Palestine Journal of Mathematics

Vol 14(1)(2025) , 569–577

Type-1 constacyclic codes of length $7p^s$ over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^e\rangle}$

Youssef Ahendouz and Ismail Akharraz

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 11T71; Secondary 11Txx.

Keywords and phrases: Constacyclic codes, Chain ring, Dual codes.

The authors express their gratitude to the reviewers and the editor for their insightful comments and valuable suggestions, which have significantly improved the quality of our paper.

Corresponding Author: Y. Ahendouz

Abstract Let p be a prime and m, e be positive integers such that $e \geq 2$. Consider the ring $R_e = \frac{\mathbb{F}_{p^m}[u]}{\langle u^e\rangle}$ and a unit $\lambda = \lambda_0 + \gamma u$, where $\lambda_0 \in \mathbb{F}_{p^m}^*$ and $\gamma \in R_e^*$. This paper provides a classification of λ-constacyclic codes of length ηp^s over R_e by determining their generator polynomials, enumeration, and dual codes. Here s, η are positive integers such that $\gcd(p, \eta) = 1$. In particular, for $p \neq 7$, we establish a complete classification of λ-constacyclic codes of length $7p^s$ over R_e by determining the factorization of $x^7 - \xi$ over $\mathbb{F}_{p^m}$, where $\xi^{p^s} = \lambda_0$.

1 Introduction

Constacyclic codes play a crucial role in the field of error-correcting codes due to their efficient encoding via simple shift registers and their rich algebraic structures, which enable effective error detection and correction. These properties make them particularly valuable in engineering applications. In particular, constacyclic codes defined over specific classes of finite rings have emerged as a compelling research topic in algebraic coding theory [3, 4, 5, 6, 14, 15, 16].

Let R be a finite commutative ring with identity $1 \neq 0$, and let $R^\times$ denote its group of units. A code of length n over R is a nonempty subset $C \subseteq R^n$, where each element $\mathbf{c}$ in C is called a codeword. A code C is said to be linear if it forms an R-submodule of R^n. Given a unit $\lambda \in R^\times$, a linear code C of length n over R is called a λ-constacyclic code if it satisfies the shift property: for every codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$, the vector $(\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ also belongs to C. Each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ can be naturally associated with the polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in R[x]$. It is well known that a linear code C of length n over R is λ-constacyclic if and only if it is an ideal of the quotient ring $\frac{R[x]}{\langle x^n - \lambda\rangle}$.

The class of finite rings of the form $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$ has been extensively utilized as an alphabet for constacyclic codes. Notably, the ring $\frac{\mathbb{F}_2[u]}{\langle u^2\rangle}$ exhibits intriguing structural properties: it is additively isomorphic to $\mathbb{F}_4$ and multiplicatively analogous to $\mathbb{Z}_4$. Due to these characteristics, codes over $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle}$ have attracted significant attention in coding theory (see, for example, [3, 4, 5, 6]). More generally, the family of rings $\frac{\mathbb{F}_{p^m}[u]}{\langle u^e\rangle} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m}$ has also been widely studied in coding theory as an alphabet for error-correcting codes. Several investigations have focused on constacyclic codes over these structures, highlighting their algebraic properties and applications (see, for example, [7, 8, 9, 2]).

Throughout this paper, we use the notation R_e to denote the finite commutative ring

$$R_e = \frac{\mathbb{F}_{p^m}[u]}{\langle u^e\rangle} = \left\{ \sum_{i=0}^{e-1} a_i u^i \mid a_i \in \mathbb{F}_{p^m} \right\}.$$

This ring consists of polynomials over $\mathbb{F}_{p^m}$ in the indeterminate u, with degree strictly less than e, where arithmetic operations are performed modulo u^e.

The set of all units in R_e consists of elements of the form $\lambda = \lambda_0 + u\lambda_1 + \cdots + u^{e-1}\lambda_{e-1}$, where $\lambda_0, \lambda_1, \ldots, \lambda_{e-1} \in \mathbb{F}_{p^m}$ and $\lambda_0 \neq 0$. In this paper, we consider only units of Type-1, which means that $\lambda_1 \neq 0$. Equivalently, we define

$$\gamma = \lambda_1 + \lambda_2 u + \cdots + \lambda_{e-1}u^{e-2},$$

which is also a unit in R_e.

Let s be a positive integer. Using the division algorithm, we write $s = q_s m + r_s$, with $0 \leq r_s < m$. Since $\lambda_0^{p^m} = \lambda_0$, we define $\xi = \lambda_0^{p^{m-r_s}} = \lambda_0^{p^{(q_s+1)m-s}}$. It follows that $\xi^{p^s} = \lambda_0$.

Throughout this paper, η denotes a positive integer with $\gcd(\eta, p) = 1$. We define the quotient ring as

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

Thus, the λ-constacyclic codes of length ηp^s over R_e are precisely the ideals of $\mathcal{R}_\lambda$.

The remainder of this paper is structured as follows. In Section 2, we classify λ-constacyclic codes of length ηp^s over R_e, where s and η are positive integers such that $\gcd(p, \eta) = 1$. We determine their generator polynomials, enumerate the number of distinct codes, and describe their duals. In Section 3, we focus on the special case where $\eta = 7$ and establish a complete classification of λ-constacyclic codes of length $7p^s$ over R_e. We analyze the factorization of $x^7 - \xi$ over $\mathbb{F}_{p^m}$ and distinguish two cases: when $p^m \equiv 1 \pmod 7$ (Subsection 3.1) and when $p^m \not\equiv 1 \pmod 7$ (Subsection 3.2).

2 λ-constacyclic codes of length ηp^s over R_e

In this section, we study λ-constacyclic codes of length ηp^s over R_e. We recall that a finite commutative ring is said to be a chain ring if its ideals are totally ordered by inclusion.

The following result is a well-known property of finite commutative chain rings (see [11]).

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

(i) R is a local ring whose maximal ideal M is principal, i.e., $M = \langle \Gamma \rangle$ for some element $\Gamma \in R$.

(ii) R is a local principal ideal ring.

(iii) R is a chain ring whose ideals are $\langle \Gamma^i \rangle$ for $0 \leq i \leq r$, where r is the nilpotency index of Γ.

Moreover, for each $0 \leq i \leq r$, the cardinality of the ideal $\langle \Gamma^i \rangle$ is given by

$$\left|\langle \Gamma^i \rangle\right| = \left|\frac{R}{M}\right|^{r-i}.$$

Clearly, R_e is a finite commutative chain ring with maximal ideal $\langle u \rangle$, nilpotency index e, and residue field $\frac{R_e}{\langle u \rangle} = \mathbb{F}_{p^m}$.

We define the natural projection

$$R_e[x] \to \mathbb{F}_{p^m}[x], \quad f(x) \mapsto \bar{f}(x),$$

where $\bar{f}(x)$ is obtained by reducing all coefficients of $f(x)$ modulo $\langle u \rangle$.

Two polynomials $f_1(x), f_2(x) \in R_e[x]$ are called coprime if

$$\langle f_1(x) \rangle + \langle f_2(x) \rangle = R_e[x],$$

or equivalently, if there exist polynomials $g_1(x), g_2(x) \in R_e[x]$ such that

$$f_1(x)g_1(x) + f_2(x)g_2(x) = 1.$$

The coprimeness of two polynomials in $\mathbb{F}_{p^m}[x]$ is defined similarly.

Now, since η and p are coprime, the polynomial $x^\eta - \xi$ has no repeated factors. Let

$$x^\eta - \xi = f_1(x)f_2(x)\cdots f_t(x)$$

be its factorization into pairwise distinct monic irreducible polynomials in $\mathbb{F}_{p^m}[x]$. Raising both sides to the power p^s gives

$$x^{\eta p^s} - \lambda_0 = f_1(x)^{p^s} f_2(x)^{p^s} \cdots f_t(x)^{p^s}.$$

By Hensel's lemma [10, Theorem XIII.4], there exist pairwise coprime monic polynomials

$$\psi_1(x), \psi_2(x), \ldots, \psi_t(x) \in R_e[x]$$

such that

$$x^{\eta p^s} - \lambda = \psi_1(x)\psi_2(x)\cdots\psi_t(x), \tag{2.1}$$

with

$$\overline{\psi_i}(x) = f_i(x)^{p^s}, \quad \text{for all } i = 1, \ldots, t.$$

For each i, we define:

- $\mathcal{R}_i = \frac{R_e[x]}{\langle \psi_i(x)\rangle}$,
- $\phi_i(x) = \frac{\psi_1(x)\cdots\psi_t(x)}{\psi_i(x)}$,
- $g_i(x) = \frac{f_1(x)\cdots f_t(x)}{f_i(x)}$.

Since $\phi_i(x)$ and $\psi_i(x)$ are coprime in $R_e[x]$, there exist polynomials $s_i(x), r_i(x) \in R_e[x]$ such that

$$s_i(x)\phi_i(x) + r_i(x)\psi_i(x) = 1. \tag{2.2}$$

Define $\varepsilon_i(x) = s_i(x)\phi_i(x)$.

Lemma 2.2. *In the ring $\mathcal{R}_\lambda$, the polynomials $\varepsilon_i(x)$ satisfy the following:*

(i) $\sum_{k=1}^{t} \varepsilon_k(x) = 1$;

(ii) for all $1 \le i \ne j \le t$, $\varepsilon_i(x)\varepsilon_j(x) = 0$;

(iii) for all $1 \le i \le t$, $\varepsilon_i(x)\varepsilon_i(x) = \varepsilon_i(x)$.

Proof. (i) For each $i = 1, \ldots, t$, we have

$$\sum_{k=1}^{t} \varepsilon_k(x) - 1 \equiv \varepsilon_i(x) - 1 \pmod{\psi_i(x)} \equiv r_i(x)\psi_i(x) \pmod{\psi_i(x)} \equiv 0 \pmod{\psi_i(x)}.$$

Since $\psi_1(x), \ldots, \psi_t(x)$ are pairwise coprime, it follows that

$$\sum_{k=1}^{t} \varepsilon_k(x) = 1 \quad \text{in } \mathcal{R}_\lambda.$$

(ii) If $i \ne j$, then $\varepsilon_i(x)\varepsilon_j(x)$ is divisible by $x^{\eta p^s} - \xi$, implying that in $\mathcal{R}_\lambda$,

$$\varepsilon_i(x)\varepsilon_j(x) = 0.$$

(iii) By (i) and (ii),

$$\varepsilon_i(x) = \varepsilon_i(x)\sum_{k=1}^{t} \varepsilon_k(x) = \varepsilon_i^2(x).$$

□

Theorem 2.3. *(i)* $\mathcal{R}_\lambda = \varepsilon_1(x)\mathcal{R}_\lambda \oplus \ldots \oplus \varepsilon_t(x)\mathcal{R}_\lambda$;

(ii) for all $i = 1, \ldots, t$, *the map* $\pi_i : \begin{array}{ccc} \mathcal{R}_i & \longrightarrow & \varepsilon_i(x)\mathcal{R}_\lambda \\ c(x) & \longmapsto & \varepsilon_i(x)c(x) \end{array}$ *is a ring isomorphism.*

Proof. (i) According to the previous lemma, for any $c(x) \in \mathcal{R}_\lambda$,

$$c(x) = c(x)\sum_{i=1}^{t}\varepsilon_i(x) = \sum_{i=1}^{t}\varepsilon_i(x)c(x) \subseteq \varepsilon_1(x)\mathcal{R}_\lambda + \ldots + \varepsilon_t(x)\mathcal{R}_\lambda.$$

Then $\mathcal{R}_\lambda = \varepsilon_1(x)\mathcal{R}_\lambda + \ldots + \varepsilon_t(x)\mathcal{R}_\lambda$. On the other hand, if $\sum_{i=1}^{t}\varepsilon_i(x)c_i(x) = 0$, then for all $j = 1, \ldots, t, \varepsilon_j(x)\sum_{i=1}^{t}\varepsilon_i(x)c_i(x) = 0$, using previous lemma again $\varepsilon_j(x)c_j(x) = 0$. So we have $\mathcal{R}_\lambda = \varepsilon_1(x)\mathcal{R}_\lambda \oplus \ldots \oplus \varepsilon_t(x)\mathcal{R}_\lambda$.

(ii) Let $i = 1, \ldots, t$, if $\varepsilon_i(x)c(x) = 0$ in $\varepsilon_i(x)\mathcal{R}_\lambda$, then there exists $b(x) \in R_e[x]$ such that $\varepsilon_i(x)c(x) = b(x)\left(x^{\eta p^s} - \xi\right)$, i.e.,

$$\left(1 - r_i(x)\psi_i(x)\right)c(x) = b(x)\left(x^{\eta p^s} - \xi\right), \text{ in } R_e[x].$$

Then $c(x) = 0$ in $\mathcal{R}_i$. So we have shown that π_i is an injection. The surjection is obvious. □

We can therefore conclude the following theorem.

Theorem 2.4. *Let C be a subset of $\mathcal{R}_\lambda$. Then C is an λ-constacyclic code of length ηp^s over R_e if and only if for each integer $i, 1 \leq i \leq t$, there is a unique ideal C_i of $\mathcal{R}_i$ such that $C = \bigoplus_{i=1}^{t}\varepsilon_i(x)C_i$.*

Lemma 2.5. *The polynomial $g_i(x)$ is a unit in $\mathcal{R}_i$.*

Proof. To prove this, we show that $g_i(x)^{p^s}$ and $\psi_i(x)$ are coprime in $R_e[x]$.

Since $g_i(x)^{p^s}$ and $f_i(x)$ are coprime in $\mathbb{F}_{p^m}[x]$, there exist polynomials $a_i(x), b_i(x) \in \mathbb{F}_{p^m}[x]$ such that

$$a_i(x)f_i(x) + b_i(x)g_i(x)^{p^s} = 1.$$

Using $\overline{\psi_i}(x) = f_i(x)^{p^s}$, we express $\psi_i(x)$ in $R_e[x]$ as

$$\psi_i(x) = f_i(x)^{p^s} + uc_i(x),$$

for some $c_i(x) \in R_e[x]$. Substituting this into the previous equation yields

$$a_i(x)\psi_i(x) + b_i(x)g_i(x)^{p^s} = 1 + ua_i(x)c_i(x).$$

Since u is nilpotent in $R_e[x]$, the term $1 + ua_i(x)c_i(x)$ is a unit in $R_e[x]$. Therefore, $\psi_i(x)$ and $g_i(x)^{p^s}$ are coprime in $R_e[x]$, proving that $g_i(x)^{p^s}$ is a unit in $\mathcal{R}_i$. □

Theorem 2.6. *In $\mathcal{R}_i$, the following properties hold:*

(i) $\langle f_i(x)^{p^s}\rangle = \langle u\rangle$, and thus $f_i(x)$ is nilpotent with nilpotency index ep^s.

(ii) The ring $\mathcal{R}_i$ is a chain ring with the following ideal chain:

$$\mathcal{R}_i = \langle 1\rangle \supsetneq \langle f_i(x)\rangle \supsetneq \cdots \supsetneq \langle f_i(x)^{kp^s-1}\rangle \supsetneq \langle f_i(x)^{ep^s}\rangle = \langle 0\rangle. \tag{2.3}$$

(iii) Each ideal $\langle f_i(x)^j\rangle$ contains $p^{\deg f_i m(ep^s-j)}$ elements for all $0 \leq j \leq ep^s$.

Proof. (i) Since $\psi_i(x)$ divides $x^{\eta p^s} - \lambda$ in $R_e[x]$, it follows that in $\mathcal{R}_i$, we have $x^{\eta p^s} - \lambda = 0$. Moreover, using $x^{\eta p^s} - \lambda = (x^\eta - \xi)^{p^s} - u\gamma$, we obtain

$$\gamma u = (x^\eta - \xi)^{p^s} = f_i(x)^{p^s}g_i(x)^{p^s}.$$

By Lemma 2.5, $g_i(x)^{p^s}$ is a unit in $\mathcal{R}_i$, and since γ is also a unit, it follows that

$$\langle f_i(x)^{p^s}\rangle = \langle u\rangle.$$

Consequently, as u has nilpotency index e, we conclude that $f_i(x)$ has nilpotency index ep^s.

(ii) Let I be a nontrivial ideal of $\mathcal{R}_i$ and denote by I_u its reduction modulo u. Since I_u is an ideal of $\frac{\mathbb{F}_{p^m}[x]}{\langle f_i(x)^{p^s}\rangle}$, it takes the form

$$I_u = \langle f_i(x)^j\rangle, \quad 1 \le j \le p^s.$$

Every $c(x) \in I$ can be written as

$$c(x) = g(x)f_i(x)^j + uh(x),$$

for some $g(x), h(x) \in \mathcal{R}_i$. By part (1), since $u \in \langle f_i(x)^{p^s}\rangle$, we deduce that $I \subseteq \langle f_i(x)\rangle$. Hence, $\mathcal{R}_i$ is a local ring with a principal maximal ideal $\langle f_i(x)\rangle$. By part (1), $f_i(x)$ is nilpotent with nilpotency index ep^s. By Proposition 2.1, $\mathcal{R}_i$ is a chain ring with ideals given by (2.3).

(iii) By Proposition 2.1, the number of elements in $\langle f_i(x)^j\rangle$ is given by

$$\left|\langle f_i(x)^j\rangle\right| = \left|\frac{\mathcal{R}_i}{\langle f_i(x)\rangle}\right|^{ep^s-j}.$$

Since $\frac{\mathcal{R}_i}{\langle f_i(x)\rangle} \cong \mathbb{F}_{p^{m\deg f_i}}$ has $p^{m\deg f_i}$ elements, it follows that

$$\left|\langle f_i(x)^j\rangle\right| = p^{\deg f_i m(ep^s-j)}.$$

□

According to Theorem 2.4 and Theorem 2.6, we establish the following result:

Theorem 2.7. *Every λ-constacyclic code of length ηp^s over R_e has the form*

$$C = \bigoplus_{i=1}^{t} \varepsilon_i(x)\langle f_i(x)^{z_i}\rangle,$$

where $0 \le z_i \le ep^s$.

The number of codewords in C is given by

$$p^{\sum_{i=1}^{t} \deg f_i m(ep^s-z_i)}.$$

Furthermore, the total number of λ-constacyclic codes of length ηp^s over R_e is

$$(ep^s+1)^t.$$

Alternatively, the structure of λ-constacyclic codes can be described in terms of their generator polynomials.

Theorem 2.8. *The λ-constacyclic codes of length ηp^s over R_e are given by*

$$C_{z_1,\ldots,z_t} = \left\langle \prod_{i=1}^{t} f_i(x)^{z_i} \right\rangle.$$

Moreover, the number of codewords in $C_{z_1,\ldots,z_t}$ is

$$|C_{z_1,\ldots,z_t}| = p^{\sum_{i=1}^{t} m\deg f_i(ep^s-z_i)},$$

where for all $1 \le i \le t$, we have $0 \le z_i \le ep^s$.

Proof. It suffices to show that $\bigoplus_{i=1}^{t} \varepsilon_i(x)\langle f_i(x)^{z_i}\rangle = \left\langle \prod_{i=1}^{t} f_i(x)^{z_i} \right\rangle$.

Let $C = \bigoplus_{i=1}^{t} \varepsilon_i(x) \langle f_i(x)^{z_i} \rangle$ and $D = \left\langle \prod_{i=1}^{t} f_i(x)^{z_i} \right\rangle$. By using same proof of Lemma 2.5 for all $i, j = 1, \ldots, t$ and $i \neq j$, $f_j(x)$ is a unit in $\mathcal{R}_i$, we have:

$$\forall i = 1, \ldots, t, \left\langle \prod_{i=1}^{t} f_i(x)^{z_i} \right\rangle = \langle f_i(x)^{z_i} \rangle \text{ in } \mathcal{R}_i.$$

Since $\sum_{i=1}^{t} \varepsilon_i(x) = 1$, we can conclude that

$$C = \bigoplus_{i=1}^{t} \varepsilon_i(x) \langle f_i(x)^{z_i} \rangle = \bigoplus_{i=1}^{t} \varepsilon_i(x) \left\langle \prod_{i=1}^{t} f_i(x)^{z_i} \right\rangle = \left\langle \prod_{i=1}^{t} f_i(x)^{z_i} \right\rangle = D.$$

□

The dual of an ideal C in $\frac{R_e[x]}{\langle x^{\eta p^s} - \lambda \rangle}$, denoted by $C^{\perp}$, is defined as

$$C^{\perp} = \left\{ a(x) = \sum_{i=0}^{\eta p^s - 1} a_i x^i \;\middle|\; \sum_{i=0}^{\eta p^s - 1} a_i \cdot b_i = 0, \text{ for any } b(x) = \sum_{i=0}^{\eta p^s - 1} b_i x^i \in C \right\}.$$

Proposition 2.9. *[11] If C is a λ-constacyclic code of length ηp^s over R_e, then*

$$|C| \cdot |C^{\perp}| = |\mathcal{R}_{\lambda}|.$$

The reciprocal polynomial of a polynomial $a(x) \in R_e[x]$ of degree r, denoted by $a^*(x)$, is defined as

$$a^*(x) = x^r a(x^{-1}).$$

The annihilator of an ideal C in $\mathcal{R}_{\lambda}$, denoted by $\mathcal{A}(C)$, is given by

$$\mathcal{A}(C) = \{a(x) \mid a(x)b(x) = 0 \text{ for any } b(x) \in C\}.$$

Proposition 2.10. *[12] If C is a λ-constacyclic code of length ηp^s over R_e, then its dual is a λ^{-1}-constacyclic code of length ηp^s over R_e, i.e., an ideal of $\frac{R[x]}{\langle x^{\eta p^s} - \lambda^{-1} \rangle}$. Moreover,*

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

Theorem 2.11. *Let $C_{z_1,\ldots,z_t} = \left\langle \prod_{i=1}^{t} f_i(x)^{z_i} \right\rangle$ be a λ-constacyclic code of length ηp^s over R_e. Then*

$$C^{\perp}_{z_1,\ldots,z_t} = \left\langle \prod_{i=1}^{t} f_i^*(x)^{ep^s - z_i} \right\rangle.$$

Proof. It is clear that in $\mathcal{R}_{\lambda}$,

$$\prod_{i=1}^{t} f_i(x)^{ep^s - z_i} \cdot \prod_{i=1}^{t} f_i(x)^{z_i} = 0.$$

Therefore,

$$D := \left\langle \prod_{i=1}^{t} f_i(x)^{ep^s - z_i} \right\rangle \subseteq \mathcal{A}\left(C_{z_1,\ldots,z_t}\right).$$

By Proposition 2.10,

$$D^* = \left\langle \prod_{i=1}^{t} f_i^*(x)^{ep^s - z_i} \right\rangle \subseteq C^{\perp}_{z_1,\ldots,z_t}.$$

On the other hand, by Theorem 2.8 and Proposition 2.9,

$$\begin{aligned}|\mathcal{R}_\lambda| &= |C| \cdot |C^{\perp}_{z_1,\ldots,z_t}| \\ &\geq |C| \cdot |D^*| \\ &= |C| \cdot |D| \\ &= p^{\sum_{i=1}^{t} m \deg f_i(ep^s - z_i)} \cdot p^{\sum_{i=1}^{t} m \deg f_i(ep^s - (ep^s - z_i))} \\ &= |\mathcal{R}_\lambda|.\end{aligned}$$

Thus,

$$C^{\perp}_{z_1,\ldots,z_t} = \left\langle \prod_{i=1}^{t} f_i^*(x)^{ep^s - z_i} \right\rangle.$$

□

3 Type-1 λ-constacyclic codes of length $7p^s$ over R_e

In this section, we classify all λ-constacyclic codes of length $7p^s$ over R_e in terms of their generator polynomials and determine their duals. The structure of C is determined by the factorization of $x^7 - \xi$ over $\mathbb{F}_{p^m}$.

Let ξ be a primitive $(p^m - 1)$th root of unity, so that

$$\mathbb{F}^*_{p^m} = \left\{1, \xi, \xi^2, \ldots, \xi^{p^m-2}, \xi^{p^m-1}\right\}.$$

Consider $\xi = \xi^{\varpi} \in \mathbb{F}^*_{p^m}$. The order of ξ in the multiplicative group $\mathbb{F}^*_{p^m}$ is given by

$$\frac{p^m - 1}{\gcd(\varpi, p^m - 1)}.$$

We consider two cases: $p^m \equiv 1 \pmod 7$ and $p^m \not\equiv 1 \pmod 7$.

3.1 Case when $p^m \equiv 1 \pmod 7$

We begin with the following lemma:

Lemma 3.1. *[13, Theorem 3.75] Assume that $n \geq 2$. For any $a \in \mathbb{F}_q^*$ with $\mathrm{ord}(a) = k$, the binomial $x^n - a$ is irreducible over $\mathbb{F}_q$ if and only if both of the following two conditions are satisfied:*

- *Every prime divisor of n divides k, but does not divide $(q-1)/k$;*
- *If $4 \mid n$, then $4 \mid (q-1)$.*

Then in the case $p^m \equiv 1 \pmod 7$, the polynomial $x^7 - \xi$ is irreducible over the finite field $\mathbb{F}_{p^m}$ if and only if 7 divides $\frac{p^m-1}{\gcd(\varpi, p^m-1)}$ but does not divide ϖ, it follows that $x^7 - \xi$ is irreducible over $\mathbb{F}_{p^m}$ if and only if 7 does not divide ϖ.

In the case where 7 divides ϖ, for any $0 \leq i \leq 6$, the element $\xi^{\frac{\varpi}{7}} \xi^{i\frac{p^m-1}{7}}$ is a root of $x^7 - \xi$, and these roots are pairwise distinct. Consequently, the polynomial $x^7 - \xi$ admits the following factorization:

$$x^7 - \xi = \prod_{i=0}^{6} \left(x - \xi^{\frac{\varpi}{7}} \xi^{i\frac{p^m-1}{7}}\right).$$

We now list all the λ-constacyclic codes of length $7p^s$ over R_e and their duals in the case where $p^m \equiv 1 \pmod 7$ in Table 1, where $0 \leq z, z_i \leq ep^s$.

Case	λ-constacyclic codes C	$C^{\perp}$
7 does not divide ϖ	$\langle (x^7-\xi)^z \rangle$	$\langle (\xi x^7-1)^{p^m e-z} \rangle$
7 divides ϖ	$\left\langle \prod_{i=0}^{6} \left(x-\xi^{\frac{\varpi}{7}}\xi^{i\frac{p^m-1}{7}}\right)^{z_i} \right\rangle$	$\left\langle \prod_{i=0}^{6} \left(\xi^{\frac{\varpi}{7}}\xi^{i\frac{p^m-1}{7}}x-1\right)^{p^m e-z_i} \right\rangle$

Table 1. The λ-constacyclic codes of length $7p^s$ over R_e and their duals in case $p^m \equiv 1 \pmod 7$.

3.2 Case when $p^m \not\equiv 1 \pmod 7$

In this case, 7 and p^m-1 are coprime. Therefore, there exist two positive integers r and t such that

$$7r + (p^m-1)t = 1.$$

Consequently,

$$7r\varpi + (p^m-1)t\varpi = \varpi.$$

Let us define $\delta = \xi^{r\varpi}$ and set $y = \frac{1}{\delta}x$. Then, we have

$$\delta^7 = \xi \quad \text{and} \quad x^7 - \xi = \delta^7(y^7-1).$$

Let θ be a primitive 7th root of unity in an extension field of $\mathbb{F}_{p^m}$. For each $k = 0, 1, \ldots, 6$, the minimal polynomial of θ^k over $\mathbb{F}_{p^m}$ is given by

$$\mathcal{M}_k(x) = \prod_{i \in \mathscr{C}_k} (x-\theta^i),$$

where $\mathscr{C}_k$ denotes the cyclotomic coset of k modulo 7 over $\mathbb{F}_{p^m}$, defined as:

$$\mathscr{C}_k = \left\{ k \cdot (p^m)^\ell \bmod 7 \mid \ell = 0, 1, \ldots \right\}.$$

The irreducible decomposition of y^7-1 in $\mathbb{F}_{p^m}[x]$ is given by the following expression (see [17, Theorem 4.1.1]):

$$y^7 - 1 = \prod_{i \in \mathcal{T}} \mathcal{M}_i(x),$$

where $\mathcal{T}$ is the set of representatives of the cyclotomic cosets modulo 7.
We obtain the factorization of $x^7-\xi$ into irreducible factors over $\mathbb{F}_{p^m}$ as follows:

$$x^7 - \xi = \begin{cases} (x-\delta)f_1(x)f_2(x)f_3(x), & \text{if } p^m \equiv 6 \bmod 7, \\ (x-\delta)f_4(x)f_5(x), & \text{if } p^m \equiv 2 \text{ or } 4 \bmod 7, \\ (x-\delta)f_6(x), & \text{if } p^m \equiv 3 \text{ or } 5 \bmod 7. \end{cases}$$

Where

$$\begin{aligned} f_1(x) &= x^2 - a\delta x + \delta^2, \\ f_2(x) &= x^2 - (a^2-2)\delta x + \delta^2, \\ f_3(x) &= x^2 - (a^3-3a)\delta x + \delta^2, \\ f_4(x) &= x^3 - b\delta x^2 - (1+b)\delta^2 x - \delta^3, \\ f_5(x) &= x^3 + (1+b)\delta x^2 + b\delta^2 x - \delta^3, \\ f_6(x) &= x^6 + \delta x^5 + \delta^2 x^4 + \delta^3 x^3 + \delta^4 x^2 + \delta^5 x + \delta^6, \end{aligned}$$

where $a = \theta + \theta^6$ and $b = \theta + \theta^2 + \theta^4$.

We then present all the λ-constacyclic codes of length $7p^s$ over R_e and their duals in case $p^m \equiv 1 \pmod 7$ in Table 2, where $0 \le z_i \le ep^s$.

Case	C	$C^{\perp}$
$p^m \equiv 6 \bmod 7$	$\langle (x-\delta)^{z_0} f_1(x)^{z_1} f_2(x)^{z_2} f_3(x)^{z_3}\rangle$	$\langle (\delta x-1)^{p^m e-z_0} f_1^*(x)^{p^m e-z_1} f_2^*(x)^{p^m e-z_2} f_3^*(x)^{p^m e-z_3}\rangle$
$p^m \equiv 2$ or $4 \bmod 7$	$\langle (x-\delta)^{z_0} f_4(x)^{z_1} f_5(x)^{z_2}\rangle$	$\langle (\delta x-1)^{p^m e-z_0} f_4^*(x)^{p^m e-z_1} f_5^*(x)^{p^m e-z_2}\rangle$
$p^m \equiv 3$ or $5 \bmod 7$	$\langle (x-\delta)^{z_0} f_6(x)^{z_1}\rangle$	$\langle (\delta x-1)^{p^m e-z_0} f_6^*(x)^{p^m e-z_1}\rangle$

Table 2. The λ-constacyclic codes of length $7p^s$ over R_e and their duals in case $p^m \not\equiv 1 \pmod 7$.

References

[1] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Transactions on Information Theory, vol. 40, no. 2, pp. 301–319, 1994.

[2] H. Q. Dinh, B. T. Nguyen, and S. Sriboonchitta, *RT distance and weight distributions of Type* 1 *constacyclic codes of length* $4p^s$ *over* $\mathbb{F}_{p^m}[u]/\langle u^a\rangle$, Turkish Journal of Mathematics, vol. 43, no. 2, pp. 561–578, 2019.

[3] H. Q. Dinh, *Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, Journal of Algebra, vol. 324, no. 5, pp. 940–950, 2010.

[4] 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 and Their Applications, vol. 37, pp. 108–130, 2016.

[5] H. Q. Dinh, *Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$*, IEEE Transactions on Information Theory, vol. 55, no. 4, pp. 1730–1740, 2009.

[6] W. Zhao, X. Tang, and Z. Gu, *All $\alpha + u\beta$-constacyclic codes of length ηp^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, Finite Fields and Their Applications, vol. 50, pp. 1–16, 2018.

[7] H. Q. Dinh, S. Dhompongsa, and S. Sriboonchitta, *Repeated-root constacyclic codes of prime power length over $\mathbb{F}_{p^m}[u]/\langle u^a\rangle$ and their duals*, Discrete Mathematics, vol. 339, no. 6, pp. 1706–1715, 2016.

[8] H. Q. Dinh, B. T. Nguyen, and S. Sriboonchitta, *On a class of constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}[u]/\langle u^a\rangle$*, Bulletin of the Korean Mathematical Society, vol. 55, no. 4, pp. 1189–1208, 2018.

[9] H. Q. Dinh, B. T. Nguyen, and S. Sriboonchitta, *On a class of constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m}[u]/\langle u^a\rangle$*, Algebra Colloquium, vol. 26, no. 2, pp. 181–194, 2019.

[10] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker Inc., 1974.

[11] H. Q. Dinh and S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Transactions on Information Theory, vol. 50, no. 8, pp. 1728–1744, 2004.

[12] H. Q. Dinh, H. D. T. Nguyen, S. Sriboonchitta, and T. M. Vo, *Repeated-root constacyclic codes of prime power lengths over finite chain rings*, Finite Fields and Their Applications, vol. 43, pp. 22–41, 2017.

[13] R. Lidl, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, pp. 1–46, 1983.

[14] M. Özkan and F. Öke, *Gray images of $(1+v)$-constacyclic codes over a particular ring*, Palestine Journal of Mathematics, vol. 6, 2017.

[15] A. Dertli, Y. Cengellenmis, and S. Eren, *On skew cyclic and quasi-cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$*, Palestine Journal of Mathematics, vol. 4, no. 1, pp. 540–546, 2015.

[16] Y. Ahendouz and I. Akharraz, *On repeated-root constacyclic codes of arbitrary lengths over Galois ring* $\mathrm{GR}(p^m, \ell)$, Palestine Journal of Mathematics, 2024.

[17] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2010.

Author information

Youssef Ahendouz, Mathematical and Informatics Engineering Laboratory , Ibn Zohr University, Morocco.
E-mail: youssef.ahendouz@gmail.com,

Ismail Akharraz, Mathematical and Informatics Engineering Laboratory , Ibn Zohr University, Morocco.
E-mail: i.akharraz@uiz.ac.ma

Received: 2024-03-07
Accepted: 2024-07-16