\mathcal{C}$ be a cyclic code of length $5p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. If $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$ and m is odd, then*

$$\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2,$$

where $\mathcal{C}_1$ is a cyclic code of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ and $\mathcal{C}_2$ is a 5-cyclotomic code of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$.

Proof. Notice that $X^4+X^3+X^2+X+1=\Phi_5(X)$ is the 5-th cyclotomic polynomial [1]. Let $R=\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. When $p\equiv 2 \pmod 5$ or $p\equiv 3 \pmod 5$ and m is odd, $\Phi_5(X)$ is irreducible in $\mathbb{F}_{p^m}[X]$. We get $(X^5-1)^{p^s}=(X-1)^{p^s}(X^4+X^3+X^2+X+1)^{p^s}$. By the Chinese remainder theorem [2] $R[X]/\langle (X^5-1)^{p^s}\rangle = R[X]/\langle (X-1)^{p^s}\rangle \bigoplus R[X]/\langle (X^4+X^3+X^2+X+1)^{p^s}\rangle$. □

In order to classify the cyclic codes of length $5p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, it is enough to classify the 5-cyclotomic codes of length $4p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ and the cyclic codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$.
Likewise, $\mathcal{C}^\perp=\mathcal{C}_1^\perp\bigoplus\mathcal{C}_2^\perp$. Then we should only compute the dual codes of the 5-cyclotomic codes of length $4p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ and the cyclic codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$.

3. Classification of the cyclic codes of length $5p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$

Theorem 1. *Let $f(x)=x^4+x^3+x^2+x+1$, and $p\equiv 2 \pmod 5$ or $p\equiv 3 \pmod 5$ and m is odd. 5-cyclotomic codes of length $4p^s$ over $R=\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ are as follows:*

1. *Type 1: $\mathcal{C}_1$:* $\langle 0\rangle$; $\langle 1\rangle$.
2. *Type 2: $\mathcal{C}_2(\tau)$:* $\langle uf(x)^\tau\rangle$*; where* $0\le\tau\le p^s-1$.
3. *Type 3: $\mathcal{C}_3(\delta,t,h(x))$:* $\langle f(x)^\delta+uf(x)^t h(x)\rangle$;
   where $\delta>t$, either $h(x)$ is 0 or $h(x)$ is a unit in $R[X]/\langle f(X)^{p^s}\rangle$ of the form $\sum_{i=0}^{L-t-1} h_i f(x)^i$ *with* $\deg(h_i)\le 1$ *and* $h_0\ne 0$.
4. *Type 4: $\mathcal{C}_4(\delta,t,h(x),\omega)$:* $\langle f(x)^\delta+uf(x)^t h(x), uf(x)^\omega\rangle$;
   where $p^s>\delta\ge L>\omega>t\ge 0$, either $h(x)$ is 0 or $h(x)$ is a unit in $R[X]/\langle f(X)^{p^s}\rangle$. Here, L is the smallest integer satisfying $uf(x)^L\in\mathcal{C}_3(\delta,t,h(x))$.

Proof. The proof consists of 3 steps:

Step 1: First, we show the general form of ideals of $A=R[X]/\langle (f(X))^{p^s}\rangle$.
Let I be an ideal in A; then $\overline{I}=(I+uA)/uA$ is an ideal in A/uA. Since $A/uA\sim\mathbb{F}_{p^m}[X]/\langle\overline{f}(X))^{p^s}\rangle$ is a principal ideal ring, $\overline{I}=\overline{a_1}A/uA$ for some $a_1\in I$. Let $x\in I$; then $\overline{x}=\overline{a_1.b}$ for some $b\in A$. Namely, $x=a_1.b+uc$ for some $c\in A$. Thus $uc=x-a_1.b\in I$. Therefore $c\in J_1=\{r\in A\mid ur\in I\}$, so that $I=a_1.A+uJ_1$. By the same logic for J_1 we get $J_1=a_2.A+u.J_2$ for $J_2=\{r\in A\mid ur\in J_1\}=\{r\in A\mid u^2r\in I\}$. Therefore, $I=a_1.A+ua_2.A$.

Step 2: Next, we show the generators a_i.
We know that R is a special principal ideal ring [3]. Then, every principal ideal J in $R[X]$ is of the form $\langle u^\mu g\rangle$, where g is a monic polynomial and $\mu=\nu(J)$ (see [4]). There exist $g_0,g_1\in\mathbb{F}_{p^m}[X]/\langle f(X)^{p^s}\rangle$ such that $g=g_0+ug_1$. For $k\in\{0,1\}$. Let $v_k=\max\{i\in\{0,\dots,p^s\}\mid f^i$ divide $g_k\}$. Then $g_k=f^{v_k}q$ for some $q\in\mathbb{F}_{p^m}[X]/\langle f(X)^{p^s}\rangle$. Then q does not divide f which is irreducible, so the Bézout identity proves that q is a unit in $\mathbb{F}_{p^m}[X]/\langle f(X)^{p^s}\rangle$. Therefore, $g=f^a+uf^bh$. If we suppose h is a unit

and $a \leq b$, we get $g = f^a(1 + uf^{b-a})$, and $1 + uf^{b-a}h$ is a unit because $uf^{a-b}h$ is nilpotent. So $J = f^aA$ or $J = (f^a + uf^bh)A$ with $a > b$.

Step 3: Finally, we have 4 cases:

1. $I = (0)$ or $I = A$, which is type 1.
2. I is a principal ideal with $\nu(I) = 1$. In this case, $I = uf^\tau A$, which is type 2.
3. I is a principal ideal with $\nu(I) = 0$. In this case $I = (f^\delta + uf^th)A$ with $\delta > t$ and h is either unit or zero. This corresponds to type 3.
4. I is not a principal ideal. In this case, $I = a_1A + ua_2A$. Since a_1A is a principal ideal, $a_1A = (f^\delta + uf^th)A$ with $\delta > t$ and h either a unit or zero. Therefore, $I = (f^\delta + uf^th)A + uf^\omega A$. Since $uf^\delta \in (f^\delta + uf^th)$, if $\omega \geq \delta$, we get $I = (f^\delta + uf^th)A + uf^\omega A = (f^\delta + uf^th)A$, which is principal, then $\omega < \delta$. Moreover, if $t \geq \omega$, the ideal I could be written as $I = f^\delta A + uf^\omega A$, which is also of type 4 for $h = 0$.

$\square$

We should now compute the parameter L.

Proposition 3. *Let $f(x) = x^4 + x^3 + x^2 + x + 1$ and $L = \min\{k \in \mathbb{N}_\delta \mid uf^k \in \langle f^\delta + uf^th\rangle\}$*

$$L = \begin{cases} \delta, & if\ h = 0, \\ \min(\delta, p^s - \delta + t), & if\ h \neq 0. \end{cases}$$

Proof. Suppose $uf^\omega = (f^\delta + uf^th)(g_0'f^{g_0} + ug_1'f^{g_1})$ with g_i' is a unit or zero and $g_0 > g_1$. Then

$$\begin{cases} g_0'f^{g_0+\delta} = 0, \\ g_1'f^{\delta+g_1} + g_0'hf^{g_0+t} = f^\omega. \end{cases}$$

Then $g_0 + \delta \geq p^s$. Let $k_0 = g_0 + \delta - p^s$. We get,

$$g_1'f^{\delta+g_1} + g_0'hf^{p^s-\delta+k_0+t} = f^\omega.$$

Since $\delta + g_1 > \omega$, if $h = 0$, the equation is impossible. Else, $\nu(g_1'f^{\delta+g_1} + g_0'hf^{p^s-\delta+k_0+t}) = p^s - \delta + k_0 + t = \omega$. It follows that $\omega \geq p^s - \delta + t$, while $h \neq 0$. $\square$

The classification of cyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ was given by Dinh in [6]:

Theorem 2 (see [6]). *Let $f'(x) = x - 1$. The cyclic codes of length p^s over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ are:*

1. *Type 1: $\mathcal{C}_1'$:* $\langle 0\rangle$; $\langle 1\rangle$.
2. *Type 2: $\mathcal{C}_2'(\tau)$:* $\langle uf'(x)^\tau\rangle$; *where $0 \leq \tau \leq p^s - 1$.*
3. *Type 3: $\mathcal{C}_3'(\delta, t, h)$:* $\langle f'^\delta + uf'^th\rangle$;
where $\delta > t$, either h is 0 or h is a unit in $R[X]/\langle(f'(X))^{p^s}\rangle$ of the form $\sum_{i=0}^{L-t-1} h_if'^i$ with $\deg(h_i) \leq 1$ and $h_0 \neq 0$.

4. *Type 4:* $\mathcal{C}'_4(\delta,t,h,\omega)$: $\langle f'^{\delta}+uf'^{t}h, uf'^{\omega}\rangle$;
where $p^s>\delta\geq T>\omega>t\geq 0$, *either* h *is* 0 *or* h *is a unit in* $R[X]/\langle (f'(X))^{p^s}\rangle$. *Here* T *is the smallest integer satisfying* $uf'^{T}\in\mathcal{C}'_3(\delta,t,h)$.

Proposition 4. *[6] Let* $f'(x)=x-1$ *and* $T=\min\{k\in\mathbb{N}_\delta \mid uf'^{k}\in\langle f'^{\delta}+uf'^{t}h\rangle\}$

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

4. Dual codes of the 5-cyclotomic codes of length $4p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$

Let $f(x)=x^4+x^3+x^2+x+1$ and $p\equiv 2 \pmod 5$ or $p\equiv 3 \pmod 5$, and let m be odd. According to Theorem 1, we compute the dual code of each type of 5-cyclotomic codes of length $4p^s$ over $R=\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$.
For a 5-cyclotomic code C, its dual is $C^{\perp}=Ann(C)^*=\{k^*\mid kg=0,(\forall g\in C)\}$, where k^* is the reciprocal polynomial of k defined by $k^*(x)=x^{\deg(k)}k(\frac{1}{x})$.

Remark 1. *Remark that* $f^*=f$. *Indeed,* $f^*(x)=x^4(\frac{1}{x^4}+\frac{1}{x^3}+\frac{1}{x^2}+\frac{1}{x}+1)=f(x)$.

For type 1, it is obvious that $\langle 0\rangle^{\perp}=\langle 1\rangle$ and $\langle 1\rangle^{\perp}=\langle 0\rangle$.
Let us now show other types.

Proposition 5. *Using the above notations, we have*

$$\mathcal{C}_2(\tau)^{\perp}=\mathcal{C}_4(p^s-\tau,0,0,0).$$

Proof. Let $g\in R[X]/\langle (f(X))^{p^s}\rangle\setminus\{0\}$ such that $uf^{\tau}\times g=0$. There exist $a_0,a_1\in\mathbb{N}$, $h_0,h_1\in\mathbb{F}_{p^m}[X]/\langle (f(X))^{p^s}\rangle$ with h_0 a unit and h_1 either a unit or zero, verifying $g=h_0(f^{a_0}+uf^{a_1}h_1)$ and $a_0>a_1$. Then, $uf^{\tau}\times g=uf^{\tau+a_0}h_0=0$. Therefore, $\tau+a_0\geq p^s$, namely $a_0\geq p^s-\tau$. Thus, $g\in\langle f^{p^s-\tau},u\rangle$. Conversely, it is obvious that $f^{p^s-\tau}\times uf^{\tau}=0$ and $u\times uf^{\tau}=0$. Therefore, $\mathcal{C}_2(\tau)^{\perp}=\langle f^{p^s-\tau},u\rangle^*=\langle f^{p^s-\tau},u\rangle=\mathcal{C}_4(p^s-\tau,0,0,0)$. □

Proposition 6. *Using the above notations, we have*

$$\mathcal{C}_3(\delta,t,h)^{\perp}=\begin{cases}\mathcal{C}_3(p^s-\delta,0,0), & if\ h=0,\\ \mathcal{C}_3(p^s-\delta,p^s+t-2\delta+v,-H), & if\ h\neq 0\ and\ p^s\geq 2\delta-t,\\ \mathcal{C}_3(\delta-t,v,-H), & if\ h\neq 0\ and\ p^s\leq 2\delta-t,\end{cases}$$

with $v=\max\{k\in\mathbb{N}\mid f^k$ *dividing* $x^{4(\delta-t)}h(\frac{1}{x})\}$ *and* $x^{4(\delta-t)}h(\frac{1}{x})=f^{v}(x)H(x)$ *for some* H, *which is either a unit or zero.*

Proof. Let $g\in R[X]/\langle f(X)^{p^s}\rangle\setminus\{0\}$ such that $(f^{\delta}+uf^{t}h)\times g=0$. There exist $a_0,a_1\in\mathbb{N}$, $h_0,h_1\in\mathbb{F}_{p^m}[X]/\langle f(X)^{p^s}\rangle$ with h_0 a unit and h_1 either a unit or zero, verifying $g=h_0(f^{a_0}+uf^{a_1}h_1)$ and $a_0>a_1$. Then, $(f^{\delta}+uf^{t}h)\times g=h_0(f^{\delta+a_0}+u(f^{\delta+a_1}h_1+f^{t+a_0}h))=0$. Therefore,

$$\begin{cases}f^{\delta+a_0}=0,\\ f^{\delta+a_1}h_1+f^{t+a_0}h=0.\end{cases}$$

By the first equation, there exists $k_0 \in \mathbb{N}$ such that $a_0 = p^s - \delta + k_0$. Then, the second equation becomes as follows:

$$f^{\delta+a_1}h_1 = -f^{t+p^s-\delta+k_0}h.$$

Case 1: If $h = 0$, we choose $t = 0$. Then, $f^{\delta+a_1}h_1 = 0$. It follows that $h_1 = 0$ or $a_1 = p^s - \delta + k_1$ for some $k_1 \in \mathbb{N}$. Therefore, $g = h_0(f^{p^s-\delta+k_0} + uf^{p^s-\delta+k_1}h_1)$ with h_1 a unit or zero. In particular, when $k_0 = k_1 = 0$, it is easy to notice that $(f^\delta + uf^t h) \times g = 0$. Thus,

$$\mathcal{C}_3(\delta, 0, 0)^\perp = \langle f^{p^s-\delta}\rangle^* = \langle f^{p^s-\delta}\rangle = \mathcal{C}_3(p^s - \delta, 0, 0).$$

Case 2: If h a unit, then we suppose that $p^s + t - \delta + k_0 < p^s$. Then $\delta + a_1 = t + p^s - \delta + k_0$, and $h_1 = -h$. Then, $g = h_0(f^{p^s-\delta+k_0} - uf^{p^s+t-2\delta+k_0}h)$ with $p^s + t - 2\delta + k_0 \geq 0$, namely $k_0 \geq 2\delta - t - p^s$. So we put $k_0 = \max\{0, 2\delta - t - p^s\}$.

If $0 \geq 2\delta - t - p^s$, then

$$\mathcal{C}_3(\delta, t, h)^\perp = \langle f^{p^s-\delta} - uf^{p^s+t-2\delta}h\rangle^* = \langle f^{p^s-\delta} - uf^{p^s+t-2\delta}x^{4(\delta-t)}h(\frac{1}{x})\rangle.$$

Let $v = \max\{k \in \mathbb{N} \mid f^k \text{ divide } x^{4(\delta-t)}h(\frac{1}{x})\}$; then $x^{4(\delta-t)}h(\frac{1}{x}) = f^v(x)H(x)$ with H either a unit or zero. Thus,

$$\mathcal{C}_3(\delta, t, h)^\perp = \mathcal{C}_3(p^s - \delta, p^s + t - 2\delta + v, -H).$$

If $0 < 2\delta - t - p^s$, then

$$\mathcal{C}_3(\delta, t, h)^\perp = \langle f^{\delta-t} - uh\rangle^* = \langle f^{\delta-t} - ux^{4(\delta-t)}h(\frac{1}{x})\rangle.$$

Let $v = \max\{k \in \mathbb{N} \mid f^k \text{ divide } x^{4(\delta-t)}h(\frac{1}{x})\}$. Then, $x^{4(\delta-t)}h(\frac{1}{x}) = f^v(x)H(x)$ with H either a unit or zero. Thus,

$$\mathcal{C}_3(\delta, t, h)^\perp = \mathcal{C}_3(\delta - t, v, -H).$$

$\square$

Proposition 7. *Using the above notations, we have*

$$\mathcal{C}_4(\delta, t, h, \omega)^\perp = \begin{cases} \mathcal{C}_4(p^s - \omega, 0, 0, p^s - \delta), & if\ h = 0, \\ \mathcal{C}_3(p^s - \omega, p^s + t - \delta - \omega + v, -H), & if\ h \neq 0\ and\ p^s \geq \delta + \omega - t, \\ \mathcal{C}_3(\delta - t, v, -H), & if\ h \neq 0\ and\ p^s \leq \delta + \omega - t, \end{cases}$$

with $v = \max\{k \in \mathbb{N} \mid f^k$ *dividing* $x^{4(\delta-t)}h(\frac{1}{x})\}$ *and* $x^{4(\delta-t)}h(\frac{1}{x}) = f^v(x)H(x)$ *for some* H *which is either a unit or zero.*

Proof. Let $g \in R[X]/\langle f(X)^{p^s}\rangle \setminus \{0\}$ such that

$$\begin{cases} g \times (f(x)^\delta + uf(x)^t h(x)) = 0, \\ g \times uf(x)^\omega = 0. \end{cases}$$

Namely, $g \in \mathcal{C}_3(\delta, t, h)^\perp \cap \mathcal{C}_2(\omega)^\perp$. By the previous proofs done, we distinguish two cases:

Case 1: If $h = 0$, then $g = h_0(f^{p^s-\omega+k_0} + uf^{v_1}h_1) \in \langle f^{p^s-\delta}\rangle$ with $k_0, v_1 \in \mathbb{N}$, h_1 either a unit or zero and h_0 a unit. It follows that

$$\begin{cases} p^s - \omega + k_0 \geq p^s - \delta \\ v_1 \geq p^s - \delta \end{cases} \qquad \Leftrightarrow \qquad v_1 \geq p^s - \delta.$$

Therefore, $g \in \langle f^{p^s-\omega}, uf^{p^s-\delta}\rangle$. Conversely, $f^{p^s-\omega}, uf^{p^s-\delta} \in \mathcal{C}_3(\delta, t, h)^\perp \cap \mathcal{C}_2(\omega)^\perp$. Thus,

$$\mathcal{C}_4(\delta, 0, 0, \omega)^\perp = \langle f^{p^s-\omega}, uf^{p^s-\delta}\rangle = \mathcal{C}_4(p^s - \omega, 0, 0, p^s - \delta).$$

Case 2: If $h \neq 0$, then $g = h_0(f^{p^s-\delta+k_0} - uf^{p^s+t-2\delta+k_0}h) \in \langle f^{p^s-\omega}, u\rangle$ with h_0 a unit and $k_0 \in \mathbb{N}$. It follows that

$$p^s - \delta + k_0 \geq p^s - \omega \qquad \Leftrightarrow \qquad k_0 \geq \delta - \omega.$$

In the proof of Proposition 6, we had $k_0 \geq \max\{0, 2\delta - t - p^s\}$. Then, we get $k_0 \geq \max\{\delta - \omega, 2\delta - t - p^s\}$.
If $\delta - \omega \geq 2\delta - t - p^s$, then $k_0 = \delta - \omega + k'$ for some $k' \in \mathbb{N}$, as well as $g = h_0(f^{p^s-\omega+k'} - uf^{p^s+t-\delta-\omega+k'}h) \in \langle f^{p^s-\omega} - uf^{p^s+t-\delta-\omega}h\rangle$. Then,

$$\begin{aligned} \mathcal{C}_4(\delta, t, h(x), \omega)^\perp &= \langle f^{p^s-\omega} - uf^{p^s+t-\delta-\omega}h\rangle^* \\ &= \langle f^{p^s-\omega} - uf^{p^s+t-\delta-\omega}x^{4(\delta-t)}h(\frac{1}{x})\rangle. \end{aligned}$$

Let $v = \max\{k \in \mathbb{N} \mid f^k \text{ divide } x^{4(\delta-t)}h(\frac{1}{x})\}$. Then $x^{4(\delta-t)}h(\frac{1}{x}) = f^v(x)H(x)$ with H either a unit or zero. Thus,

$$\mathcal{C}_4(\delta, t, h, \omega)^\perp = \mathcal{C}_3(p^s - \omega, p^s + t - \delta - \omega + v, -H).$$

If $\delta - \omega \leq 2\delta - t - p^s$, then $k_0 = 2\delta - t - p^s + k'$ for some $k' \in \mathbb{N}$, as well as $g = h_0(f^{\delta-t+k'} - uf^{k'}h) \in \langle f^{\delta-t} - uh\rangle$. Then,

$$\mathcal{C}_4(\delta, t, h, \omega)^\perp = \langle f^{\delta-t} - uh\rangle^* = \langle f^{\delta-t} - ux^{4(\delta-t)}h(\frac{1}{x})\rangle.$$

Let $v = \max\{k \in \mathbb{N} \mid f^k \text{ divide } x^{4(\delta-t)}h(\frac{1}{x})\}$. Then $x^{4(\delta-t)}h(\frac{1}{x}) = f^v(x)H(x)$ with H either a unit or zero. Thus,

$$\mathcal{C}_4(\delta, t, h, \omega)^\perp = \mathcal{C}_3(\delta - t, v, -H).$$

□

Now, for $f'(x) = x - 1$, we have $f'^* = -f$. We will get the same results with very little difference that some powers of -1 will appear.

Proposition 8. *Using the above notations, we have*

$$\mathcal{C}'_2(\tau)^\perp = \mathcal{C}'_4(p^s - \tau, 0, 0, 0).$$

Proposition 9. *Using the above notations, we have*

$$\mathcal{C}_3'(\delta,t,h)^{\perp}=\begin{cases}\mathcal{C}_3'(p^s-\delta,0,0), & if\ h=0,\\ \mathcal{C}_3'(p^s-\delta,p^s+t-2\delta+v,(-1)^{p^s+t+1}H), & if\ h\neq 0\ and\ p^s\geq 2\delta-t,\\ \mathcal{C}_3'(\delta-t,v,-H), & if\ h\neq 0\ and\ p^s\leq 2\delta-t,\end{cases}$$

with $v=\max\{k\in\mathbb{N}\mid f'^k$ *dividing* $x^{\delta-t}h(\frac{1}{x})\}$ *and* $x^{\delta-t}h(\frac{1}{x})=f'^v(x)H(x)$ *for some* H *which is either a unit or zero.*

Proposition 10. *Using the above notations, we have*

$$\mathcal{C}_4'(\delta,t,h,\omega)^{\perp}=$$

$$\begin{cases}\mathcal{C}_4'(p^s-\omega,0,0,p^s-\delta) & if\ h=0,\\ \mathcal{C}_3'(p^s-\omega,p^s+t-\delta-\omega+v,(-1)^{p^s+t-\delta-\omega+1}H) & if\ h\neq 0\ and\ p^s\geq \delta+\omega-t,\\ \mathcal{C}_3'(\delta-t,v,-H) & if\ h\neq 0\ and\ p^s\leq \delta+\omega-t,\end{cases}$$

with $v=\max\{k\in\mathbb{N}\mid f'^k$ *dividing* $x^{\delta-t}h(\frac{1}{x})\}$ *and* $x^{\delta-t}h(\frac{1}{x})=f'^v(x)H(x)$ *for some* H *which is either a unit or zero.*

References

[1] A. Arnold, M. Monagan, *Calculating cyclotomic polynomials*, Math. Comp. **80**(2011), 2359–2379.

[2] M. Atiyah, *Introduction to commutative algebra*, CRC Press, Boca Raton, 2018.

[3] W. C. Brown, *Matrices over commutative rings*, Marcel Dekker Inc., New York, 1993.

[4] M. E. Charkani, B. Boudine, *On the integral ideals of R[X] when R is a special principal ideal ring*, Sao Paulo J. Math. Sci. **14**(2020), 698–702.

[5] B. Chen, H. Q. Dinh, H. Liu, *Repeated-root constacyclic codes of length* lp^s *and their duals*, Discrete Appl. Math. **177**(2014), 60–70.

[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, *Structure of repeated-root constacyclic codes of length* $3p^s$ *and their duals*, Discrete Math. **313**(2013) 983-991.

[9] H. Q. Dinh, *On repeated-root constacyclic codes of length* $4p^s$, Asian-Eur. J. Math. **6**(2013), 1350020.

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

[11] H. M. Kiah, K. H. Leung, S. Ling, *A note on cyclic codes over* $GR(p^2,m)$ *of length* p^k, Des. Codes Cryptogr. **63**(2012), 105–112.

[12] H. M. Kiah, K. H. Leung, S. Ling, *Cyclic codes over* $GR(p^2,m)$ *of length* p^k, Finite Fields Appl. **14**(2008), 834–846.

[13] S. Ling, X. Chaoping, *Coding theory: a first course*, Cambridge University Press, Cambridge, 2004.

[14] X. Liu, X. Xu, *Cyclic and negacyclic codes of length* $2p^s$ *over* $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, Acta Math. Sci. B **34**(2014), 829–839.

[15] J. Neukirch, *Algebraic number theory*, Springer Science & Business Media **322**, Springer, Berlin, Heidelberg, 2013.

[16] J. PHUTO, C. KLIN-EAM, *Explicit constructions of cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, Discrete Math. Algorithms Appl. **12**(2020), 2050063.

[17] E. PRANGE, *Cyclic error-correcting codes in two symbols*, Air Force Cambridge Research Center, 1957.

[18] E. PRANGE, *Some Cyclic Error-Correcting Codes with Simple Decoding Algorithms*, Air Force Cambridge Research Center-TN-58-156, Cambridge, MA, April 1958.

[19] R. SOBHANI, *Complete classification of $(\sigma + \alpha u^2)$-constacyclic codes of length p^k over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$*, Finite Fields Appl. **34**(2015), 123–138.

[20] H. WU, L. ZHU, R. FENG, S. YANG, *Explicit factorizations of cyclotomic polynomials over finite fields*, Des. Codes Cryptogr. **83**(2016), 197–217.