Gulf Journal of Mathematics
Vol 8, Issue 2 (2020) 55-67

PRIMITIVE IDEMPOTENTS AND CONSTACYCLIC CODES OVER FINITE CHAIN RINGS

MOHAMMED ELHASSANI CHARKANI[1] AND JOËL KABORE[2*]

Abstract. Let R be a commutative local finite ring. In this paper, we construct the complete set of pairwise orthogonal primitive idempotents of $R[X]/\langle g\rangle$ where g is a regular polynomial in $R[X]$. We use this set to decompose the ring $R[X]/\langle g\rangle$ and to give the structure of constacyclic codes over finite chain rings. This allows us to describe generators of the dual code $\mathcal{C}^\perp$ of a constacyclic code $\mathcal{C}$ and to characterize non-trivial self-dual constacyclic codes over finite chain rings.

1. Introduction

Constacyclic codes over finite commutative rings are an important class of linear block codes. Let R be a commutative ring with identity, it's well-known that for a given unit λ, the λ-constacyclic codes over R are ideals of the ring $\frac{R[X]}{\langle X^n-\lambda\rangle}$. When studying constacyclic codes over finite chain rings, many authors assume that the code length is prime with the characteristic of its residue field. This ensures that the polynomial $X^n - \lambda$ have no multiple factor; in this case the codes are called simple root constacyclic codes, else they are called repeated root constacyclic codes. Simple root constacyclic codes have been extensively study by many authors [9, 3, 13, 6, 4, 7].

P. Kanwar and S. Lopez-Permouth gave the structure of cyclic codes over $\mathbb{Z}_{p^m}$, the ring of integers modulo p^m [9] . H. Q. Dinh and S. Lopez-Permouth extended this structure to cyclic codes and negacyclic codes of odd length over finite chain ring [4]. They gave some necessary and sufficient conditions for the existence of non-trivial self-dual cyclic codes. E. Martínez-Moro and I. F. Rúa generalized these results to multivariable codes over finite chain rings. S.T. Dougherty studied the cyclic codes of arbitrary length over the ring of integers modulo m [5]. Using these results, A. Batoul et al. considered the self-duality of cyclic codes over finite chain rings [1]. Some additionally necessary and sufficient conditions for the existence of non-trivial negacyclic and cyclic self-dual codes are given in [7] with a different method from that given in [9, 4].

Idempotents are very excellent tools to describe finitely generated modules over a decomposable commutative ring $A = \prod_{i=1}^n A_i$. Indeed if $A \simeq \prod_{i=1}^n A_i$

Date: Received: Sep 2, 2019; Accepted: Mar, 23 2020.
* Corresponding author.
2010 *Mathematics Subject Classification.* Primary 16U99; 94B05; Secondary 94B60.
Key words and phrases. Finite chain ring, Idempotent, Constacyclic code, Self-dual code.

is a decomposable ring, then the studying of the structure of finitely generated modules over the ring A is reduced to studying the structure of finitely generated modules over each component ring A_i. Idempotents have been used to describe minimal cyclic codes over finite fields [14].

In this paper, we use idempotents of the quotient ring $\frac{R[X]}{\langle X^n-\lambda\rangle}$ to determine the structure of constacyclic codes over finite chain rings. Our method standardize the results of [9, 4, 7, 1]. We first construct a complete set of primitive pairwise orthogonal idempotents of $R[X]/\langle g\rangle$, where R is a commutative finite local ring and g is a regular polynomial in $R[X]$. We use this family of idempotents to construct simple root constacyclic codes over finite chain rings. We also investigate the dual code $\mathcal{C}^\perp$ of a constacyclic code $\mathcal{C}$ and characterize non-trivial self-dual constacyclic codes over finite chain ring. We show that all non-trivial constacyclic self-dual codes can be determined by non-trivial cyclic or non-trivial negacyclic self-dual codes.

2. Preliminaries

Let R be a finite local commutative ring, $\mathfrak{m}$ be the maximal ideal of R and $\mathbb{F}_q$ its residue field. Let $^-$ be the natural surjective ring morphism given by:

$$\begin{array}{cccc} ^-: & R & \longrightarrow & \mathbb{F}_q \\ & r & \longmapsto & r+\mathfrak{m}. \end{array}$$

This map extends naturally to a ring morphism from $R[X]$ to $\mathbb{F}_q[X]$ by sending X to X.

An ideal I in R is primary if $I \neq R$ and whenever $xy \in I$, then either $x \in I$ or $y^n \in I$ for some positive integer n. We say that two ideals I and J are coprime in R if $I+J=R$. A polynomial f in $R[X]$ is called primary if $fR[X]$ is a primary ideal; regular if f is not a zero divisor; basic irreducible if $\bar{f}$ is irreducible in $\mathbb{F}_q[X]$. Two polynomials $f, g \in R[X]$ are called coprime if $fR[X]$ and $gR[X]$ are coprime in $R[X]$; that is to say, there exists u and v in $R[X]$ such that $fu+gv=1$. This last relation is well-known as Bézout Identity. Let Recall the Gauss Lemma which is an additive property.

Proposition 2.1 (Gauss Lemma)**.** *Let R be a commutative ring with identity. Let f and g be two monic coprime polynomials in $R[X]$. If f divides the product hg in $R[X]$ then f divides h in $R[X]$.*

Proof. Indeed, if f and g are two monic coprime polynomials in $R[X]$, then there exists u and v in $R[X]$ such that $fu+gv=1$. This implies that $h=hfu+hgv$. Since f divides hg, then there exists w in $R[X]$ such that $hg=wf$ and $h= hfu+wfv=f(hu+wv)$. Therefore f divides h in $R[X]$. □

Proposition 2.2 ([12], Theorem XIII.11)**.**

Let R be a commutative local finite ring and f be a regular polynomial in $R[X]$. Then $f=\delta g_1...g_r$ where δ is a unit and $g_1, g_2, ..., g_r$ are regular primary pairwise-coprime polynomials.

Moreover, $g_1, ..., g_r$ are unique in the sense that if $f=\delta g_1...g_r=\beta h_1...h_s$, where δ, β are units, and $\{g_i\}$, $\{h_i\}$ are regular primary coprime polynomials, then $r=s$, and after renumbering $g_iR[X]=h_iR[X]$, $1\leq i\leq r$.

The following result is very useful for determining coprime polynomials.

Proposition 2.3 ([12])**.** *Let R be a finite chain ring. Let f and g be two regular polynomials in $R[X]$. Then f and g are two coprime polynomials in $R[X]$ if and only if $\overline{f}$ and $\overline{g}$ are two coprime polynomials in $k[X]$.*

The following result shows that we can reduce a study with regular polynomials to monic polynomials.

Proposition 2.4 ([12], Theorem XIII.6)**.** *Let R be a commutative finite local ring and f be a regular polynomial in $R[X]$. Then there is a monic polynomial g with $\bar{f} = \bar{g}$ and, for an element a in R, $f(a) = 0$ if and only if $g(a) = 0$. Further, there is a unit δ in $R[X]$ with $\delta f = g$.*

A code $\mathcal{C}$ of length n over R is nonempty subset of R^n; if in addition the code is a submodule of R^n, it is called linear code. In this paper all codes are assumed to be linear. For a given unit $\lambda \in R$, the λ-constacyclic shift σ on R^n is defined by $\sigma(a_0, ..., a_{n-1}) = (\lambda a_{n-1}, a_0, ..., a_{n-2})$ and a code of length n over R is said to be λ-constacyclic if it is invariant under the λ-constacyclic shift σ. Cyclic and negacyclic codes are examples of λ-constacyclic codes for $\lambda = 1$ and -1 respectively. The λ-constacyclic codes of length n over R are identified with ideals of $\frac{R[X]}{\langle X^n-\lambda\rangle}$ by the identification: $(a_0, a_1, ..., a_{n-1}) \longmapsto a_0 + a_1x + ...a_{n-1}x^{n-1}$; where $x = X + \langle X^n - \lambda\rangle$ is the equivalence class of X in $\frac{R[X]}{\langle X^n-\lambda\rangle}$.
Given codewords $a = (a_0, a_1, ..., a_{n-1})$, $b = (b_0, b_1, ..., b_{n-1}) \in R^n$, their inner product is defined in the usual way:

$$a.b = a_0b_0 + a_1b_1 + ...a_{n-1}b_{n-1}, \text{ evaluated in } R.$$

The codewords a, b are called orthogonal if $a.b = 0$. The dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ is the set of n-tuples over R that are orthogonal to all codewords of $\mathcal{C}$:

$$\mathcal{C}^\perp = \{a \mid a.b = 0, \forall a \in \mathcal{C}\}.$$

A code $\mathcal{C}$ is called self-orthogonal code if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and self-dual code if $\mathcal{C} = \mathcal{C}^\perp$.

Proposition 2.5 ([8], Lemma 2.1)**.** *Let λ be a unit in R, the dual of a λ-constacyclic code is a λ^{-1}-constacyclic code.*

Let f be the polynomial $f = a_0 + a_1x + ... + a_{n-1}x^{n-1} \in R[x]$, where $x = X + \langle X^n - \lambda\rangle$ and $a_0, a_1, ..., a_{n-1} \in R$. The reciprocal polynomial of f denoted by f^* is defined as $f^* = a_0x^{n-1} + a_1x^{n-2} + ... + a_{n-1}$. Note that $(f^*)^* = f$. The following result is easy to check.

Proposition 2.6. *Let f and g be two polynomials in $R[x]$ with $\deg f \geq \deg g$. Then the followings hold:*

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

Let λ be a unit in R and $\mathcal{C}$ be an ideal of $R[X]/\langle X^n - \lambda\rangle$. We define $\mathcal{C}^*$ by $\mathcal{C}^* = \{f(x)^* \in R[x] : f(x) \in \mathcal{C}\}$. We let

$$\mathcal{A}(\mathcal{C}) = \{g(x) \in R[x] : f(x)g(x) = 0, \ \forall \ f(x) \in \mathcal{C}\}.$$

The set $\mathcal{A}(\mathcal{C})$ is an ideal of $R[X]/\langle X^n - \lambda\rangle$ called annihilator of $\mathcal{C}$.

Proposition 2.7 ([8], Proposition 2.3)**.**
Let λ be a unit in R, $\mathcal{C}$ be a λ-constacyclic code of length n over R and $\mathcal{C}^{\perp}$ be the dual code of $\mathcal{C}$. Then

$$\mathcal{C}^{\perp} = \mathcal{A}(\mathcal{C})^{*}.$$

3. The quotient ring $R[X]/\langle g\rangle$ and the idempotents

Let R be a commutative ring with identity. An element e of R is called idempotent if $e = e^2$; two idempotents e_1, e_2 are said to be orthogonal if $e_1e_2 = 0$. An idempotent of R is said primitive if it is non-zero and cannot be written as sum of non-zero orthogonal idempotents. A set $\{e_1, ..., e_r\}$ of elements of R is called a complete set of idempotents if $\sum_{i=1}^{r} e_i = 1$. If $\{e_1, ..., e_r\}$ is a complete set of pairwise orthogonal idempotents of R, it's easy to show that $R = \oplus_{i=1}^{r} e_iR$.

Proposition 3.1. *([10], Proposition 22.1)*
Let R be a commutative ring with identity. There exists at most one complete set of pairwise orthogonal primitive idempotents $\{e_1, ..., e_r\}$ of R. Moreover, any idempotent in R is uniquely written as a finite sum of primitive idempotents of this set.

Proof. Let $\{e_1, ..., e_r\}$ be a complete set of pairwise orthogonal primitive idempotents in R. If θ is an idempotent in R, then $1 - \theta$ is also an idempotent in R and we have: $1 = \theta + (1 - \theta)$. This implies that $e_i = \theta e_i + (1 - \theta)e_i$. Since e_i is primitive for all $i \in \{1, .., r\}$, then $\theta e_i = 0$ or $\theta e_i = e_i$. There exists $I \subseteq \{1, .., r\}$ such that $\theta = \sum_{i=1}^{r} \theta e_i = \sum_{i\in I} \theta e_i = \sum_{i\in I} e_i$. Moreover, if θ is primitive, then there exists $i \in \{1, .., r\}$ such that $\theta = e_i$, whence the set $\{e_1, ..., e_r\}$ is unique.
We suppose that there exists $J \subseteq \{1, .., r\}$ such that $J \neq I$ and $\theta = \sum_{i\in I} e_i = \sum_{i\in J} e_i$. Then, there exists $j \notin I \cap J$ such that $\theta e_j = e_j$ and $\theta e_j = 0$, absurd. □

Let R be a finite local commutative ring and g be a regular polynomial in $R[X]$. From Propositions 2.2 and 2.4, we can assume g is a monic polynomial in $R[X]$ and factors uniquely as a product of monic primary pairwise coprime polynomials: $g = \prod_{i=1}^{r} g_i$. We let $\hat{g}_i = \frac{g}{g_i}$. Note that g_i and $\hat{g}_i$ are coprime and regular polynomials.

Theorem 3.2. *Let R be a finite local commutative ring and g be a monic polynomial in $R[X]$ such that $g = \prod_{i=1}^{r} g_i$ is the unique factorization of g into a product of monic primary pairwise coprime polynomials. Let $x = X + \langle g\rangle$ be the equivalence class of X in $R[X]/\langle g\rangle$. The ring $R[X]/\langle g\rangle$ admits a unique complete set of primitive pairwise orthogonal idempotents $\{e_1, e_2, ..., e_r\}$ given by:*

$$e_i = v_i(x)\hat{g}_i(x), \text{ where } v_i(x) \in R[x].$$

Moreover $e_iR[x] \cong \frac{R[X]}{\langle g_i\rangle}$ and $R[x] = \oplus_{i=1}^{r} e_iR[x]$.

Proof. Let $g = \prod_{i=1}^{r} g_i$ be the unique factorization of g into a product of monic primary pairwise coprime polynomials of g in $R[X]$. Since g_i and $\hat{g}_i = g/g_i$ are coprime in $R[X]$, then there exists $u_i, v_i \in R[X]$ such that $u_ig_i + v_i\hat{g}_i = 1$. We let

$e_i = v_i(x)\hat{g}_i(x)$ where $x = X + \langle g \rangle$ is the equivalence class of X in $R[X]/\langle g \rangle$. We have:

$$e_i^2 = v_i(x)\hat{g}_i(x)(1 - u_i(x)g_i(x)) = v_i(x)\hat{g}_i(x) = e_i.$$

If $i \neq j$, then $e_i e_j = v_i(x)\hat{g}_i(x)v_j(x)\hat{g}_j(x) = 0$. Hence $\{e_1, e_2, ..., e_r\}$ is a set of pairwise orthogonal idempotents.

The Proposition 2.1 (Gauss Lemma) ensures the uniqueness of e_i. Indeed, assume $(u_i^{'}, v_i^{'})$ is another pair of polynomials in $R[X]$ such that: $u_i^{'} g_i + v_i^{'}\hat{g}_i = 1$; then $u_i^{'} g_i + v_i^{'}\hat{g}_i = u_i g_i + v_i \hat{g}_i$, which gives $(u_i^{'} - u_i)g_i = (v_i - v_i^{'})\hat{g}_i$. Since g_i and $\hat{g}_i$ are coprime and regulars, then g_i divides $v_i - v_i{'}$ from Gauss Lemma. Then there exists h in $R[X]$ such that: $v_i - v_i^{'} = hg_i$. Hence $v_i = hg_i + v_i^{'}$, and $e_i = v_i(x)\hat{g}_i(x) = v_i^{'}(x)\hat{g}_i(x)$.

Since $\hat{g}_1, \hat{g}_2, ..., \hat{g}_r$ are coprime, there exists $v_1, v_2, ..., v_r \in R[X]$ such that $\sum_{i=1}^r v_i \hat{g}_i = 1$; hence $\sum_{i=1}^r e_i = 1$. Let

$$\begin{array}{llll} T: & R[X] & \longrightarrow & e_i R[x] \\ & h & \longmapsto & e_i h = v_i(x)\hat{g}_i(x)h. \end{array}$$

T is an onto ring homomorphism and by the Gauss Lemma (Proposition 2.1) we see that $\ker T = \langle g_i \rangle$, and hence by the first isomorphism theorem, we deduce $R[X]/\langle g_i \rangle \cong e_i R[x]$. Since g_i is primary in $R[X]$, then $R[X]/\langle g_i \rangle$ is a local ring, so it is an indecomposable ring. Therefore $\{e_1, e_2, ..., e_r\}$ is a set of primitive idempotents. □

4. Constacyclic codes over finite chain ring

A finite chain ring is a finite commutative ring with identity such that its ideals are linearly ordered by inclusion. The following result is well know and characterizes finite chain rings.

Proposition 4.1 ([4], Proposition 2.1)**.** *Let R be a finite commutative ring with identity, the following conditions are equivalent:*

(1) *R is a local ring and the maximal ideal of R is principal,*
(2) *R is a local principal ideal ring,*
(3) *R is a chain ring.*

If R is a finite chain ring with maximal ideal γR; then γ is nilpotent with nilpotency index some integer t and the ideals of R form the following chain:

$$0 = \gamma^t R \subsetneq \gamma^{t-1} R \subsetneq ... \subsetneq \gamma R \subsetneq R.$$

We denote the residue field $R/\langle \gamma \rangle$ by $\mathbb{F}_{p^r}$. It's well-known that for linear codes of length n over a finite chain ring R, $|\mathcal{C}||\mathcal{C}^{\perp}| = |R|^n$ (see [13]).

Lemma 4.2 ([4], Lemma 3.1)**.**
Let R be a finite chain ring with maximal ideal γR, index of nilpotency t and residue field $\mathbb{F}_q$. Let f be a monic basic irreducible polynomial in the ring $R[X]$ and $x = X + \langle f \rangle$ be the equivalence class of X in $\frac{R[X]}{\langle f \rangle}$. Then $\frac{R[X]}{\langle f \rangle}$ is a finite chain ring with maximal ideal $\gamma R[x]$ and index of nilpotency t.

Since $(n, p) = 1$, the polynomial $X^n - \lambda$ factors uniquely as a product of monic basic irreducible pairwise coprime polynomials in R ([4], Proposition 2.7). In the rest of paper we denote by $x = X + \langle X^n - \lambda \rangle$ the equivalence class of X in $R[X]/\langle X^n - \lambda \rangle$, thus $R[X]/\langle X^n - \lambda \rangle = R[x]$.

Theorem 4.3. *Let R be a finite chain ring with maximal ideal γR, index of nilpotency t and residue field $\mathbb{F}_q$. Let λ be a unit in R, $X^n - \lambda = f_1 f_2 ... f_r$ be the unique decomposition of $X^n - \lambda$ into product of monic basic irreducible pairwise coprime polynomials and $\{e_1, ..., e_r\}$ be the complete set of primitive pairwise orthogonal idempotents in $R[x]$.*
Let $\mathcal{C}$ be a λ-constacyclic code of length n over R. Then there exists a unique sequence of integers $(s_1, ..., s_r)$ such that $0 \leq s_i \leq t$ and

$$\mathcal{C} = \oplus_{i=1}^{r} \gamma^{s_i} e_i R[x].$$

Proof. Since $R[x] = \oplus_{i=1}^{r} e_i R[x]$; then any ideal I in $R[x]$ is written in the form $I = \oplus_{i=1}^{r} I_i$, where I_i is an ideal of $e_i R[x]$. By Theorem 3.2, we have $e_i R[x] \cong R[X]/\langle f_i \rangle$. From previous lemma, we know that ideals of $R[X]/\langle f_i \rangle$ are in the form $\gamma^j (R[X]/\langle f_i \rangle),\ 0 \leq j \leq t$; therefore $I_i = \gamma^j e_i R[x],\ 0 \leq j \leq t$. □

Theorem 4.4. *Let R be a finite chain ring with maximal ideal γR, index of nilpotency t and residue field $\mathbb{F}_q$. Let λ be a unit in R and $\mathcal{C}$ be a λ-constacyclic code of length n over R. Then there exists a complete set of pairwise orthogonal idempotents $\{\theta_0, ..., \theta_l\}$ in $R[x]$ such that:*

$$\mathcal{C} = \oplus_{i=0}^{l-1} \gamma^{r_i} \theta_i R[x];$$

with $0 \leq r_0 < r_1 < ... < r_{l-1} < r_l = t$ and $\sum_{i=0}^{l} \theta_i = 1$.
Moreover there exists a unique family of pairwise coprime polynomials $g_0, g_1, ..., g_l$ in $R[X]$ such that:
$\theta_i R[x] \cong R[X]/\langle g_i \rangle,\ \forall\ i \in \{0, 1, ..., l\}$ et $\prod_{i=0}^{l} g_i = X^n - \lambda$.

Proof. Let $X^n - \lambda = f_1 f_2 ... f_r$ be the decomposition of $X^n - \lambda$ into product of monic basic irreducible pairwise coprime polynomials in R and $\{e_1, ..., e_r\}$ be the complete set of primitive pairwise orthogonal idempotents of $R[x]$.
From the previous theorem: $\mathcal{C} = \oplus_{i=1}^{r} \gamma^{s_i} e_i R[x],\ 0 \leq s_i \leq t$. By reordering if necessary according to the powers of γ, we can write $\mathcal{C}$ in the form:

$$\mathcal{C} = \bigoplus_{j\ |s_j = r_0} \gamma^{r_0} e_j R[x] \bigoplus_{j\ |s_j = r_1} \gamma^{r_1} e_j R[x] \bigoplus ... \bigoplus_{j\ |s_j = r_{l-1}} \gamma^{r_{l-1}} e_j R[x]$$

with $0 \leq r_1 < r_2 < ... < r_l = t$. We let $\theta_i = \sum_{j\ |s_j = r_i} e_j,\ \forall i \in \{0, ..., l-1\}$ and $\theta_l = 1 - \sum_{i=0}^{l-1} \theta_i$. Therefore, the set $\{\theta_0, \theta_1, ..., \theta_l\}$ is a complete set of pairwise orthogonal idempotents; by construction this set is unique. We have:

$$\mathcal{C} = \oplus_{i=0}^{l-1} \gamma^{r_i} \theta_i R[x].$$

Since $e_j R[x] \cong \frac{R[X]}{\langle f_j \rangle},\ \forall\ 1 \leq j \leq r$, then $\theta_i R[x] \cong \prod_{j\ |s_j = r_i} \frac{R[X]}{\langle f_j \rangle} \cong \frac{R[X]}{\langle \prod_{j\ |s_j = r_i} f_j \rangle}$, by the Chinese Remainder Theorem. We let $g_i = \prod_{j\ |s_j = r_i} f_j,\ \forall\ 0 \leq i \leq l$. It is clear that $\prod_{i=0}^{l} g_i = X^n - \lambda$. □

Corollary 4.5. *Under the same assumptions as the Theorem 4.4, let $\mathcal{C}$ be a λ-constacyclic code of length n over R. Then*

$$\mathcal{C} = (\oplus_{i=0}^{l-1}\gamma^{r_i}\theta_i)R[x].$$

Proof. From previous theorem, we have: $\mathcal{C} = \oplus_{i=0}^{l-1}\gamma^{r_i}\theta_i R[x]$ with $0 \leq r_0 < r_1 < ... < r_l = t$. We let $w = \sum_{i=0}^{l-1}\gamma^{r_i}\theta_i$. It's clear that $wR[x] \subseteq \mathcal{C}$. Reciprocally, if $b \in \mathcal{C}$, then $b = \sum_{i=0}^{l-1}\gamma^{r_i}\theta_i b_i$ with $b_i \in R[x]$, $\forall\ 0 \leq i \leq l-1$. For any idempotent $\theta_j \in R[x]$, we have: $\theta_j b = \gamma^{r_j}\theta_j b_j = \theta_j w b_j$. Therefore $b = \sum_{j=0}^{l-1}\theta_j b = \sum_{j=0}^{l-1}\theta_j w b_j = (\sum_{j=0}^{l-1}\theta_j b_j)w$; hence $b \in wR[x]$. □

Corollary 4.6. *Under the same assumptions as the Theorem 4.4, let $\mathcal{C}$ be a λ-constacyclic code of length n over R such that*

$$\mathcal{C} = \oplus_{i=0}^{l-1}\gamma^{r_i}\theta_i R[x]$$

with $0 \leq r_0 < r_1 < ... < r_l = t$. Then:

$$|\mathcal{C}| = |\mathbb{F}_q|^{\sum_{i=0}^{l-1}(t-r_i)\deg g_i}.$$

Proof. Since $\theta_i R[x] \cong R[X]/\langle g_i\rangle$ then

$$|\gamma^{r_i}\theta_i R[x]| = |\gamma^{r_i}(R[X]/\langle g_i\rangle)|.$$

We let $A_i = R[X]/\langle g_i\rangle$. The map

$$\begin{array}{cccc} \phi_i : & A_i & \longrightarrow & \gamma^{r_i}A_i \\ & h & \longmapsto & \gamma^{r_i}h \end{array}$$

is an epimorphism and $\ker\phi_i = \gamma^{t-r_i}A_i$. By the first isomorphism theorem $A_i/(\gamma^{t-r_i}A_i) \cong \gamma^{r_i}A_i$. But $A_i/(\gamma^{t-r_i}A_i) \cong R_i[X]/\langle\widetilde{g}_i\rangle$, where $R_i = R/\langle\gamma^{t-r_i}\rangle$ and $\widetilde{g}_i = g_i + \langle\gamma^{t-r_i}\rangle$. Therefore:

$$\begin{aligned} |\gamma^{r_i}A_i| &= |A_i/(\gamma^{t-r_i}A_i)| = |R_i[X]/\langle\widetilde{g}_i\rangle| = |R_i|^{\deg g_i} \\ &= \left(\tfrac{|R|}{|\gamma^{t-r_i}R|}\right)^{\deg g_i} = |\mathbb{F}_q|^{(t-r_i)\deg g_i}. \end{aligned}$$

We deduce:

$$|\mathcal{C}| = \prod_{i=0}^{l-1}|\gamma^{r_i}\theta_i R[x]| = |\mathbb{F}_q|^{\sum_{i=0}^{l-1}(t-r_i)\deg g_i}.$$

□

Lemma 4.7. *Let R be a commutative ring.*

i) If e_1 et e_2 are orthogonal idempotents in $R[X]$ then $(e_1+e_2)^* = e_1^* + e_2^*$.
ii) If e is a primitive idempotent in $R[X]$, then e_1^* is a primitive idempotent in $R[X]$.

Proof. i) If e_1 et e_2 are orthogonal idempotents in $R[X]$, then $e = e_1 + e_2$ is also an idempotent. Since $ee_i = e_i$, for all $i \in \{1,2\}$ we have $(ee_i)^* = e^*e_i^* = e_i^*$, for all $i \in \{1,2\}$. Then e^* is written in the form: $e^* = e_1^* + e_2^* + \theta$ where e_1^*, e_2^*, θ are pairwise orthogonal idempotents. Likewise

$$e_1 + e_2 = e = (e^*)^* = (e_1^*)^* + (e_2^*)^* + \theta^* + \beta = e_1 + e_2 + \theta^* + \beta,$$

where $e_1, e_2, \theta^*, \beta$ are pairwise orthogonal idempotents. We deduce $\theta^* + \beta = \theta^* = \beta = 0$; whence $(e_1+e_2)^* = e_1^* + e_2^*$.

ii) It's obvious from *i*).

□

Lemma 4.8. *Let I be an ideal of $R[x]$ such that $I = \oplus_{1\leq i\leq r}\ h_iR[x]$, then $I^* = \oplus_{1\leq i\leq r}\ h_i^*R[x]$.*

Proof. Let I be an ideal of $R[x]$ such that $I = h_1R[x]+h_2R[x]$; it is clear that $I^* = h_1^*R[x] + h_2^*R[x]$. Let $f \in h_1^*R[x] \cap h_2^*R[x]$, then $f = h_1^*u = h_2^*v$ with $u, v \in R[x]$. If f is non zero then $f^* = h_1u^* = h_2v^*$. This implies that $f^* \in h_1R[x] \cap h_2R[x]$ and hence we deduce that $f^* = 0$. We deduce that $h_1^*R[x] \cap h_2^*R[x] = \{0\}$. □

Theorem 4.9. *Under the same assumptions as the Theorem 4.4, let $\mathcal{C}$ be a λ-constacyclic code of length n over R such that*

$$\mathcal{C} = \oplus_{i=0}^{l-1}\gamma^{r_i}\theta_iR[x],$$

with $0 \leq r_0 < r_1 < ... < r_l = t$. Then:

$$\mathcal{C}^{\perp} = \oplus_{i=0}^{l}\gamma^{t-r_i}\theta_i^*R[x].$$

Proof. Let $D = \oplus_{i=0}^{l}\gamma^{t-r_i}\theta_iR[x]$. For all $i, j \in \{0, ..., l\}$, we have:
$(\gamma^{r_i}\theta_i)(\gamma^{t-r_j}\theta_j) = 0$, then $D \subseteq \mathcal{A}(\mathcal{C})$.
From Corollary 4.6, $|D| = |\mathbb{F}_q|^{\sum_{i=0}^{l} r_i \deg g_i}$. We recall that $|\mathcal{C}||\mathcal{C}^{\perp}| = |R|^n$(see [13]).
Then:

$$\begin{aligned} |\mathcal{C}^{\perp}| &= \tfrac{|R|^n}{|\mathcal{C}|} = |\mathbb{F}_q|^{nt-\sum_{i=0}^{l-1}(t-r_i)\deg g_i} \\ &= |\mathbb{F}_q|^{nt-\sum_{i=0}^{l-1} t\deg g_i+\sum_{i=0}^{l-1} r_i \deg g_i} \\ &= |\mathbb{F}_q|^{t\deg g_l+\sum_{i=0}^{l-1} r_i \deg g_i} \end{aligned}$$

Therefore: $|\mathcal{A}(\mathcal{C})| = |\mathcal{A}(\mathcal{C})^*| = |\mathcal{C}^{\perp}| = |D|$; whence $D = \mathcal{A}(\mathcal{C})$. We conclude that

$$\mathcal{C}^{\perp} = D^* = \sum_{i=0}^{l}\gamma^{t-r_i}\theta_i^*R[x].$$

□

Let $\lceil \frac{t}{2} \rceil$ be the smallest integer greater than or equal to $t/2$. If $\mathcal{C}$ is a linear code over R such that $\mathcal{C} \subseteq \gamma^{\lceil \frac{t}{2} \rceil}R^n$, it is easy to see that $\mathcal{C} \subseteq \mathcal{C}^{\perp}$. These codes are called trivial self-orthogonal codes. Moreover, if t is even, then the code $\mathcal{C} = \gamma^{t/2}R^n$ is self-dual and called trivial self-dual code.

Let $\mathcal{C} \subseteq R^n$ be a linear code. The submodule quotient of $\mathcal{C}$ by $r \in R$ is a linear code defined by $(\mathcal{C} : r) = \{a \in R^n : ra \in \mathcal{C}\}$. We have the following tower of linear codes over R

$$\mathcal{C} = (\mathcal{C} : \gamma^0) \subseteq ... \subseteq (\mathcal{C} : \gamma^{t-1})$$

and its projection to $\mathbb{F}_{p^r}$

$$\overline{\mathcal{C}} = \overline{(\mathcal{C} : \gamma^0)} \subseteq ... \subseteq \overline{(\mathcal{C} : \gamma^{t-1})}.$$

For a unit $\lambda \in R$, note that if $\mathcal{C}$ is a λ-constacyclic code over R, then $(\mathcal{C} : \gamma^i)$ is a λ-constacyclic code over R and $\overline{(\mathcal{C} : \gamma^i)}$ is a $\overline{\lambda}$-constacyclic code over $\mathbb{F}_{p^r}$, for $i \in \{0, 1, ..., t-1\}$. The following result generalises Lemma 3.3 in [8] to finite chain rings.

Proposition 4.10. *Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$, index of nilpotency t and residue field $\mathbb{F}_q$. Let λ be a unit in R and $\mathcal{C}$ be a non-trivial λ-constacyclic self-orthogonal code over R. Then $\overline{\lambda} = \pm 1$.*

Proof. We suppose $\mathcal{C}$ is a nontrivial λ-constacyclic self-orthogonal code over R. If $\overline{\mathcal{C}} \neq \{0\}$, then $\overline{\mathcal{C}}$ is a $\overline{\lambda}$-constacyclic self-orthogonal code over $\mathbb{F}_q$. It is well-known that the only constacyclic self-orthogonal codes over a finite field are cyclic and negacyclic codes([8], Proposition 2.4); whence $\overline{\lambda} = \pm 1$.

If $\overline{\mathcal{C}} = \{0\}$, then there exists a smallest positive integer i with $1 \leq i \leq t-1$ such that any codeword $c \in \mathcal{C}$ can be written as: $c = \gamma^i a$, with $a \in R^n$. Without loss of generality, we can suppose $\mathcal{C} \subseteq \langle\gamma^i\rangle$. Since $\mathcal{C}$ is a non-trivial λ-constacyclic self-orthogonal code over R, then $i < \lceil \frac{t}{2} \rceil$, that is to say $2i < t$ and $\overline{(\mathcal{C} : \gamma^i)}$ is self-orthogonal. Indeed if $a, b \in (\mathcal{C} : \gamma^i)$, then $c_1 = \gamma^i a$ and $c_2 = \gamma^i b$ verify $c_1.c_2 = \gamma^{2i}(a.b) = 0$; hence $a.b = 0$. Then $\overline{(\mathcal{C} : \gamma^i)}$ is self-orthogonal over $\mathbb{F}_q$ and $\bar{\lambda} = \pm 1$. $\square$

The following result shows us there exists a one-to-one correspondence between cyclic codes (respectively negacyclic codes) and $(1+\gamma^i\beta)$-constacyclic codes (respectively $(1+\gamma^i\beta)$-constacyclic codes) over R, with $\beta \in R$.

Proposition 4.11 ([2], Corollary 4.5)**.**
Let R be a finite chain ring with maximal ideal γR, index of nilpotency t and residue field $\mathbb{F}_q$. Let n be a positive integer such that $(n, q) = 1$, $\lambda \in 1 + \gamma R$ and $\beta \in -1 + \gamma R$. Then there exists a ring isomorphism between $R[X]/\langle X^n - 1\rangle$ (respectively $R[X]/\langle X^n + 1\rangle$) and $R[X]/\langle X^n - \lambda\rangle$ (respectively $R[X]/\langle X^n - \beta\rangle$).

From Proposition 4.10 and Proposition 4.11, we can reduce the study of non-trivial constacyclic self-dual codes over R to non-trivial cyclic and negacyclic self-dual codes over R.

5. Self-dual cyclic codes

Theorem 5.1. *Under the same assumptions as the Theorem 4.4, let $\mathcal{C}$ be a λ-constacyclic code of length n over R such that*

$$\mathcal{C} = \oplus_{i=0}^{l-1} \gamma^{r_i} \theta_i R[x]$$

with $0 \leq r_0 < r_1 < \ldots < r_l = t$. Then $\mathcal{C}$ is a non-trivial self-dual code if and only if θ_i and θ_j^* are associated and $r_i + r_j = t$, for all $i, j \in \{0, \ldots, l-1\}$ such that $i + j \equiv 0 \mod l-1$.

Proof. If $\mathcal{C} = \oplus_{i=0}^{l-1} \gamma^{r_i} \theta_i R[x]$, then by Theorem 4.9,

$$\mathcal{C}^{\perp} = \sum_{i=0}^{l} \gamma^{t-r_i} \theta_i^* R[x].$$

If $\mathcal{C}$ is self-dual we must have $\theta_l = 0$. In this case $\mathcal{C}^{\perp} = \sum_{i=0}^{l-1} \gamma^{t-r_i} \theta_i^* R[x]$ with $\sum_{i=0}^{l-1} \theta_i = 1$ and $0 \leq r_0 < r_1 < \ldots < r_{l-1} < t$. We obtain the result by comparing γ exponents. $\square$

Corollary 5.2. *Under the same assumptions as the Theorem 4.4, let $\mathcal{C}$ be a cyclic code of length n over R such that*

$$\mathcal{C} = \oplus_{i=0}^{l-1} \gamma^{r_i} \theta_i R[x]$$

with $0 \le r_0 < r_1 < ... < r_l = t$. If there exists a non-trivial cyclic self-dual code over R, then t is necessary even.

Proof. If $\mathcal{C}$ is self-dual, then by Theorem 5.1, $\mathcal{C} = \oplus_{i=0}^{l-1} \gamma^{r_i} \theta_i R[x]$, with $0 \le r_0 < r_1 < ... < r_{l-1} < t; r_i + r_j = t$, for all $i, j \in \{0, ..., l-1\}$ such that $i + j \equiv 0 \mod l-1$. Let $X^n - 1 = \prod_{i \in I} f_i$ be the decomposition of $X^n - 1$ into a product of monic basic irreducible pairwise coprime polynomials in $R[X]$. Let $\{e_i\}_{i \in I}$ be the complete set of primitive pairwise orthogonal idempotents of $R[X]/\langle X^n - 1\rangle = R[x]$ given in Theorem 3.2; For $i \in I$, there exists $u_i \in R[x]$ such that $e_i = u_i(x)\hat{f}_i(x)$. Let $\theta_{i_0} \in \{\theta_0, ..., \theta_{l-1}\}$ be the idempotent containing e_0, that is to say $\theta_{i_0} = e_0 + \beta$ where β is an idempotent orthogonal to e_0.
Since that $f_0 = X - 1$, and e_0 is unique, we have

$$e_0^* = u_0^*(x)\hat{f_0}^*(x) = u_0^*(x)\hat{f}_0 = \eta e_0$$

where η is inversible in $R[x]$. Hence $\theta_{i_0}^* = e_0^* + \beta^* = \eta(e_0 + \mu\beta^*) = \epsilon\theta_{i_0}$ where $\eta\mu = 1$ in $R[x]$ and ϵ is inversible in $R[x]$.

Let $i_1 \in \{0, ..., l-1\}$ such that $i_1 + i_0 \equiv 0 \mod l-1$. If $\mathcal{C}$ is self-dual then θ_{i_1} and $\theta_{i_0}^*$ are associated, hence θ_{i_1} and θ_{i_0} are associated. This gives $i_1 = i_0$ and $2r_{i_0} = t$, whence t is even. □

Theorem 5.3. *Under the same assumptions as the Theorem 4.4, let $\mathcal{C}$ be a cyclic code of length n over R with even index of nilpotency t such that*

$$\mathcal{C} = \oplus_{i=0}^{l-1} \gamma^{r_i} \theta_i R[x]$$

with $0 \le r_0 < r_1 < ... < r_l = t$.

Then there exists a non-trivial cyclic self-dual code over R if and only if there exists an idempotent $\theta_i \in \{\theta_0, ..., \theta_{l-1}\}$ such that θ_i and θ_i^* are not associated.

Proof. Assume that there exists $\theta_i \in \{\theta_0, ..., \theta_{l-1}\}$ such that θ_i and θ_i^* are not associated. We have $1 + x^{n-1} = \sum_{j=0}^{l-1} \theta_j + \sum_{j=0}^{l-1} \theta_j^* = \theta_i + \theta_i^* + \beta$, with $\beta = 1 + x^{n-1} - \theta_i - \theta_i^*$. Note that $\beta^* = \beta$. Let $\mathcal{C} = \gamma^{t/2-1}\theta_i R[x] \oplus \gamma^{t/2}\beta R[x] \oplus \gamma^{t/2+1}\theta_i^* R[x]$. From Theorem 4.9, we deduce that $\mathcal{C}$ is self-dual.
Reciprocally, let $\mathcal{C}$ be a non-trivial self-dual cyclic code such that $\mathcal{C} = \oplus_{i=0}^{l-1} \gamma^{r_i} \theta_i R[x]$, with $0 \le r_0 < r_1 < ... r_{l-1} < t$. Assume that for all $i \in \{0, ..., l-1\}$, θ_i and θ_i^* are associated. Then by Theorem 5.1, we must have $r_i = t/2$, $\forall\ 0 \le i \le l-1$. Then $\mathcal{C}$ is thus written in the form: $\mathcal{C} = \gamma^{t/2} \oplus_{i=0}^{l-1} \theta_i R[x]$, which is absurd, since $\mathcal{C}$ is assumed to be non-trivial self-dual code. □

Example 5.4. We give a non-trivial cyclic self-dual code of length 6 over $\mathbb{Z}_{7^2}$.

Let $x = X + \langle X^6 - 1\rangle$. The irreducible factors of $X^6 - 1$ over $\mathbb{Z}_7$ are: $f_0 = X - 1; f_1 = X - 3; f_2 = X - 2; f_3 = X - 6; f_4 = X - 4; f_5 = X - 5$ and the complete set of primitive pairwise orthogonal idempotents of $\mathbb{Z}_7[X]/\langle X^6 - 1\rangle$ is given by:

$$\begin{aligned}
\theta_0 =& \ 6(x^5+x^4+x^3+x^2+x+1);\\
\theta_1 =& \ 4x^5+5x^4+x^3+3x^2+2x+6;\\
\theta_2 =& \ 5x^5+3x^4+6x^3+5x^2+3x+6;\\
\theta_3 =& \ x^5+6x^4+x^3+6x^2+x+6;\\
\theta_4 =& \ 3x^5+5x^4+6x^3+3x^2+5x+6;\\
\theta_5 =& \ 2x^5+3x^4+x^3+5x^2+4x+6.
\end{aligned}$$

From Theorem 5.4 of [9], we deduce the complete set of primitive pairwise orthogonal idempotents of $\mathbb{Z}_{7^2}[X]/\langle X^6-1\rangle$:

$$\begin{aligned}
e_0 =& \ \theta_0^7 = \ 41(x^5+x^4+x^3+x^2+x+1);\\
e_1 =& \ \theta_1^7 = \ 46x^5+5x^4+8x^3+3x^2+44x+41;\\
e_2 =& \ \theta_2^7 = \ 5x^5+3x^4+41x^3+5x^2+3x+41;\\
e_3 =& \ \theta_3^7 = \ 8x^5+41x^4+8x^3+41x^2+8x+41;\\
e_4 =& \ \theta_4^7 = \ 3x^5+5x^4+41x^3+3x^2+5x+41;\\
e_5 =& \ \theta_5^7 = \ 44x^5+3x^4+8x^3+5x^2+46x+41.
\end{aligned}$$

This gives:

$$\begin{aligned}
e_0^* =& \ 41(x^5+x^4+x^3+x^2+x+1) = & e_0;\\
e_1^* =& \ 41x^5+44x^4+3x^3+8x^2+5x+46 = & 31e_5;\\
e_2^* =& \ 41x^5+3x^4+5x^3+41x^2+3x+5 = & 30e_4;\\
e_3^* =& \ 41x^5+8x^4+41x^3+8x^2+41x+8 = & 48e_3;\\
e_4^* =& \ 41x^5+5x^4+3x^3+41x^2+5x+3 = & 18e_2;\\
e_5^* =& \ 41x^5+46x^4+5x^3+8x^2+3x+44 = & 19e_1.
\end{aligned}$$

We let $\beta = 1+x^5-e_2-e_2^* = 4x^5+43x^4+3x^3+3x^2+43x+4$. It's clear that $\beta^* = \beta$. By the previous theorem, we have the following self-dual cyclic code $\mathcal{C} = e_2\mathbb{Z}_{49}[x] \oplus 7\beta\mathbb{Z}_{49}[x]$.

Let $0 \le i \le n-1$ and $C_q(i,n)$ be the set defined by: $C_q(i,n) = \{i, iq, iq^2, ..., iq^{m_i-1}\}$ where m_i is the smallest positive integer such that $iq^{m_i} \equiv i \mod n$. This set is called the q-cyclotomic coset of n containing i. Let I be a complete set of representatives of the q-cyclotomic cosets modulo n. We recall that the decomposition of X^n-1 into a product of basic irreducible pairwise coprime polynomials in $R[X]$ is given by: $X^n-1 = \prod_{i\in I} f_i(X)$, where $f_i(X) = \prod_{j\in C_q(i,n)}(X-\xi^j)$, and ξ is a primitive nth-root of unity. It is well-known that f_i and f_i^* are associated if and only if $C_q(i,n) = C_q(n-i,n)$ if and only if $q^l \equiv -1 \mod n$ for some integer l (see [4, 9]).

Theorem 5.5. *Let $\mathcal{C}$ be a cyclic code of length n over R with even index of nilpotency t. There exists a non-trivial self-dual code of length n over R if and only if $q^i \not\equiv -1 \mod n$, for all positive integers i.*

Proof. Assume that there exists a non-trivial self-dual code $\mathcal{C}$ over R such that $\mathcal{C} = \oplus_{i=0}^{l-1}\gamma^{r_i}\theta_i R[x]$, with $0 \le r_0 < r_1 < ... < r_{l-1} < t$, then by previous theorem, there exists $\theta_i \in \{\theta_0, ..., \theta_{l-1}\}$ such that θ_i and θ_i^* are not associated. We can write θ_i in the form $\theta_i = \sum_{\substack{j\in J\\ J\subset I}} e_j$, where $(e_j)_{j\in J}$ is a subset of the complete set of primitive pairwise orthogonal idempotents of $R[x]$. Since θ_i and θ_i^* are not associated, then e_j and e_j^* are not associated $\forall\ j \in J$. From Theorem 4.4, there exists $u_i \in R[x]$ such that $e_j = u_j(x)\hat{f}_j(x)$. Then e_j and e_j^* are associated if and only if $\hat{f}_j$ and $\hat{f}_j^*$ are associated if and only if f_j and f_j^* are associated. But f_j and f_j^* are associated if and only if $C_q(j,n) = C_q(n-j,n)$ if and only if $q^k \equiv -1 \mod n$ for some integer k. □

The following result characterizes non-trivial cyclic self-dual codes over R of odd or oddly even length.

Theorem 5.6 ([1] Theorem 4.6)**.**
Let n be an odd integer and R be a finite chain ring with even index of nilpotency t. There exists non-trivial cyclic self-dual codes of length n or $2n$ over R if and only if the multiplicative order of q modulo n is odd.

The following two results are consequences of Theorem 5.5 and Theorem 5.6.

Proposition 5.7 ([4], Corollary 4.6)**.**
Let R be a finite chain ring with even index of nilpotency t and residue field $\mathbb{F}_{p^r}$. If n is prime, then non-trivial self-dual codes of length n do not exist in the following cases:

- $p = 2,\ n \equiv 3, 5 \mod 8$;
- $p = 3,\ n \equiv 5, 7 \mod 12$;
- $p = 5,\ n \equiv 3, 7, 13, 17 \mod 20$;
- $p = 7,\ n \equiv 5, 11, 13, 15, 17, 23 \mod 28$;
- $p = 11,\ n \equiv 3, 13, 15, 17, 21, 23, 27, 29, 31, 41 \mod 44$.

Proposition 5.8 ([1], Corollary 4.8 and 4.9)**.**
Let R be a finite chain ring with even index of nilpotency t and residue field $\mathbb{F}_{p^r}$.

(1) *Let $n = \prod_{i=1}^{s} p_i^{k_i}$ be the prime factorization of an odd integer n. If q is a quadratic residue of $p_i^{k_i}$ and $p_i \equiv -1 \mod 4$, $\forall\ 1 \leq i \leq s$; then there exists a non-trivial self-dual code of length n over R.*

(2) *Let n be an odd prime integer such that $n \equiv -1 \mod 4$. Then there exists a non-trivial self-dual code of length n over R if and only if p is a quadratic residue of n^k; for k a non-zero positive integer.*

6. Self-dual negacyclic codes

Note that if n is odd, then there exists a one-to-one correspondence between cyclic and negacyclic codes of length n over R (see [2], Theorem 4.3 or [4], Proposition 5.1). For this reason, we only consider negacyclic codes of even length. The following result and its proof are similar to Theorem 5.3.

Theorem 6.1. *Under the same assumptions as the Theorem 4.4, let $\mathcal{C}$ be a negacyclic code of even length n over R with index of nilpotency t, such that*

$$\mathcal{C} = \oplus_{i=0}^{l-1} \gamma^{r_i} \theta_i R[x],$$

with $0 \leq r_0 < r_1 < ... < r_l = t$.

i) If t is even, there exists a non-trivial self-dual code over R if and only if there exists an idempotent $\theta_i \in \{\theta_0, ..., \theta_{l-1}\}$ such that θ_i and θ_i^* are not associated.

ii) If t is odd, there exists a negacyclic self-dual code over R if and only if θ_i and θ_i^* are not associated for all $\theta_i \in \{\theta_0, ..., \theta_{l-1}\}$.

Since $X^n + 1 = (X^{2n} - 1)/(X^n - 1)$, then $X^n + 1$ can be factored uniquely into monic irreducible pairwise coprime polynomials as follows (see [7]):

$X^n + 1 = \prod_{i \in I_{2n} \cap O_{2n}} f_i(X)$ with $f_i = \prod_{i \in C_q(i,2n) \cap O_{2n}} (X - \xi_{2n}^i)$, where I_{2n} is a complete set of representatives of cyclotomic cosets modulo $2n$, O_{2n} is the set of odd integers from 1 to $2n - 1$ and ξ_{2n} is a $2nth$-root of unity. Similarly to Theorem 5.5, we have the following result.

Theorem 6.2. *Let $\mathcal{C}$ be a negacyclic code of even length n over R. There exists a non-trivial negacyclic self-dual code over R if and only if $q^i \not\equiv -1 \mod 2n$, for all positive integers i.*

References

1. A. Batoul, K. Guenda, T. A. Gulliver, *On self-dual cyclic codes over finite chain rings*, Des. Codes Cryptogr. **70** (2014), 347-358.
2. A. Batoul, K. Guenda, T. A. Gulliver, *Some constacyclic codes over finite chain rings*, Adv. Math Commun. **10** (2016), 683-694.
3. A. R. Calderbank, N. J. A. Sloane, *Modular and p-adic codes*, Des. Codes Cryptogr. **6** (1995), 21-35.
4. H. Q. Dinh, S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50**, (2004), 1728-1744.
5. S. T. Dougherty, Y. H. Park, *On modular cyclic codes*, Finite Fields Appl. **13** (2007), 31-57.
6. K. Guenda, T. A. Gulliver, *MDS and self-dual codes over rings*, Finite Fields Appl. **18** (2012), 1061-1075.
7. X. Kai, S. Zhu, *Negacyclic self-dual codes over finite chain rings*, Des. Codes Cryptogr. **62** (2012), 161-174.
8. X. Kai, S. Zhu, Y. Tang, *Some constacyclic self-dual codes over integers modulo* 2^m, Finite Fields Appl. **18** (2012), 258-270.
9. P. Kanwar, S. R. López-Permouth, *Cyclic codes over the integers modulo* p^m, Finite Fields Appl. **3** (1997), 334-352.
10. T. Y. Lam, A First Course in Noncommutative Rings, Graduate Texts in Math., Vol. 131, Springer-Verlag, Berlin-Heidelberg-New York , 1991.
11. E. Martínez-Moro, I. F. Rúa, *Multivariable Codes Over Finite Chain Rings: Serial Codes*, SIAM J. Discrete Math., **20** (2006), 947-959.
12. B. R. McDonald, Finite Rings with Identity, Marcel Dekker, New York, 1974.
13. G. H. Norton, A. Salagean, *On the structure of linear and cyclic codes over a finite chain ring*, Appl. Algebra Eng. Commun. Comput. **10** (2000), 489-506.
14. J. H. van Lint, Introduction to Coding Theory, Graduate Texts in Math., Vol. 86, Springer-Verlag, Berlin-Heidelberg, 1999.

[1] Department of Mathematics, Faculty of Sciences Dhar-Mahraz, University Sidi Mohamed Ben Abdellah, Fez-Atlas, 30003, Morocco

Email address: mcharkani@gmail.com

[2] Department of Mathematics, University Joseph Ki-Zerbo, Ouagadougou, Burkina-Faso

Email address: jokabore@yahoo.fr