Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

On negacyclic codes of length $5p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

Brahim Boudine[1,✉], Jamal Laaaouine[2], Hamid Ben Yakkou[3]

[1] *Faculty of Sciences, Moulay Ismail University, Meknes, Morocco*
[2] *Faculty of Sciences Dhar El Mahraz, Sidi Mohamed Ben Abdellah University, Fez, Morocco*
[3] *Polydisciplinary Faculty Beni Mellal, Sultan Moulay Slimane University, Beni Mellal, Morocco*

ABSTRACT

Let $p > 5$ be a prime positive integer, m and s be positive integers. We classify the negacyclic codes of length $5p^s$ over $R = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, with $u^2 = 0$ using the factorisation of cyclotomic polynomials, and we investigate their Hamming distances.

Keywords: negacyclic code, cyclotomic polynomial, Hamming distance

1. Introduction

The classification of error-correcting codes is an important task in the algebraic coding theory. Many kinds of error-correcting codes have been classified for example Ghose and Dey [14] classified $[5, 3]$ error-correcting codes over $GF(5)$. In particular, for any positive integer n, negacyclic codes of length n are the codes $\mathscr{C}$ such that: $(c_0, ..., c_n)$ is a codeword in $\mathscr{C}$ implies that $(-c_n, c_0, c_1, ..., c_{n-1})$ is a codeword in $\mathscr{C}$. Therefore, the negacyclic codes of length n over a given field K are the ideals of the ring $K[X]/\langle X^n + 1\rangle$ [13].

Let p be a prime integer, m and s be two positive integers. Then, negacyclic codes of length p^s over $\mathbb{F}_{p^m}$ was completely classified, see [5, 10, 11, 12]. Then, they have been generalized over finite rings instead of fields only, due to their successful application in combined coding and modulation [7]. In 2010, Dinh [9] classified λ-constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where λ is a unit. In particular, if $\lambda = -1$, then we get negacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. In 2014, Liu and Xu [19] classified cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. In 2020, Phuto and Klin-Eam [21] classified cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Afterward, Laaouine et al. [17] classified constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$. Then, in 2022 Boudine et al. classified cyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$ [3], negacyclic codes of

✉ Corresponding author.
E-mail address: b.boudine@umi.ac.ma (B. Boudine).

Received 03 May 2025; Revised 29 May 2025; Accepted 3 June 2025; Published 24 June 2025.

DOI: 10.61091/jcmcc126-21

length $3p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$ [4], and cyclic codes of length $5p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ [2].

Recall that for any codeword $x=(x_0,x_1,...,x_{n-1})\in R^n$, the number of nonzero components of x is called the Hamming weight of x, denoted by $wt_H(x)$. Then, the Hamming distance $d_H(x,y)$ of two codewords x and y is the number of components in which they differ; namely, it is the Hamming weight $wt_H(x-y)$ of $x-y$. Let $\mathscr{C}$ be a nonzero linear code, the Hamming weight $wt_H(\mathscr{C})$ and the Hamming distance $d_H(\mathscr{C})$ are the same and defined to be the smallest Hamming weight of nonzero codewords of $\mathscr{C}$; formally, $d_H(\mathscr{C})=\min\{wt_H(x)\mid 0\neq x\in\mathscr{C}\}$, and the zero code is conventionally said to have Hamming distance 0. The Hamming distance is an important tool in the algebraic coding theory. It allows to compute how many errors could be corrected by the code, and it is used also to construct new quantum codes. In 2021, Laaouine and Charkani [18] completed the determination of Hamming distance of constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^s}+u\mathbb{F}_{p^s}$, and Dinh et al. [16] computed Hamming distance of constacyclic codes of length p^s over $\mathbb{F}_{p^s}+u\mathbb{F}_{p^s}+u^2\mathbb{F}_{p^s}$.

In this paper, we give a complete classification of negacyclic codes of length $5p^s$ over $R=\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, and we give their Hamming distances in terms of the Hamming distances of codes of the form $\langle f(x)^q\rangle$ for a given monic polynomial $f(x)$ and an integer q. Our classification method is based on the valuation ideas used in number theory over fields (see [20]), and we use cyclotomic polynomials and their factorizations. This gives the opportunity to simplify proofs and transforms the codes classification problem to the polynomials factorization problem. Furthermore, we compute an important parameter L which allows to avoid the repetition of codes in different given types, and it will be crucial to determine Hamming distances.

We show that negacyclic codes of length $5p^s$ could be written as a direct sum of $n-$cyclotomic codes. So we recall some generalities of $n-$cyclotomic codes. Then, the factorization of the cyclotomic polynomial $\Phi_{10}(X)$ yields a decomposition of our negacyclic code according to the $\Phi_{10}(X)$ irreducible factors. Therefore, we distinguish 3 cases for $q=p^m$:

Case 1: when $q\equiv 3 \pmod{10}$ or $q\equiv 7 \pmod{10}$.

Case 2: when $q\equiv 1 \pmod{10}$.

Case 3: when $q\equiv 9 \pmod{10}$.

For each case, we get a different factorization of $\Phi_{10}(X)$ and then a different structure for the negacyclic code. So we give the Hamming distances for each case.

2. Preliminaries

Let $p>5$ be a prime number, m and s be positive integers and $R=\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ with $u^2=0$. For each element x of R there are $x_1,x_2\in\mathbb{F}_{p^m}$ such that $x=x_0+ux_1$. Let $\nu(x)=min\{i\in\{0,1\}\mid x_i\neq 0\}$. For each ideal I of R we set $\nu(I)=max\{i\in\{0,1\}\mid I\subseteq u^iR\}$. Also in $R[X]$, for each polynomial $f(X)$, there are $f_0(X),f_1(X)\in\mathbb{F}_{p^m}[X]$ such that $f(X)=f_0(X)+uf_1(X)$. So we set $\nu(f)=min\{i\in\{0,1\}\mid f_i\neq 0\}$, and $\nu(I)=max\{i\in\{0,1\}\mid I\subseteq u^iR[X]\}$ for each ideal I in $R[X]$.

Negacyclic codes of length k over R are the ideals of the ring $R[X]/\langle X^k+1\rangle$ [13]. In order to factorize the polynomial X^k+1 we may need cyclotomic polynomials denoted by $\Phi_n(X)$, they are defined as special divisors of polynomials of the form X^n-1. When n is prime [1]

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

For the negacyclic codes of length $5p^s$ over R, we should factorize the polynomial $X^{5p^s}+1$. Since $\mathbb{F}_{p^m}$ is a field of characteristic p,

$$(X^{5p^s}+1)=(X^5)^{p^s}+1^{p^s}=(X^5+1)^{p^s}=(X+1)^{p^s}\times\Phi_{10}(X)^{p^s}.$$

Lemma 2.1. *With the above notations. If $\mathscr{C}$ is a negacyclic code of length $5p^s$ over $\mathbb{F}_{p^m}$ then:*

$$\mathscr{C} = \mathscr{C}_1 \oplus \mathscr{C}',$$

with $\mathscr{C}_1$ is a negacyclic code of length p^s over R and $\mathscr{C}'$ is an ideal of $R[X]/\langle \Phi_{10}(X)^{p^s}\rangle$.

Proof. We know that $\mathscr{C}$ is an ideal of $R[X]/\langle (X^5+1)^{p^s}\rangle$. Since $X^5+1 = (X+1)\Phi_{10}(X)$ with $(X+1)$ and $\Phi_{10}(X)$ are coprime, the Chinese remainder theorem proves that

$$\mathbb{F}_{p^m}[X]/\langle (X^5+1)^{p^s}\rangle = \mathbb{F}_{p^m}[X]/\langle (X+1)^{p^s}\rangle \oplus \mathbb{F}_{p^m}[X]/\langle \Phi_{10}(X)^{p^s}\rangle.$$

Thus $\mathscr{C}$ is a direct sum of an ideal of $R[X]/\langle (X+1)^{p^s}\rangle$ (which is a negacyclic code of length p^s) and an ideal of $R[X]/\langle \Phi_{10}(X)^{p^s}\rangle$. □

Negacyclic codes of length p^s over R was already classified by Dinh [9], so we should classify the ideals of $R[X]/\langle \Phi_{10}(X)^{p^s}\rangle$.

Let $q = p^m$, since p is a prime and $p \geq 7$, q does not divide neither 2 nor 5. Then, $q \equiv 1 \pmod{10}$, $q \equiv 3 \pmod{10}$, $q \equiv 7 \pmod{10}$ or $q \equiv 9 \pmod{10}$.

3. Classification of the ideals of $R[X]/(\Phi_{10}(X))^{p^s}$ when $q \equiv 3 \pmod{10}$ or $q \equiv 7 \pmod{10}$

Lemma 3.1. [23] *$\Phi_n(X)$ 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.*

Corollary 3.2. *$\Phi_{10}(X)$ is irreducible in $\mathbb{F}_q[X]$ if and only if $q \equiv 3 \pmod{10}$ or $q \equiv 7 \pmod{10}$.*

Proof. Indeed, $\langle\overline{3}\rangle = \langle\overline{7}\rangle = \{\overline{1}, \overline{3}, \overline{9}, \overline{7}\} = U(\mathbb{Z}/10\mathbb{Z})$ is the group of units of $\mathbb{Z}/10\mathbb{Z}$. However, $\langle\overline{9}\rangle = \{\overline{1}, \overline{9}\} \neq U(\mathbb{Z}/10\mathbb{Z})$. □

Lemma 3.3. *$q = p^m \equiv 3 \pmod{10}$ if and only if one of the following cases holds:*

(a) $p \equiv 3 \pmod{10}$ *and* $m \equiv 1 \pmod{4}$.

(b) $p \equiv 7 \pmod{10}$ *and* $m \equiv 3 \pmod{4}$.

Proof. If $p \equiv 1 \pmod{10}$ it is impossible to get $p^m \equiv 3 \pmod{10}$.

If $p \equiv 3 \pmod{10}$ we get $p^2 \equiv 9 \pmod{10}$, $p^3 \equiv 7 \pmod{10}$, $p^4 \equiv 1 \pmod{10}$ and $p^5 \equiv 3 \pmod{10}$ again. Then, $p^m \equiv 3 \pmod{10}$ if and only if $m \equiv 1 \pmod{4}$.

If $p \equiv 7 \pmod{10}$ we get $p^2 \equiv 9 \pmod{10}$, $p^3 \equiv 3 \pmod{10}$. Then $p^m \equiv 3 \pmod{10}$ if and only if $m \equiv 3 \pmod{4}$.

If $p \equiv 9 \pmod{10}$ we have $p^2 \equiv 1 \pmod{10}$ then it is impossible to get $p^m \equiv 3 \pmod{10}$. □

Lemma 3.4. *$q = p^m \equiv 7 \pmod{10}$ if and only if one of the following cases holds:*

(a) $p \equiv 3 \pmod{10}$ *and* $m \equiv 3 \pmod{4}$.

(b) $p \equiv 7 \pmod{10}$ *and* $m \equiv 1 \pmod{4}$.

Proof. Similar to the proof of Lemma 3.3. □

Theorem 3.5. *If p and m are as in Lemma 3.4 or in Lemma 3.3, then the ideals of $R[X]/\langle\Phi_{10}^{p^s}\rangle$ are:*

(a) *Type 1: $\mathscr{C}_1$, trivial ideals:*

$$\langle 0\rangle \quad ; \quad \langle 1\rangle.$$

(b) *Type 2: $\mathscr{C}_2(\tau)$, principal ideals in $\langle u\rangle$:*

$$\langle u\Phi_{10}(x)^{\tau}\rangle;\ \textit{where}\ 0\leq\tau\leq p^s-1.$$

(c) *Type 3: $\mathscr{C}_3(\delta,t,h(x))$, principal ideals which are not in $\langle u\rangle$:*

$$\langle\Phi_{10}(x)^{\delta}+u\Phi_{10}(x)^{t}h(x)\rangle;$$

where $\delta>t$, $h(x)$ is either 0 or a unit in $R[X]/\langle\Phi_{10}(X)^{p^s}\rangle$ of the form $\sum_{i=0}^{L-t-1}h_i\Phi_{10}(x)^i$ with $deg(h_i)\leq 1$, $h_0\neq 0$, and L is the smallest integer which satisfies $u\Phi_{10}(x)^L\in\mathscr{C}_3(\delta,t,h(x))$.

(d) *Type 4: $\mathscr{C}_4(\delta,t,h(x),\omega)$, non principal ideals:*

$$\langle\Phi_{10}(x)^{\delta}+u\Phi_{10}(x)^{t}h(x),u\Phi_{10}(x)^{\omega}\rangle;$$

where $p^s>\delta\geq L>\omega>t\geq 0$, $h(x)$ is either 0 or a unit in $R[X]/\langle\Phi_{10}(X)^{p^s}\rangle$, and L is the smallest integer verifying $u\Phi_{10}(x)^L\in\mathscr{C}_3(\delta,t,h(x))$.

Proof. Notice first that $\Phi_{10}(X)$ is irreducible. Let $A=R[X]/\langle\Phi_{10}(X)^{p^s}\rangle$, I be an ideal of A, and $\overline{I}=(I+uA)/uA$ be its image in A/uA. Since $A/uA\sim\mathbb{F}_{p^m}[X]/\langle\overline{\Phi_{10}}(X)^{p^s}\rangle$ is a principal ideal ring, there exists $a_1\in I$ such that $\overline{I}=\overline{a_1}A/uA$; namely, for each $x\in I$, we have $\overline{x}=\overline{a_1.b}$, where $b\in A$. Then $x=a_1.b+uc$ for some $c\in A$. As well $uc=x-a_1.b\in I$, and $c\in J_1=\{r\in A\mid ur\in I\}$. Therefore $I=a_1.A+uJ_1$. By the same method applied on J_1 we get that $J_1=a_2.A+u.J_2$ for $a_2\in I$, and $J_2=\{r\in A\mid ur\in J_1\}=\{r\in A\mid u^2r\in I\}$. Hence $I=a_1.A+ua_2.A$. Let $i\in\{1,2\}$. Since R is a special principal ideal ring [6], there exists a monic polynomial $g(x)$ such that $a_iA=\langle u^{\mu}g(x)\rangle$ where $\mu=\nu(a_iA)$ [see [8]]. Let $g_0,g_1\in\mathbb{F}_{p^m}[X]/\langle\Phi_{10}(X)^{p^s}\rangle$ such that $g=g_0+ug_1$, and $v_k=max\{i\in\{0,...,p^s\}\mid\Phi_{10}(X)^i$ divides $g_k\}$, for each $k\in\{0,1\}$. Then $g_k=\Phi_{10}(X)^{v_k}q$ where $q\in\mathbb{F}_{p^m}[X]/\langle\Phi_{10}(X)^{p^s}\rangle$. Since $\Phi_{10}(X)$ is irreducible and does not divide q, the Bezout identity proves that q is a unit in $\mathbb{F}_{p^m}[X]/\langle\Phi_{10}(X)^{p^s}\rangle$. Then we can take $g(x)=\Phi_{10}(x)^a+u\Phi_{10}(x)^bh(x)$, where a and b are two integers, and $h(x)$ is a unit in $\mathbb{F}_{p^m}[X]/\langle\Phi_{10}(X)^{p^s}\rangle$. Suppose that $a\leq b$, then $g=\Phi_{10}^a(1+u\Phi_{10}^{b-a})$ where $1+u\Phi_{10}^{b-a}h(x)$ is a unit since $u\Phi_{10}(x)^{a-b}h(x)$ is nilpotent. Hence, we have two possibilities: either $a_iA=\Phi_{10}^aA$ or $a_iA=(\Phi_{10}^a+u\Phi_{10}^bh(x))A$ with $a>b$. Therefore we distinguish four different cases:

(a) If either $I=(0)$ or $I=A$, then we obtain an ideal of the type 1.

(b) If I is a principal ideal with $\nu(I)=1$, then we get $I=u\Phi_{10}^{\tau}A$, and we obtain an ideal of the type 2.

(c) If I is a principal ideal with $\nu(I)=0$, then we get $I=(\Phi_{10}^{\delta}+u\Phi_{10}^th(x))A$ where $\delta>t$ and $h(x)$ is either a unit or zero. Then we obtain an ideal of type 3.

(d) If I is not a principal ideal, then $I=a_1A+ua_2A$. Since a_1A is a principal ideal, we get $a_1A=(\Phi_{10}^{\delta}+u\Phi_{10}^th(x))A$, where $\delta>t$ and $h(x)$ is either a unit or zero. Therefore $I=(\Phi_{10}^{\delta}+u\Phi_{10}^th(x))A+u\Phi_{10}^{\omega}A$. Furthermore, we know that $u\Phi_{10}^{\delta}\in\langle\Phi_{10}^{\delta}+u\Phi_{10}^th\rangle$. It follows that: if $\omega\geq\delta$, then $I=(\Phi_{10}^{\delta}+u\Phi_{10}^th(x))A+u\Phi_{10}^{\omega}A=(\Phi_{10}^{\delta}+u\Phi_{10}^th(x))A$, which is a principal ideal. It follows that $\omega<\delta$. And if $t\geq\omega$, then the ideal I will be of the form $I=\Phi_{10}^{\delta}A+u\Phi_{10}^{\omega}A$. Then we obtain an ideal of the type 4 where $h=0$. □

Let us compute the parameter L.

Proposition 3.6. *As above notations, for* $L=min\{k\in\mathbb{N}_{\delta}\mid\Phi_{10}^{k}\in\langle\Phi_{10}^{\delta}+u\Phi_{10}^{t}h(x)\rangle\}$ *we have:*

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

Proof. Suppose that $u\Phi_{10}^{\omega}=(\Phi_{10}^{\delta}+u\Phi_{10}^{t}h)(g_0'\Phi_{10}^{g_0}+ug_1'\Phi_{10}^{g_1})$, where g_i' is either a unit or zero and $g_0>g_1$. Then we obtain the equations:

$$\begin{cases}g_0'\Phi_{10}^{g_0+\delta}=0,\\ g_1'\Phi_{10}^{\delta+g_1}+g_0'h\Phi_{10}^{g_0+t}=\Phi_{10}^{\omega}.\end{cases}$$

Then $g_0+\delta\geq p^s$. Set $k_0=g_0+\delta-p^s$. It follows that

$$g_1'\Phi_{10}^{\delta+g_1}+g_0'h\Phi_{10}^{p^s-\delta+k_0+t}=\Phi_{10}^{\omega}.$$

We know that $\delta+g_1>\omega$. If $h=0$, then the equation has no solution. Else, we get $\nu(g_1'\Phi_{10}^{\delta+g_1}+g_0'h\Phi_{10}^{p^s-\delta+k_0+t})=p^s-\delta+k_0+t=\omega$. Therefore $\omega\geq p^s-\delta+t$, since $h\neq 0$. □

Theorem 3.7. *Let us keeping the same notations as in Theorem 3.5. Then:*

$$\begin{cases}d_H(\mathscr{C}_2(\tau))=d_H(\langle\Phi_{10}(x)^{\tau}\rangle),\\ d_H(\mathscr{C}_3(\delta,t,h(x)))=d_H(\langle\Phi_{10}(x)^{L}\rangle),\\ d_H(\mathscr{C}_4(\delta,t,h(x),\omega))=d_H(\langle\Phi_{10}(x)^{\omega}\rangle).\end{cases}$$

Proof. • If we multiply the codewords of $\langle\Phi_{10}(x)^{\tau}\rangle$, then we get all the codewords of $\mathscr{C}_2(\tau)$. Therefore, $d_H(\mathscr{C}_2(\tau))=d_H(\langle\Phi_{10}(x)^{\tau}\rangle)$.

• Let us compute $d_H(\mathscr{C}_3(\delta,t,h(x)))$. Suppose that $c(x)$ is a nonzero element of $\mathscr{C}_3(\delta,t,h(x))$. Then $c(x)=(g_0(x)+ug_1(x))(f(x)^{\delta}+uf(x)^{t}h(x))$, where $g_0(x),g_1(x)\in\mathbb{F}_{p^m}[x]$. It follows that $uc(x)=ug_0(x)\Phi_{10}(x)^{\delta}$. Thus, we get:

$$\begin{aligned}wt_H(c(x)) &\geq wt_H(uc(x))\\ &=wt_H(ug_0(x)\Phi_{10}(x)^{\delta})\\ &\geq d_H(\langle u\Phi_{10}(x)^{\delta}\rangle)\\ &=d_H(\mathscr{C}_2(\delta)).\end{aligned}$$

Furthermore, we know that L is the smallest integer which satisfies $\langle u\Phi_{10}(x)^{L}\rangle\subseteq\langle\Phi_{10}(x)^{\delta}+u\Phi_{10}(x)^{t}h(x)\rangle$ and $\langle u\Phi_{10}(x)^{\delta}\rangle\subseteq\langle\Phi_{10}(x)^{\delta}+u\Phi_{10}(x)^{t}h(x)\rangle$, then $L\leq\delta$ and $\langle u\Phi_{10}(x)^{\delta}\rangle\subseteq\langle u\Phi_{10}(x)^{L}\rangle$. So we get that $d_H(\langle u\Phi_{10}(x)^{\delta}\rangle)\geq d_H(\langle u\Phi_{10}(x)^{L}\rangle)$. Therefore $wt_H(c(x))\geq d_H(\langle u\Phi_{10}(x)^{L}\rangle)$, for each nonzero element $c(x)$ of $\mathscr{C}_3(\delta,t,h(x))$; namely, $d_H(\mathscr{C}_3(\delta,t,h(x)))\geq d_H(\langle\Phi_{10}(x)^{L}\rangle)$. Finally, we have $\langle\Phi_{10}(x)^{L}\rangle\subseteq\mathscr{C}_3(\delta,t,h(x))$, then we obtain that $d_H(\langle\Phi_{10}(x)^{L}\rangle)=d_H(\mathscr{C}_3(\delta,t,h(x)))$.

• Let us compute $d_H(\mathscr{C}_4(\delta, t, h(x), \omega))$. Suppose that $c'(x)$ is a nonzero element in $\mathscr{C}_4(\delta, t, h(x), \omega)$. Then, we get

$$\begin{aligned} wt_H(c'(x)) &\geq \min(d_H(\mathscr{C}_3(\delta, t, h(x)), d_H(\langle \Phi_{10}(x)^{\omega} \rangle)) \\ &= \min(d_H(\langle \Phi_{10}(x)^{L} \rangle), d_H(\langle \Phi_{10}(x)^{\omega} \rangle)) \\ &= d_H(\langle \Phi_{10}(x)^{\omega} \rangle) \text{ since } L > \omega. \end{aligned}$$

Furthermore, we have

$$\langle \Phi_{10}(x)^{\omega} \rangle \subseteq \mathscr{C}_4(\delta, t, h(x), \omega),$$

which yields that $d_H(\mathscr{C}_4(\delta, t, h(x), \omega)) = d_H(\langle \Phi_{10}(x)^{\omega} \rangle)$. □

4. Classification of the ideals of $R[X]/\langle \Phi_{10}(X)^{p^s} \rangle$ when $q \equiv 1 \pmod{10}$

Lemma 4.1 (Theorem 3.1 and Theorem 3.2, [22]). *If $q \equiv 1 \pmod{10}$, then*

$$\Phi_{10}(X) = (X + \omega_1)(X + \omega_2)(X + \omega_3)(X + \omega_4),$$

where ω_k are different primitive roots modulo 5.

Lemma 4.2. *$q = p^m \equiv 1 \pmod{10}$ if and only if one of the following cases holds:*

(a) *$p \equiv 1 \pmod{10}$.*
(b) *$p \equiv 3 \pmod{10}$ and $m \equiv 0 \pmod{4}$.*
(c) *$p \equiv 7 \pmod{10}$ and $m \equiv 0 \pmod{4}$.*
(d) *$p \equiv 9 \pmod{10}$ and m is even.*

Proof. If $p \equiv 1 \pmod{10}$, then it is obvious that $p^m \equiv 1 \pmod{10}$. If $p \equiv 3 \pmod{10}$, then we get $p^2 \equiv 9 \pmod{10}$, $p^3 \equiv 7 \pmod{10}$, and $p^4 \equiv 1 \pmod{10}$. Then $p^m \equiv 1 \pmod{10}$ if and only if $m \equiv 0 \pmod{4}$. Likewise, if $p \equiv 7 \pmod{10}$, then we get $p^m \equiv 1 \pmod{10}$ if and only if $m \equiv 0 \pmod{4}$. If $p \equiv 9 \pmod{10}$, then we get $p^2 \equiv 1 \pmod{10}$, then $p^m \equiv 1 \pmod{10}$ if and only if m is even. □

Theorem 4.3. *If p and m are as in the Lemma 4.2, then the ideals of $R[X]/\langle \Phi_{10}(X)^{p^s} \rangle$ are of the form*

$$\mathscr{C} = \mathscr{C}_1 \oplus \mathscr{C}_2 \oplus \mathscr{C}_3 \oplus \mathscr{C}_4,$$

such that, for each $k \in \{1, 2, 3, 4\}$, $\mathscr{C}_k$ is a $-\omega_k^{p^s}$-constacyclic code of length p^s over R, and ω_k are some different primitive roots modulo 5.

Proof. By Lemma 4.1, $\Phi_{10}(X) = (X + \omega_1)(X + \omega_2)(X + \omega_3)(X + \omega_4)$. The Chinese remainder theorem proves that

$$R[X]/\langle \Phi_{10}(X)^{p^s} \rangle = \bigoplus_{k=1}^{4} R[X]/\langle (X + \omega_k)^{p^s} \rangle.$$

For any $k \in \{1, 2, 3, 4\}$ we can see that the ideals of $R[X]/\langle (X+\omega_k)^{p^s} \rangle$ are $-\omega_k^{p^s}$-constacyclic codes of length p^s over R. □

Constacyclic codes of length p^s over R are already given by Dinh in [9], and their Hamming distances had been computed by Dinh et al. [15].

5. Classification of the ideals of $R[X]/\langle(\Phi_{10}(X))^{p^s}\rangle$ when $q\equiv 9 \pmod{10}$

Lemma 5.1 (Theorem 3.4 and Theorem 3.5, [22]). *If $q\equiv 9 \pmod{10}$ then*

$$\Phi_{10}(X)=(X^2+(\alpha+\alpha^{-1})X+1)(X^2+(\alpha^2+(\alpha^2)^{-1})X+1),$$

where α is a primitive root modulo 5.

Lemma 5.2. *$q=p^m\equiv 9 \pmod{10}$ if and only if one of the following cases holds:*
(a) *$p\equiv 3 \pmod{10}$ and $m\equiv 2 \pmod{10}$.*
(b) *$p\equiv 7 \pmod{10}$ and $m\equiv 2 \pmod{10}$.*
(c) *$p\equiv 9 \pmod{10}$ and m is odd.*

Proof. The same proof given for Lemma 4.2. □

Theorem 5.3. *If p and m are as in Lemma 5.2, then the ideals of $R[X]/\langle\Phi_{10}(X)^{p^s}\rangle$ are of the form*

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

with $\mathscr{C}_1$ is an ideal of $R[X]/\langle(X^2+(\alpha+\alpha^{-1})X+1)^{p^s}\rangle$, and $\mathscr{C}_2$ is an ideal of $R[X]/\langle(X^2+(\alpha^2+(\alpha^2)^{-1})X+1)^{p^s}\rangle$, where α is a primitive root modulo 5.

Proof. By Lemma 5.1, $\Phi_{10}(X)=(X^2+(\alpha+\alpha^{-1})X+1)(X^2+(\alpha^2+(\alpha^2)^{-1})X+1)$. Then the Chinese remainder theorem proves that

$$R[X]/\langle\Phi_{10}(X)^{p^s}\rangle=R[X]/\langle(X^2+(\alpha+\alpha^{-1})X+1)^{p^s}\rangle\oplus R[X]/\langle(X^2+(\alpha^2+(\alpha^2)^{-1})X+1)^{p^s}\rangle.$$

This gives the result. □

It is enough now to show how the ideals of $R[X]/\langle(X^2+(\alpha+\alpha^{-1})X+1)^{p^s}\rangle$ and $R[X]/\langle(X^2+(\alpha^2+(\alpha^2)^{-1})X+1)^{p^s}\rangle$ are.

Theorem 5.4. *If p and m are as in Lemma 5.2, then the ideals of $R[X]/\langle(X^2+(\alpha+\alpha^{-1})X+1)^{p^s}\rangle$ are:*
(a) *Type 1: $\mathscr{C}_1$, trivial ideals:*

$$\langle 0\rangle \quad ; \quad \langle 1\rangle.$$

(b) *Type 2: $\mathscr{C}_2(\tau)$, principal ideals in $\langle u\rangle$:*

$$\langle u(x^2+(\alpha+\alpha^{-1})x+1)^{\tau}\rangle;\ \textit{where } 0\le\tau\le p^s-1.$$

(c) *Type 3: $\mathscr{C}_3(\delta,t,h(x))$, principal ideals which are not in $\langle u\rangle$:*

$$\langle(x^2+(\alpha+\alpha^{-1})x+1)^{\delta}+u(x^2+(\alpha+\alpha^{-1})x+1)^{t}h(x)\rangle;$$

where $\delta>t$, $h(x)$ is either 0 or a unit in $R[X]/\langle X^2+(\alpha+\alpha^{-1})X+1)^{p^s}\rangle$ of the form $\sum_{i=0}^{L-t-1}h_i(x^2+(\alpha+\alpha^{-1})x+1)^i$, where $deg(h_i)\le 1$, $h_0\neq 0$, and L is the smallest integer which satisfies $u(x^2+(\alpha+\alpha^{-1})x+1)^L\in\mathscr{C}_3(\delta,t,h(x))$.

(d) *Type 4: $\mathscr{C}_4(\delta, t, h(x), \omega)$, non principal ideals:*

$$\langle (x^2+(\alpha+\alpha^{-1})x+1)^{\delta}+u(x^2+(\alpha+\alpha^{-1})x+1)^t h(x), u(x^2+(\alpha+\alpha^{-1})x+1)^{\omega}\rangle,$$

where $p^s > \delta \geq L > \omega > t \geq 0$, $h(x)$ is either 0 or a unit in $R[X]/\langle (X^2+(\alpha+\alpha^{-1})X+1)^{p^s}\rangle$, where L is the smallest integer verifying $u(x^2+(\alpha+\alpha^{-1})x+1)^L \in \mathscr{C}_3(\delta, t, h(x))$.

Proof. The same method of the proof given for Theorem 5.4, it suffices to replace $\Phi_{10}(X)$ by $X^2+(\alpha+\alpha^{-1})X+1$. □

The parameter L is given by Proposition 3.6, and we can prove it using the same proof by replacing $\Phi_{10}(X)$ by $X^2+(\alpha+\alpha^{-1})X+1$.

Theorem 5.5. *Let us keeping the same notations as in Theorem 3.5. Then:*

$$\begin{cases} d_H(\mathscr{C}_2(\tau)) = d_H(\langle (x^2+(\alpha+\alpha^{-1})x+1)^{\tau}\rangle), \\ d_H(\mathscr{C}_3(\delta, t, h(x))) = d_H(\langle (x^2+(\alpha+\alpha^{-1})x+1)^{L}\rangle), \\ d_H(\mathscr{C}_4(\delta, t, h(x), \omega)) = d_H(\langle (x^2+(\alpha+\alpha^{-1})x+1)^{\omega}\rangle). \end{cases}$$

Proof. The same method of the proof given for Theorem 3.7, it suffices to replace $\Phi_{10}(x)$ by $x^2+(\alpha+\alpha^{-1})x+1$. □

Theorem 5.6. *If p and m are as in Lemma 5.2 then the ideals of $R[X]/\langle (X^2+(\alpha^2+(\alpha^2)^{-1})X+1)^{p^s}\rangle$ are:*

(a) *Type 1: $\mathscr{C}_1$, trivial ideals:*

$$\langle 0\rangle \quad ; \quad \langle 1\rangle.$$

(b) *Type 2: $\mathscr{C}_2(\tau)$, principal ideals in $\langle u\rangle$:*

$$\langle u(x^2+(\alpha^2+(\alpha^2)^{-1})x+1)^{\tau}\rangle; \text{ where } 0 \leq \tau \leq p^s-1.$$

(c) *Type 3: $\mathscr{C}_3(\delta, t, h(x))$, principal ideals which are not in $\langle u\rangle$:*

$$\langle (x^2+(\alpha^2+(\alpha^2)^{-1})x+1)^{\delta}+u(x^2+(\alpha^2+(\alpha^2)^{-1})x+1)^t h(x)\rangle;$$

where $\delta > t$, $h(x)$ is either 0 or a unit in $R[X]/\langle (X^2+(\alpha^2+(\alpha^2)^{-1})X+1)^{p^s}\rangle$ of the form $\sum\limits_{i=0}^{L-t-1} h_i(x^2+(\alpha^2+(\alpha^2)^{-1})x+1)^i$, where $deg(h_i) \leq 1$, $h_0 \neq 0$, and L is the smallest integer which satisfies $u(x^2+(\alpha^2+(\alpha^2)^{-1})x+1)^L \in \mathscr{C}_3(\delta, t, h(x))$.

(d) *Type 4: $\mathscr{C}_4(\delta, t, h(x), \omega)$, non principal ideals:*

$$\langle (x^2+(\alpha^2+(\alpha^2)^{-1})x+1)^{\delta}+u(x^2+(\alpha^2+(\alpha^2)^{-1})x+1)^t h(x), u(x^2+(\alpha^2+(\alpha^2)^{-1})x+1)^{\omega}\rangle,$$

where $p^s > \delta \geq L > \omega > t \geq 0$, $h(x)$ is either 0 or a unit in $R[X]/\langle (X^2+(\alpha^2+(\alpha^2)^{-1})X+1)^{p^s}\rangle$, where L is the smallest integer verifying $u(x^2+(\alpha^2+(\alpha^2)^{-1})x+1)^L \in \mathscr{C}_3(\delta, t, h(x))$.

Proof. The same method of the proof given for Theorem 3.5, it suffices to replace $\Phi_{10}(X)$ by $X^2+(\alpha^2+(\alpha^2)^{-1})X+1$. □

The parameter L is given by Proposition 3.6, and we can prove it using the same proof by replacing $\Phi_{10}(X)$ by $X^2+(\alpha^2+(\alpha^2)^{-1})X+1$.

Theorem 5.7. *Let us keeping the same notations as in Theorem 5.6. Then:*

$$\begin{cases} d_H(\mathscr{C}_2(\tau)) = d_H(\langle (x^2+(\alpha^2+(\alpha^2)^{-1})x+1)^{\tau}\rangle), \\ d_H(\mathscr{C}_3(\delta,t,h(x))) = d_H(\langle (x^2+(\alpha^2+(\alpha^2)^{-1})x+1)^{L}\rangle), \\ d_H(\mathscr{C}_4(\delta,t,h(x),\omega)) = d_H(\langle (x^2+(\alpha^2+(\alpha^2)^{-1})x+1)^{\omega}\rangle). \end{cases}$$

Proof. The same method of the proof given for Theorem 3.7, it suffices to replace $\Phi_{10}(x)$ by $x^2+(\alpha^2+(\alpha^2)^{-1})x+1$. □

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] A. Arnold and M. Monagan. Calculating cyclotomic polynomials. *Mathematics of Computation*, 80(276):2359–2379, 2011. https://doi.org/10.1090/S0025-5718-2011-02467-1.

[2] J. L. B. Boudine and M. E. Charkani. The cyclic codes of length $5p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ and their dual codes. *Mathematical Communications*, 27(1):127–135, 2022. https://hrcak.srce.hr/275700.

[3] J. L. B. Boudine and M. E. Charkani. Complete classification of cyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$. *Discrete Mathematics, Algorithms and Applications*, 15(03):2250091, 2023. http://dx.doi.org/10.1142/S1793830922500914.

[4] J. L. B. Boudine and M. E. Charkani. Complete classification of negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$. *Asian-European Journal of Mathematics*, 16(01):2350011, 2023. https://doi.org/10.1142/S1793557123500110.

[5] H. Q. D. B. Chen and H. Liu. Repeated-root constacyclic codes of length lp^s and their duals. *Discrete Applied Mathematics*, 177:60–70, 2014. https://doi.org/10.1016/j.dam.2014.05.046.

[6] W. C. Brown. *Matrices over commutative Rings*. Monographs, Textbooks in Pure, and Applied Mathematics 169, 1993, pages 175–179.

[7] Y. Cao. Generalized quasi-cyclic codes over galois rings: structural properties and enumeration. *Applicable Algebra in Engineering, Communication and Computing*, 22(3):219–233, 2011. https://doi.org/10.1007/s00200-011-0145-5.

[8] M. E. Charkani and B. Boudine. On the integral ideals of $R[X]$ when R is a special principal ideal ring. *Sao Paulo Journal of Mathematical Sciences*, 14(2):698–702, 2020. http://dx.doi.org/10.1007/s40863-020-00177-1.

[9] H. Q. Dinh. Constacyclic codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$. *Journal of Algebra*, 324:940–950, 2010. https://doi.org/10.1016/j.jalgebra.2010.05.027.

[10] H. Q. Dinh. Repeated-root constacyclic codes of length $2p^s$. *Finite Fields and Their Applications*, 18(1):133–143, 2012. https://doi.org/10.1016/j.ffa.2011.07.003.

[11] H. Q. Dinh. On repeated-root constacyclic codes of length $4p^s$. *Asian-European Journal of Mathematics*, 6(02):1350020, 2013. https://doi.org/10.1142/S1793557113500204.

[12] H. Q. Dinh. Structure of repeated-root constacyclic codes of length $3p^s$ and their duals. *Discrete Mathematics*, 313(9):983–991, 2013. https://doi.org/10.1016/j.disc.2013.01.024.

[13] H. Q. Dinh and S. R. Lòpez-Permouth. Cyclic and negacyclic codes over finite chain rings. *IEEE Transactions on Information Theory*, 50:1728–1744, 2004. https://doi.org/10.1109/TIT.2004.831789.

[14] A. K. Ghose and P. P. Dey. An investigation of [5,3] error correcting codes over gf(5). *Journal of Information and Optimization Sciences*, 39(3):695–703, 2018. https://doi.org/10.1080/02522667.2017.1400744.

[15] A. K. S. H. Q. Dinh B. T. Nguyen and S. Sriboonchitta. Hamming and symbol-pair distances of repeated root constacyclic codes of prime power lengths over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *IEEE Communications Letters*, 22(12):2400–2403, 2018. https://doi.org/10.1109/LCOMM.2018.2868637.

[16] M. E. C. H. Q. Dinh J. Laaouine and W. Chinnakum. Hamming distance of constacyclic codes of length p^s over $\mathbb{F}_{p^s} + u\mathbb{F}_{p^s} + u^2\mathbb{F}_{p^s}$. *IEEE Access*, 9:141064–141078, 2021. https://doi.org/10.1109/ACCESS.2021.3117658.

[17] M. E. C. J. Laaouine and L. Wang. Complete classification of repeated-root σ-constacyclic codes of prime power length over $\mathbb{F}_{p^m}[u]/{<}u^3{>}$. *Discrete Mathematics*, 344:112325, 2021. https://doi.org/10.1016/j.disc.2021.112325.

[18] J. Laaouine and M. E. Charkani. A note on ”h. q. dinh et al., hamming distance of repeated-root constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$”. *Applicable Algebra in Engineering, Communication and Computing*, 34:157–163, 2021. https://doi.org/10.1007/s00200-021-00492-w.

[19] X. Liu and X. Xu. Cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *Acta Mathematica Scientia*, 34:829–839, 2014.

[20] J. Neukirch. *Algebraic Number Theory*. Springer Science & Business Media 322, 2013.

[21] J. Phuto and 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 Mathematics, Algorithms and Applications*, 12(05):2050063, 2020. https://doi.org/10.1142/S1793830920500639.

[22] L. Wang and Q. Wang. On explicit factors of cyclotomic polynomials over finite fields. *Designs, Codes and Cryptography*, 63(1):87–104, 2012. https://doi.org/10.1007/s10623-011-9537-6.

[23] H. Wu, L. Zhu, R. Feng, and S. Yang. Explicit factorizations of cyclotomic polynomials over finite fields. *Designs, Codes and Cryptography*, 83(1):197–217, 2016. https://doi.org/10.1007/s10623-016-0224-5.