Finite Fields and Their Applications 79 (2022) 101993

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On LCD, self dual and isodual cyclic codes over finite chain rings [☆]

Amel Benyettou [a], Aicha Batoul [a], Cristina Fernández-Córdoba [b,*]

[a] *Faculty of Mathematics USTHB, University of Science and Technology of Algiers, Algeria*
[b] *Department of Information and Communication Engineering, University Autonomous of Barcelona, Spain*

A R T I C L E   I N F O

Article history:
Received 24 May 2021
Received in revised form 21 December 2021
Accepted 28 December 2021
Available online 13 January 2022
Communicated by W. Cary Huffman

MSC:
94B25
94B60

Keywords:
LCD
Isodual
Self dual
Cyclic codes
Finite chain rings

A B S T R A C T

In this paper, LCD cyclic, self dual and isodual codes over finite chain rings are investigated. It was proven recently that a non-free LCD cyclic code does not exist over finite chain rings. Based on algebraic number theory, we introduce necessary and sufficient conditions for which all free cyclic codes over a finite chain ring are LCD. We have also obtained conditions on the existence of non trivial self dual cyclic codes of any length when the nilpotency index of the maximal ideal of a finite chain ring is even. Further, several constructions of isodual codes are given based on the factorization of the polynomial $x^n - 1$ over a finite chain ring.

[☆] This work has been partially supported by the Spanish MINECO under Grant PID2019-104664GB-I00 (AEI/FEDER, UE).

[*] Corresponding author.

E-mail addresses: benyettouamel@yahoo.fr (A. Benyettou), a.batoul@hotmail.fr (A. Batoul), cristina.fernandez@uab.cat (C. Fernández-Córdoba).

https://doi.org/10.1016/j.ffa.2022.101993

1. Introduction

Codes over finite rings were studied in the early 1970s, and this study has grown enormously since the seminal work of Hammons et al. [11], where it is shown in that some of the best nonlinear codes over $\mathbb{F}_2$ can be viewed as linear codes over $\mathbb{Z}_4$.

Linear complementary dual or LCD codes are linear codes that intersect with their dual trivially. LCD cyclic codes have applications in data storage. Due to a newly discovered application in cryptography [6,9], interest in LCD codes has increased again.

An LCD code defined over a finite field $\mathbb{F}_q$ which is also known as reversible code was first introduced by Massey in [17]. Following his first study, Massey also showed the existence of asymptotically good LCD codes. Furthermore, Yang and Massey in [20] provided a necessary and sufficient condition under which a cyclic code has a complementary dual. In [15], Liu and Liu studied LCD codes over finite chain rings and provided a necessary and sufficient condition for a free linear code to be LCD. In [14], Lina and Nocon give parameters of some LCD codes using generator matrices and give some methods to construct new LCD from previous ones. Recently, in [5], existence conditions are given for LCD codes over $\mathbb{F}_2$ which are images under the Gray map of additive codes over $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$. Finally, in [7], the authors proved that there are no non-free LCD codes over finite commutative local Frobenius rings. It was also shown that a free cyclic code C over any finite chain ring is LCD code if and only if C is reversible when the length n of the code is relatively prime to the characteristic of a finite chain ring. Several types of equivalence between codes can be defined, but here we only consider monomial equivalence. Two codes C and C' are called monomially equivalent if there exists a monomial permutation which sends C to C'. Isodual codes are codes which are monomially equivalent to their duals. The class of isodual codes is important in coding theory because it contains the self dual codes as a subclass. In addition, isodual codes are contained in the larger class of formally self dual codes. In [1,3,4] the authors gave some specific constructions of self dual and isodual codes over finite fields and finite chain rings. The purpose of this paper is to examine linear codes with complementary duals and isodual codes over finite chain rings. We give necessary and sufficient conditions for which all codes are LCD, and generalize the result given in [2] by giving condition on the existence of non trivial self dual codes. Some of the codes obtained are both isodual and LCD, and so are called LCD-isodual codes. The paper is organized as follows, the necessary background material on codes over finite chain rings is given in Section 2. In Section 3, we give the first part of the main results of this paper. Based on algebra number theory properties, we provide conditions under which all free cyclic codes over finite chain rings are LCD. In Section 4, we generalize the result given in [2] of the existence of non trivial self dual codes when the nilpotency index of the maximal ideal of the finite chain ring considered is even. In Section 5, the structure of cyclic codes of length $2^a m$ over finite chain rings is given along with conditions on the existence of isodual cyclic codes. Using these results, several constructions of isodual are given.

2. Preliminaries

We begin with some definitions and properties about finite chain rings. Let R be a finite commutative ring with identity. A commutative ring is called a chain ring if the lattice of all its ideals is a chain. It is well known that if R is a finite chain ring, then R is a principal ideal ring and it has a unique maximal ideal $\langle\gamma\rangle$. Its chain of ideals is

$$\{0\} = \langle\gamma^e\rangle \subsetneq \langle\gamma^{e-1}\rangle \subsetneq \ldots \subsetneq \langle\gamma\rangle \subsetneq R,$$

where $\langle\gamma^i\rangle$ (with $i \in \{1,\cdots,e\}$) is the ideal of R generated by γ^i. The integer e is called the nilpotency index of $\langle\gamma\rangle$. The nilradical of R is $\langle\gamma\rangle$, so all the elements of $\langle\gamma\rangle$ are nilpotent. Therefore, the elements of $R\backslash\langle\gamma\rangle$ are units. We denote this group by R^*. Since $\langle\gamma\rangle$ is maximal, the residue ring $R/\langle\gamma\rangle$ is a field with q elements which we denote by $\mathbb{F}_q$.

Let $|R|$ denote the cardinality of R, then $|R| = |\mathbb{F}_q| \cdot |\langle\gamma\rangle| = |\mathbb{F}_q| \cdot |\mathbb{F}_q|^{e-1} = |\mathbb{F}_q|^e = q^e$. Moreover, from [19],

$$|\langle\gamma^i\rangle| = |\mathbb{F}_q|^{e-i} = q^{e-i} \text{ for } i = 1,2,\ldots,e-1$$

The natural surjective ring morphism is given by

$$\begin{aligned} - : R &\longrightarrow \mathbb{F}_q \\ a &\longmapsto \bar{a} = a \bmod \gamma \end{aligned} \tag{1}$$

The map given in (1) extends naturally to a map from $R[x] \longrightarrow \mathbb{F}_q[x]$. A polynomial $f(x)$ of $R[x]$ is called basic irreducible if $\overline{f(x)}$ is irreducible in $\mathbb{F}_q[x]$. Two polynomials $f_1(x)$ and $f_2(x)$ in $R[x]$ are called coprime if $\langle f_1(x)+f_2(x)\rangle = R[x]$ or equivalently there exist $\lambda_1(x)$ and $\lambda_2(x)$ in $R[x]$ such that $\lambda_1(x)f_1(x)+\lambda_2(x)f_2(x) = 1$. A polynomial $f(x)$ of $R[x]$ is a unit if and only if $\overline{f(x)}$ is a unit and also f is a zero divisor if and only if $\overline{f(x)} = 0$. Hensel's lemma is an important tool for studying finite chain rings, which can lift the factorization into a product of pairwise coprime polynomials over $\mathbb{F}_q$ to such factorization over R.

Lemma 1. *[18, Hensel lifting, Theorem XIII.4] Let $g(x)$ in $R[x]$ be monic. Assume that there are monic, pairwise coprime polynomials $f_1(x), f_2(x), \ldots, f_k(x)$ in $\mathbb{F}_q[x]$ such that $\overline{g(x)} = \prod_{i=1}^{i=k} f_i(x)$, then there are monic pairwise coprime polynomials $g_1(x), g_2(x), \ldots, g_k(x)$ in $R[x]$ such that $g(x) = \prod_{i=1}^{i=k} g_i(x)$ and $\overline{g_i(x)} = f_i(x)$, for all $0 \le i \le k$.*

Lemma 2. *[19, Theorem 2.7] If $f(x)$ is a monic polynomial over R such that $\overline{f(x)}$ is square free, then $f(x)$ factors uniquely as product of monic basic irreducible pairwise coprime polynomials.*

Let R be a finite chain ring, $\mathbb{F}_q$ its residue field, and $\langle \gamma \rangle$ its maximal ideal with nilpotency index e. A linear code C of length n over R is a submodule of R^n. A linear code C of length n over R is called cyclic if $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is in C whenever $(c_0, c_1, \ldots, c_{n-1})$ is in C. Each codeword c where $c = (c_0, c_1, ..., c_{n-1})$ is customarily identified with its polynomial representation $c(x)$ where $c(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}$. In this way, any cyclic code of length n over R is identified with exactly one ideal of the ring $R[x]/\langle x^n - 1 \rangle$ and $xc(x)$ correspond to a cyclic shift of $c(x)$.

A monomial transformation over R^n is an R-linear homomorphism τ such that there exist scalars $\lambda_1, \lambda_2, ..., \lambda_n$ in R^* and a permutation σ in S_n, where S_n is the group of permutation of $\{1, 2, ..., n\}$, such that for all $(x_1, x_2, ..., x_n)$ in R^n, we have

$$\tau(x_1, x_2, ..., x_n) = (\lambda_1 x_{\sigma(1)}, \lambda_2 x_{\sigma(2)}, ..., \lambda_n x_{\sigma(n)}).$$

Recall that two codes are called equivalent if there is a monomial permutation which sends one to the other. In this paper, whenever we say that two codes are equivalent, we mean that they are monomially equivalent. Suppose that $f(x) = a_0 + a_1 x + ... + a_r x^r$ is a polynomial of $R[x]$ of degree r such that $f(0) = a_0$ is a unit in R. The monic reciprocal polynomial of $f(x)$ is defined by $f^*(x) = f(0)^{-1} x^r f(x^{-1})$. If $f^*(x) = f(x)$, the polynomial $f(x)$ is called self reciprocal.

A code C over R is reversible if for each code word $(c_0, c_1, ..., c_{n-1})$ in C implies that the code word $(c_{n-1}, c_{n-2}, ..., c_0)$ is also in C. It is known that a cyclic code C is reversible if and only if its generator polynomial is self reciprocal. We attach the standard inner product to R^n

$$x \cdot y = \sum_{i=1}^{n} x_i y_i, \text{ for each } x = (x_1, x_2, ..., x_n) \text{ and } y = (y_1, y_2, ..., y_n) \text{ in } R^n.$$

The Euclidean dual code $C^\perp$ of C is defined as

$$C^\perp = \{x \in R^n : \forall y \in C; x \cdot y = 0\}.$$

A code C is said to be self dual if $C = C^\perp$, it is isodual if $C = \tau(C^\perp)$, where τ is a monomial transformation, and it is called LCD or linear complementary dual if $C \cap C^\perp = \{0\}$.

A code C over a finite chain ring and its dual satisfies the following

$$|C||C^\perp| = q^{en} = |R|^n \text{ and } (C^\perp)^\perp = C.$$

The following theorem gives the structure of a cyclic code and its dual over a finite chain ring.

Lemma 3. *[8, Theorem 3.8] Let R be a finite chain ring with maximal ideal γ with nilpotency index e and residue field $\mathbb{F}_q$. Let C be a cyclic code over R of length n such that $\gcd(n, q) = 1$, where p is the characteristic of $\bar{R}$. Then there exists a unique family of pairwise coprime polynomials $F_i(x), 0 \leq i \leq e$ in $R[x]$ satisfying $F_0(x)F_1(x)...F_e(x) = x^n - 1$ such that*

$$C = \left\langle \hat{F}_1(x), \gamma\hat{F}_2(x), ..., \gamma^{e-1}\hat{F}_e(x) \right\rangle, C^{\perp} = \left\langle \hat{F}_0^*(x), \gamma\hat{F}_e^*(x), ..., \gamma^{e-1}\hat{F}_2^*(x) \right\rangle,$$

where $\hat{F}_i(x) = \dfrac{x^n - 1}{F_i(x)}$ for $0 \leq i \leq e$. Moreover, we have that the ring $R[x]/\langle x^n - 1\rangle$ is a principal ideal ring.

In particular, when the code is free as a submodule, we have the following statement.

Lemma 4. *[10, Theorem 4.16] Let C be a cyclic code of length n over a finite chain ring R with residue field $\mathbb{F}_q$ such that $\gcd(n, q) = 1$. Then, C is a free cyclic code with rank k if and only if there is a monic polynomial $f(x)$ in $R[x]$ such that $f(x)$ divides $x^n - 1$ and $f(x)$ generates C. In this case, we have $k = n - deg(f)$. Further the dual code of C is also free and it is generated by $\left\langle \left(\dfrac{x^n - 1}{f(x)}\right)^* \right\rangle$.*

3. On LCD cyclic codes over finite chain rings

The aim of this section is to present some new constructions of LCD cyclic codes, and provide necessary and sufficient conditions for the existence of non trivial LCD cyclic codes over finite chain rings.

Let n be a positive integer and q a prime power coprime to n. We denote by $ord_n(q)$ the multiplicative order of q modulo n. This is the smallest integer l such that $q^l \equiv 1 \mod n$.

To process cyclic codes of length n, we have to study the factorization into irreducible polynomials of $x^n - 1$ over $\mathbb{F}_q$. To this end, we need to introduce the q-cyclotomic cosets modulo n. Note that $x^n - 1$ has no repeated factors over $\mathbb{F}_q$ if and only if $gcd(n, q) = 1$. For any s in $\{0, 1, 2, ..., n - 1\}$, the q-cyclotomic coset of s modulo n is defined by

$$C_s = \left\{s, sq, sq^2, ..., sq^{l_s - 1}\right\},$$

where l_s is the smallest positive integer such that $s \equiv sq^{l_s} (\mod n)$, and is the size of the q-cyclotomic coset. The smallest integer in C_s is called the coset leader of C_s. Let $P_{n,q}$ be the set of all the coset leaders. We have then $C_s \cap C_t = \emptyset$ for any two distinct elements s and t in $P_{n,q}$, and

$$\bigcup_{s \in P_{n,q}} C_s = \{0, 1, 2, ..., n - 1\}.$$

Hence, the distinct q-cyclotomic cosets modulo n partition $\{0, 1, 2, ..., n-1\}$.

The cyclotomic coset C_s is said to be reversible if and only if $C_{n-s} = C_s$ if and only if $n-s$ is in C_s.

Lemma 5. *[2, Lemma 4] If C_1 is reversible then C_s is reversible for all s in $P_{n,q}$.*

Let $r = ord_n(q)$, and let α be a generator of $(\mathbb{F}_{q^r})^*$. Put $\beta = \alpha^{\frac{q^r-1}{n}}$, then β is a primitive n-th root of unity in $\mathbb{F}_{q^r}$. The minimal polynomial $m_s(x)$ of β^s for s in $P_{n,q}$ over $\mathbb{F}_{q^r}$ is given by

$$m_s(x) = \prod_{j \in C_s} \left(x - \beta^j\right),$$

which is irreducible over $\mathbb{F}_q$, and hence the factorization of $x^n - 1$ into irreducible factors over $\mathbb{F}_q$ is given by

$$x^n - 1 = \prod_{s \in P_{n,q}} m_s(x).$$

The following lemma is well known in literature.

Lemma 6. *[13, Lemma 5] The minimal polynomial $m_s(x)$ is self reciprocal if and only if the cyclotomic coset associated C_s is reversible.*

3.1. Some properties of positive integers

In this section, we give some properties of positive integers which will be needed later.

Lemma 7. *Let q be a prime power, p an odd prime number coprime to q, then we have*

(i) *If $ord_p(q)$ is even then for all k in $\mathbb{N}^*$, $ord_{p^k}(q)$ is even.*
(ii) *If there is k in $\mathbb{N}^*$ such that $ord_{p^k}(q)$ is even, then $ord_p(q)$ is also even.*

Proof. Since p divides p^k, we have $q^{ord_{p^k}(q)} \equiv 1 \mod p^k$ implies that $q^{ord_{p^k}(q)} \equiv 1 \mod p$. Hence $ord_p(q) \mid ord_{p^k}(q)$, therefore if $ord_p(q)$ is even then $ord_{p^k}(q)$ is even too.

To prove (ii), assume that there is k in $\mathbb{N}^*$ such that $ord_{p^k}(q)$ is even, and by way of contradiction we suppose that $ord_{p^{k-1}}(q)$ is odd. Therefore, there exist some integer i and there exists m in $\mathbb{N}$, such that $q^{2i+1} = 1 + mp^{k-1}$. Since p is a prime number, it divides the binomial coefficient $\binom{p}{j}$ for all $1 \leq j \leq p-1$. Hence we get $(q^{2i+1})^p = \left(1 + mp^{k-1}\right)^p \equiv 1 \mod p^k$. It follows that $ord_{p^k}(q) \mid (2i+1)p$. Since $(2i+1)p$ is odd, this leads to a contradiction. So that $ord_{p^{k-1}}(q)$ must be even, and by descending recurrence we get that $ord_p(q)$ is even. □

Lemma 8. *Let q be a prime power and p an odd prime number such that $gcd(p,q)=1$. The three following statements are equivalents.*

(i) *There exits l in $\mathbb{N}$, such that $q^l \equiv -1 \mod p$.*
(ii) *For all k in $\mathbb{N}$, there exists l_k in $\mathbb{N}$, such that $q^{l_k} = -1 \mod p^k$.*
(iii) *There is i in $\mathbb{N}^*$ such that $ord_{p^i}(q)$ is even.*

Further, if $q^l \equiv -1 \mod p$, then $l = \frac{1}{2}(1+2m)ord_p(q)$ for some m in $\mathbb{N}$.

Proof. Suppose that (i) is satisfied and we prove (ii) by induction. For $k=1$ we have $q^l \equiv -1 \mod p$. Assume $q^{l_{k-1}} \equiv -1 \mod p^{k-1}$ for $k \geq 2$. Since p is odd, we can write

$$\sum_{i=0}^{p^{k-1}-1}(-q^{l_{k-1}})^i = \frac{(-q^{l_{k-1}})^{p^{k-1}}-1}{(-q^{l_{k-1}})-1} = \frac{q^{l_{k-1}p^{k-1}}+1}{q^{l_{k-1}}+1}.$$

On the other hand, we have

$$\sum_{i=0}^{p^{k-1}-1}(-q^{l_{k-1}})^i = \sum_{i=0}^{p^{k-1}-1}(-1)^i(q^{l_{k-1}})^i \equiv \sum_{i=0}^{p^{k-1}-1}(-1)^i(-1)^i \mod p^{k-1} \equiv 0 \mod p^{k-1},$$

which means that $p^{k-1} \mid \sum_{i=0}^{p^{k-1}-1}(-q^{l_{k-1}})^i$. Since $p \mid p^{k-1} \mid q^{l_{k-1}}+1$, it follows that

$$p^k \mid (q^{l_{k-1}}+1)(\sum_{i=0}^{p^{k-1}-1}(-q^{l_{k-1}})^i) = q^{l_{k-1}p^{k-1}}+1.$$

Thus, for $l_k = l_{k-1}\cdot p^{k-1}$, we have that $q^{l_k} \equiv -1 \mod p^k$. Note that when $q^l \equiv -1 \mod p$, then $l_k = l_{k-1}\cdot p^{k-1} = l_{k-2}\cdot p^{k-2}\cdot p^{k-1}$. We obtain that $l_k = l \cdot p^{\frac{k(k-1)}{2}}$.

Conversely, if the statement (ii) holds, then the statement (i) follows immediately for $k=1$.

Assume that (iii) is satisfied. Lemma 7 shows that the integer $ord_p(q)$ is also even. We have, $q^{ord_p(q)} \equiv 1 \mod p$ if and only if $p \mid (q^{\frac{1}{2}ord_p(q)}-1)(q^{\frac{1}{2}ord_p(q)}+1)$. Since p is prime it must divide one of the factors and it can not divide $(q^{\frac{1}{2}ord_p(q)}-1)$ because of the definition of the order of q, thus $q^{\frac{1}{2}ord_p(q)} = -1 \mod p$.

Conversely, if (ii) is satisfied, then by Lemma 8 there exits l in $\mathbb{N}^*$ such that $q^l \equiv -1 \mod p$, which means $q^{2l} \equiv 1 \mod p$, so that $ord_p(q) \mid 2l$. If $ord_p(q)$ is odd, then $ord_p(q) \mid l$, which contradicts the fact that $q^l \equiv -1 \mod p$. Hence $ord_p(q)$ must be even and (iii) holds.

It remains to prove that if there exists an integer l such that $q^l \equiv -1 \mod p$, then $l = \frac{1}{2}(1+2m)ord_p(q)$ for some m in $\mathbb{N}$. By definition of order, the integers $q^{ord_p(q)}$ and q^j are distinct for all $1 \leq j \langle ord_p(q)$. Since p is odd, we obtain that if l' is the smallest integer such that $q^{l'} \equiv -1 \mod p$, then on the one hand $1 \leq l' \langle ord_p(q)$ and, on the other hand, $ord_p(q) \mid 2l'$. This gives $2l' = \lambda ord_p(q)$ and $\lambda \geq 1$. Since $l' \langle ord_p(q)$, then $l' = \frac{1}{2} ord_p(q)$. Further, if l is an integer that satisfies $q^l \equiv -1 \mod p$, then by division algorithm we can write $l = sl' + r$ with $r \langle l'$. Hence, we get

$$q^l = q^{sl'+r} = (q^{l'})^s q^r \equiv (-1)^s q^r \mod p \equiv -1 \mod p.$$

Which forces that s is odd and $r = 0$. Thus,

$$l = (2m+1)l' = \frac{1}{2}(2m+1) ord_p(q). \quad \square$$

Corollary 1. *Let q be a prime power and p an odd prime number coprime to q. Let a be a positive integer such that $2^a \| ord_p(q)$. Then for all $k \in \mathbb{N}^*$ we have $2^a \| ord_{p^k}(q)$, where the notation $2^a \| ord_p(q)$ means that $2^a | ord_p(q)$ but $2^{a+1} \nmid ord_p(q)$.*

Proof. Let a be a positive integer such that $2^a \| ord_p(q)$. From Lemma 8, there exists l in $\mathbb{N}^*$, such that $q^l \equiv -1 \mod p$ and $l = \frac{1}{2}(1+2m) ord_p(q)$ for some m in $\mathbb{N}$. On the other hand, since $ord_p(q)$ is even, then $ord_{p^k}(q)$ is also even for all $k \in \mathbb{N}^*$. Hence, from Lemma 8 again, there exists l_k in $\mathbb{N}^*$, such that $q^{l_k} \equiv -1 \mod p^k$ and $l_k = \frac{1}{2}(1+2m_k) ord_{p^k}(q)$ for some m_k in $\mathbb{N}$. From the proof of Lemma 8, we have that $l_k = l \cdot p^{\frac{k(k-1)}{2}}$. Therefore

$$l_k = \frac{1}{2}(1+2m_k) ord_{p^k}(q) = \frac{1}{2}(1+2m) ord_p(q) \cdot p^{\frac{k(k-1)}{2}}.$$

Since $(1+2m)p^{\frac{k(k-1)}{2}}$ and $(1+2m_k)$ are both odd, we conclude that $2^a \| ord_{p^k}(q)$. $\square$

3.2. New constructions of LCD cyclic codes over finite chain rings

Recall that a cyclic code is an LCD code if it satisfies $C \cap C^{\perp} = \{0\}$. It was shown recently in [7] that non-free LCD code don't exist over finite commutative chain rings.

Lemma 9. *[7, Theorem 2] Over finite commutative chain rings, any LCD code is free.*

In [7] again, Bhowmick et al., generalized the characterization of LCD codes on finite chain rings.

Lemma 10. *[7, Theorem 6] Let C be a cyclic code over a finite chain ring R with residue field $\mathbb{F}_q$ of length n such that $\gcd(n,q) = 1$. Let g be a generator polynomial of C. Then C is an LCD code if and only if C is reversible if and only if the polynomial g is self reciprocal.*

Liu and Wang generalized Massey's criterion [20] for LCD codes over any finite field of any length to finite chain rings.

Lemma 11. *[16, Theorem 25] A cyclic code C of length n over a finite chain ring R with the residue field $\mathbb{F}_q$ is an LCD code if and only if $C = \langle g(x)\rangle$, where $g(x)$ is a monic divisor of $x^n - 1$ such that $g(x) = g^*(x)$, and $g(x)$ and $(x^n - 1)/g(x)$ are coprime.*

Let $q = p^s$ and $n = mp^r$, where $gcd(m, p) = 1$. Thus the polynomial $x^m - 1$ is a monic square free, hence it factors uniquely as a product of pairwise coprime monic irreducible polynomials $f_1(x), ..., f_l(x)$. Hence the factorization of $x^n - 1$ over $\mathbb{F}_q$ is given by

$$x^n - 1 = x^{mp^r} - 1 = (x^m - 1)^{p^r} = f_1(x)^{p^r} ... f_l(x)^{p^r} \tag{2}$$

Denote the factors $f_i(x)$ in the factorization of $x^m - 1$ which are self reciprocal by $g_1(x), ...g_s(x)$, and the remaining $f_j(x)$ grouped in pairs by $h_1(x), h_1^*(x), ..., h_t(x), h_t^*(x)$. Hence $l = s + 2t$, and the factorization given in (2) becomes

$$x^n - 1 = g_1(x)^{p^r} g_2(x)^{p^r} ... g_s(x)^{p^r} h_1(x)^{p^r} h_1^*(x)^{p^r} ... h_t(x)^{p^r} h_t^*(x)^{p^r}$$

Using Hensel's Lemma and the properties of the reciprocal polynomial, we get a factorization of $x^n - 1$ over R, which is given by

$$x^n - 1 = G_1(x)G_2(x)...G_l(x)H_1(x)H_1^*(x)...H_t(x)H_t^*(x),$$

where $G_i(x), H_j(x)$ are monic coprime polynomials such that $\overline{G_i(x)} = g_i^{p^r}(x), \overline{H_j(x)} = h_j^{p^r}(x)$.
By Lemma 11, we obtain a characterization of LCD codes over finite chain rings. Those are codes generated by

$$C = \left\langle G_1(x)^{k_1} G_2(x)^{k_2} ... G_l(x)^{k_l} H_1(x)^{r_1} H_1^*(x)^{r_1} ... H_t(x)^{r_t} H_t^*(x)^{r_t} \right\rangle,$$

where $k_i, r_j \in \{0, 1\}$ for all $1 \leq i \leq l,\ 1 \leq j \leq t$.
Now, using the algebraic properties of integers given in the section 3.1, and according to the decomposition of n into product of powers of prime numbers, we give some new constructions of LCD codes over R.

Theorem 1. *Let R be a finite chain ring with residue field $\mathbb{F}_q$, and p^k an odd prime power coprime to q. Then, all free cyclic codes of length p^k over R are LCD if and only if $ord_p(q)$ is even.*

Proof. Let p^k be an odd prime power coprime to q. From Lemma 10 we have that a cyclic code C is an LCD code if it is generated by a self reciprocal polynomial $g(x)$ which divide $x^{p^k} - 1$. On the other hand, Lemma 8 shows that if $ord_p(q)$ is even, then there exits l in $\mathbb{N}^*$, such that $q^l \equiv -1 \mod p^k$, which means that -1 is in the cyclotomic coset C_1. Hence, $C_1 = C_{-1} \mod p^k$. In other words, C_1 is reversible, and so all the other cyclotomic cosets are also reversible by Lemma 5. Therefore, all divisors of $x^{p^k}-1$ are self reciprocal.

Conversely, assume that all free cyclic codes of length p^k are LCD, then all divisors of $x^{p^k}-1$ are self reciprocal. Hence all cyclotomic cosets are reversible and, in particular, the cyclotomic coset C_1 is reversible. This means that there is an integer l such that $q^l \equiv -1 \mod p^k$. Finally, Lemma 8 shows that in such case $ord_p(q)$ is even. □

Example 1. Let $R=\mathbb{Z}_9$ with residue field $\mathbb{F}_3$ and $n=49$. We have $ord_7(3)=6$ and the factorization into irreducible polynomials is given by:

$$\begin{aligned} x^{49}-1 &= (x+8)(x^6+x^5+x^4+x^3+x^2+x+1)(x^{42}+x^{35}+x^{28}+x^{21}+x^{14}+x^7+1) \\ &= g_1(x)g_2(x)g_3(x) \end{aligned}$$

So, all codes generated by $\left\langle \prod_{i=1}^{3} g_i^{k_i}(x) \right\rangle$, where $0 \le k_i \le 1$, are LCD codes over $\mathbb{Z}_9$ of length 49.

Example 2. Let $R=\mathbb{Z}_4$, $n=17$, we have

$$\begin{aligned} x^{17}-1 &= (x+3)(x^8+2x^6+3x^5+x^4+3x^3+2x^2+1)(x^8+x^7+3x^6+3x^4+3x^2+x+1) \\ &= g_1(x)g_2(x)g_3(x), \end{aligned}$$

and it is easy to see that $g_1(x), g_2(x)$ and $g_3(x)$ are monic basic-irreducible over $\mathbb{Z}_4$. Since $ord_{17}(2)=8$, then all cyclic codes generated by polynomials of the form $\left\langle \prod_{i=1}^{3} g_i^{k_i}(x) \right\rangle$, with $0 \le k_i \le 1$, are LCD codes.

Lemma 12. *Let q and n be positive integers coprime such that n is odd and the irreducible factorization of n is given by $n=p_1^{k_1}p_2^{k_2}...p_t^{k_t}$, with $ord_{p_i}(q)$ even for $1 \le i \le t$. Let a_i be the positive integers for which $2^{a_i} \| ord_{p_i}(q)$, with $1 \le i \le t$. Then we have*

$$a_1=a_2=...=a_t=a \text{ if and only if } \text{ there exists } l \in \mathbb{N}^*, \text{ such that } q^l \equiv -1 \mod n.$$

Further, $2^a \| ord_n(q)$.

Proof. Assume that $a_1=a_2=...=a_t=a$. Recall that if $2^a \| ord_{p_i}(q)$ then $2^a \| ord_{p_i^{k_i}}(q)$ for all k_i in $\mathbb{N}$. Thus, we can write $ord_{p_i^{k_i}}(q)=2^a m_i$, with m_i an odd integer for $1 \le i \le t$. From Lemma 8 and Corollary 1, we deduce that there exits $l_i \in \mathbb{N}^*$, such that $q^{l_i} \equiv -1 \mod p_i^{k_i}$. The smallest integer l_i' satisfying this congruence is $l_i' = \frac{1}{2} ord_{p_i^{k_i}}(q) = 2^{a-1}m_i,$ for $1 \le i \le t$. Let $m=\prod_{i=1}^{t} m_i$. Since m is odd, we get $q^{2^{a-1}m} \equiv -1 \mod p_i^{k_i}$. Hence, $p_i^{k_i} \mid q^{2^{a-1}m}+1$ for all $1 \le i \le t$. Therefore, $n=\prod_{i=1}^{t} p_i^{k_i} \mid q^{2^{a-1}m}+1$. In other words $q^{2^{a-1}m} \equiv -1 \mod n$.

Conversely, assume there is an integer l such that $q^l \equiv -1 \mod n$. Without loss of generality, we suppose $a_1 \neq a_2$ such that $2^{a_1} \| ord_{p_1}(q)$ and $2^{a_2} \| ord_{p_2}(q)$. Write $ord_{p_1}(q) = 2^{a_1}m_1$ and $ord_{p_2}(q)=2^{a_2}m_2$ for odd integers m_1 and m_2. We have

$$q^l \equiv -1 \mod n \text{ implies } q^l \equiv -1 \mod p_i \text{ which give } q^{2l} \equiv 1 \mod p_i, \text{ for } 1 \leq i \leq t.$$

Hence, $2^{a_1}m_1 \mid 2l$ and $2^{a_2}m_2 \mid 2l$. Since both of a_1 and a_2 are not null, we get $2^{a_1-1}m_1 \mid l$ and $2^{a_2-1}m_2 \mid l$. Since $a_1 \neq a_2$, we can suppose that $a_1 \rangle a_2$. Consequently, $2^{a_2}m_2 \mid l$. In other words, $q^l \equiv 1 \mod p_2$, which is a contradiction.
Further, we have $n = p_1^{k_1}p_2^{k_2}...p_t^{k_t}$, so

$$ord_n(q) = lcm(ord_{p_1^{k_1}}(q), ord_{p_2^{k_2}}(q), ..., ord_{p_t^{k_t}}(q)) = 2^a(2k+1), \text{ for some } k \in \mathbb{N}$$

Thus, $2^a \| ord_n(q)$. □

Theorem 2. *Let R be a finite chain ring with residue field $\mathbb{F}_q$ and n an odd integer coprime to q such that the factorization of n is given by $n = p_1^{k_1}p_2^{k_2}...p_t^{k_t}$ with $k_i \in \mathbb{N}^*$ for $1 \leq i \leq t$. Assume that the numbers $ord_{p_i}(q), 1 \leq i \leq t$ are even and let $a_i \in \mathbb{N}^*$ such that $2^{a_i} \| ord_{p_i}(q)$. Then all free cyclic codes of length n over R are LCD if and only if $a_1 = a_2 = ... = a_t = a$.*

Proof. Assume that there is a positive integer a such that $2^a \| ord_{p_i}(q), 1 \leq i \leq t$. From Lemma 12, there exists an integer l such that $q^l \equiv -1 \mod n$. This means that the q cyclotomic coset C_1 is reversible. Hence, all the other cyclotomic cosets are reversible by Lemma 5. Thus all divisors of the polynomial $x^n - 1$ are self reciprocal. Therefore, all free cyclic codes of length n over R are LCD.

Conversely, suppose that all free cyclic codes are LCD. So that all divisors of $x^n - 1$ are self reciprocal. We deduce that all cyclotomic cosets are reversible. In particular C_1 is reversible. Hence -1 is a power of $q \mod n$. The desired result follows immediately from Lemma 12. □

As a corollary we construct LCD codes of oddly even length.

Corollary 2. *Let R be a finite chain ring with residue field $\mathbb{F}_q$ such that q is an odd integer. Let n be an oddly even integer coprime to q such that the irreducible factorization of n is given by $n = 2p_1^{k_1}p_2^{k_2}...p_t^{k_t}$ with k_i in $\mathbb{N}^*$ for $1 \leq i \leq t$. Assume that for all $1 \leq i \leq t$ the integers $ord_{p_i}(q)$ are even. Let a_i in $\mathbb{N}^*$ such that $2^{a_i} \| ord_{p_i}(q)$. Then $a_1 = a_2 = ... = a_t = a$ if and only if all free cyclic codes of length n over R are LCD.*

Proof. On the one hand and according to Lemma 12, we have $a_1 = a_2 = ... = a_t = a$ if and only if there exists l in $\mathbb{N}^*$, such that $\prod_{i=1}^{t} p_i^{k_i} \mid q^l + 1$. On the other hand, since q is an odd integer then $2 \mid q^l + 1$. Hence $n = 2\prod_{i=1}^{t} p_i^{k_i} \mid q^l + 1$. This means $q^l \equiv -1 \mod n$. Thus the cyclotomic coset C_1 is reversible, so according to Lemma 5 all the other cyclotomic cosets are reversibles. Hence, all free cyclic codes of length n are LCD codes.

Conversely, assume that all codes of length n are LCD. Then, the cyclotomic coset C_1 is reversible. Hence there is an integer l such that $q^l \equiv -1 \mod n$. It follows that $q^l \equiv -1 \mod \prod_{i=1}^{t} p_i^{k_i}$. Therefore, from Lemma 12, we get the desired result. □

Example 3. Let $R = \mathbb{Z}_{25}$, $n = 2646 = 2 \cdot 7^2 \cdot 3^3$. We have $ord_7(5) = 6$ and $ord_3(5) = 2$. Since $2 \| ord_7(5)$ and $2 \| ord_3(5)$, so all free cyclic codes of length 2646 are LCD codes.

In the remainder of this section, we provide necessary and sufficient conditions for cyclic codes to be LCD when the lengths are divisible by 4. The following lemmas are needed.

Lemma 13. *[12, Theorem 2'] The integer 2^k has primitive roots for $k = 1$ or 2 but not for $k \geq 3$. If $k \geq 3$, then $\{(-1)^a 5^b;\ a = 0, 1$ and $0 \leq b \leq 2^{k-2}\}$ constitutes a reduced residue system $\mod 2^k$. It follows that for $k \geq 3$, the group $(\mathbb{Z}/2^k\mathbb{Z})^*$ is not cyclic; it is the direct product of two cyclic groups, one of order 2, the other of order 2^{k-2}*

Lemma 14. *Let q be an odd prime power. Assume that there is an integer l in $\mathbb{N}^*$ such that $q^l \equiv -1 \mod 2^k$ with $k \geq 2$. Then $q \equiv -1 \mod 2^k$. Further, the integer l is odd and $ord_{2^k}(q) = 2$.*

Proof. Assume that there is an integer l such that $q^l \equiv -1 \mod 2^k$. If $k \rangle 2$, then from Lemma 13, q can be written as $q = (-1)^i \cdot 5^j$, with (i, j) in $\mathbb{N}^2$. Hence $q^l = (-1)^{il} \cdot 5^{jl} \equiv -1 \mod 2^k$, which requires that the integer il must be odd and that the order $ord_{2^k}(5)$ of the integer 5 which equal to 2^{k-2} must divide jl. Thus l is odd and then 2^{k-2} divides j. Write $j = 2^{k-2} \cdot j'$, we get

$$q = (-1)^i \cdot 5^j = (-1)^i \cdot 5^{2^{k-2}j'} \equiv (-1)^i \mod 2^k \equiv -1 \mod 2^k$$

For $k = 2$ and since q is odd we have clearly that $q^l \equiv -1 \mod 4$ leads to $q \equiv -1 \mod 4$. Hence l must be odd. Further, $q \equiv -1 \mod 2^k$ implies $ord_{2^k}(q) = 2$. □

Theorem 3. *Let R be a finite chain ring with residue field $\mathbb{F}_q$, and let n be a doubly even integer coprime to q such that the factorization of n is given by $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \ldots p_t^{k_t}$ with $k_i \in \mathbb{N}$ for all $1 \leq i \leq t$ and $k_0 \geq 2$. Then the following statements are equivalent:*

(i) $2 \| ord_{p_i}(q)$ *for* $1 \leq i \leq t$ *and* $2^{k_0} \mid q + 1$.
(ii) *All free cyclic codes over R of length n are LCD codes.*

Proof. Suppose that (i) is satisfied. Proving (ii) is equivalent to proving the existence of an integer l such that $q^l \equiv -1 \mod n$. The assumption $2 \| ord_{p_i}(q)$ and Corollary 1 give that $ord_{p_i^{k_i}}(q) = 2m_i$, with m_i odd . Using Lemma 8, we get $q^{m_i} \equiv -1 \mod p_i^{k_i}$. Therefore, $q^{\prod_{i=1}^t m_i} \equiv -1 \mod p_i^{k_i}$. Hence, there exists $l = \prod_{i=1}^t m_i$ an odd integer such that $q^l \equiv -1 \mod \prod_{i=1}^t p_i^{k_i}$. On the other hand, $q \equiv -1 \mod 2^{k_0}$ implies $q^l \equiv -1 \mod 2^{k_0}$. Consequently $n = 2^{k_0} \prod_{i=1}^t p_i^{k_i}$ divide $q^l + 1$. Thus $q^l \equiv -1 \mod n$.

Conversely, assume that all free cyclic codes over R are LCD. This means that all cyclotomic cosets are reversible and, in particular, the cyclotomic coset C_1. Hence there exists l in $\mathbb{N}^*$ such that $q^l \equiv -1 \mod n$. Therefore

$$q^l \equiv -1 \mod p_i^{k_i}, \text{ for } 1 \leq i \leq t \tag{3}$$

and

$$q^l \equiv -1 \mod 2^{k_0} \tag{4}$$

Equation (3) and Lemma 8 give that $l = \frac{1}{2}(1 + 2m_i)ord_{p_i}(q)$, for some integers m_i. Equation (4) and Lemma 14 give $q \equiv -1 \mod 2^{k_0}$ and that the integer l must be odd. It follows that $2l = (1 + 2m_i)ord_{p_i}(q)$. Which means that $2 \| ord_{p_i}(q)$. This completes the proof. □

Example 4. Let $R = \mathbb{Z}_9$, $n = 3724 = 2^2 \cdot 7^2 \cdot 19$. We have $ord_7(3) = 6$, $ord_{19}(3) = 18$. Note that $2\|6$, $2\|18$ and $2^2 \mid 4$. So all free cyclic codes of length $n = 3724$ are LCD codes.

4. Self dual cyclic codes over finite chain rings

Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$. If the nilpotency index e of $\langle\gamma\rangle$ is even, the cyclic code $\langle\gamma^{\frac{e}{2}}\rangle$ is self dual and is called the trivial self dual code. The following result gives a necessary and sufficient conditions for the existence of non trivial self dual cyclic codes of length n over R.

Lemma 15. *[8, Theorem 4.4] Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$, even index of nilpotency e, and residue field $\mathbb{F}_q$. Then non trivial cyclic self dual codes of length n over R exist if and only if there is no positive integer i, such that $q^i \equiv -1 \mod n$.*

Cyclic codes of length n which is not divisible by the characteristic of R are called simple root cyclic codes. It was proven that there are no simple root self dual cyclic codes over finite chain rings when the nilpotency index of the generator of the maximal ideal is odd.

Theorem 4. *[2, Theorem 12] Let R be a finite chain ring where $\langle\gamma\rangle$ is the maximal ideal with nilpotency index e and $\mathbb{F}_q$ is the residue field. If e is odd, then there are no non trivial self dual cyclic codes of length n over R when $\gcd(n, q) = 1$.*

In [2], authors introduce a simple criterion for the existence of non trivial self dual codes over R when the length is an odd prime power and the nilpotency index of the maximal ideal of the ring is even.

Lemma 16. *[2, Theorem 6] Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$, even index of nilpotency e and residue field $\mathbb{F}_q$. If n is an odd prime power coprime with q,* *then there exists a non trivial cyclic self dual code of length n over R if and only if $ord_n(q)$ is odd.*

Using Lemmas 12 and 15, we will generalize this result and provide conditions on the existence of non trivial self dual codes of arbitrary length over R.

Theorem 5. *Let R be a finite chain ring with maximal ideal of even index of nilpotency e, and residue field $\mathbb{F}_q$. Let n be an odd integer coprime to q such that the factorization of n is given by $n = p_1^{k_1} p_2^{k_2} ... p_t^{k_t}$, with k_i in $\mathbb{N}^*$ for all $1 \leq i \leq t$ and $t \geq 2$. Denote by a_i the integers of $\mathbb{N}$ such that $2^{a_i} \| ord_{p_i}(q)$, for all $1 \leq i \leq t$. Then a non trivial self dual cyclic codes of length n exist if and only if one of the following statements holds:*

(i) *There exists at least i_0, $1 \leq i_0 \leq t$ such that $a_{i_0} = 0$.*
(ii) *For all $1 \leq i \leq t$, $a_i \neq 0$, and there exist two distinct integers i_1, i_2 with $1 \leq i_1, i_2 \leq t$ such that $a_{i_1} \neq a_{i_2}$.*

Proof. Assume that there exits i_0, $1 \leq i_0 \leq t$ such that $a_{i_0} = 0$. This means that $ord_{p_{i_0}}(q)$ is odd. Lemma 8 guarantees that there is no integer l such that $q^l \equiv -1 \mod p_{i_0}$. Hence, for all i in $\mathbb{N}$ we can't have $q^i \equiv -1 \mod n$. Thus, from Lemma 15, a non trivial self dual cyclic code over R exists.

Assume now that (ii) is satisfied. Therefore, all $ord_{p_i}(q)$, for $1 \leq i \leq t$, are even. Lemma 12 shows that if there exist two distinct integers i_1, i_2, $1 \leq i_1, i_2 \leq t$ such that $a_{i_1} \neq a_{i_2}$, then there is no integer l such that $q^l \equiv -1 \mod n$. Hence, a non trivial self dual codes over R exist.

Conversely, assume that a non trivial self dual codes exist. So there is no integer l such that $q^l \equiv -1 \mod n$. We need to prove that either there exists i_0 such that $a_{i_0} = 0$ or every a_i is different to zero and at least two of them are distinct. Suppose that for all $1 \leq i \leq t$, $a_i \neq 0$. This implies that $ord_{p_i}(q)$ is even for all $1 \leq i \leq t$. Since there is no integer l such that $q^l \equiv -1 \mod n$, by Lemma 12, we have that there exists i_1, i_2 with $1 \leq i_1, i_2 \leq t$ such that $a_{i_1} \neq a_{i_2}$. □

Example 5. Let $R = \mathbb{Z}_4$ and $n = 3 \cdot 5$. We have $ord_3(2) = 2$ and $ord_5(2) = 4$, and hence $2^1 \| ord_3(2)$ and $2^2 \| ord_5(2)$. So there exist non trivial self dual codes over $\mathbb{Z}_4$ of length 15. The factorization of $x^{15} - 1$ over $\mathbb{Z}_4$ is given by

$$x^{15} - 1 = f_1(x) f_2(x) f_3(x) f_4(x) f_4^*(x),$$

where

$$f_1(x) = x+3, \; f_2(x) = x^2+x+1, \; f_3(x) = x^4+x^3+x^2+x+1, \text{ and } f_4(x) = x^4+2x^2+3x+1.$$

Let $g(x) = f_1(x) f_2(x) f_3(x)$ and $h(x) = f_4(x)$. Then the following codes

$$\langle g(x)h(x), 2h(x)h^*(x)\rangle \text{ and } \langle g(x)h^*(x), 2h(x)h^*(x)\rangle$$

are non trivial self dual cyclic codes of length 15.

Example 6. Let $R = \mathbb{Z}_{16}$ and $n = 21$. We have $ord_3(2) = 2$ and $ord_7(2) = 3$. Then, there exist non trivial self dual cyclic codes over R of length 21. The factorization of $x^{21} - 1$ over R is equal to

$$x^{21} - 1 = f_1(x)f_2(x)f_3(x)f_3^*(x)f_4(x)f_4^*(x),$$

where

$$f_1(x) = x-1,\ f_2(x) = x^2+x+1,\ f_3(x) = x^3+6x^2+5x-1,\ f_4(x) = x^6-6x^5-x^4-x^2+5x+1.$$

Let $x^{21} - 1 = g(x)h(x)h^*(x)$, where $g(x) = f_1(x)f_2(x)$ is a self reciprocal polynomial and $h(x) = f_3(x)f_4(x)$. Thus, for example, the code $\langle g(x)h(x), 2h(x)h^*(x)\rangle$ is self dual.

We give now the necessary and sufficient conditions for the existence of non trivial self dual codes when the length is an oddly even integer.

Theorem 6. *Let R be a finite chain ring with maximal ideal of even index of nilpotency e, and residue field $\mathbb{F}_q$. Let n be an oddly even integer coprime to q such that the irreducible factorization of n is given by $n = 2.p_1^{k_1}p_2^{k_2}...p_t^{k_t}$, where $t \geq 2$, and k_i in $\mathbb{N}^*$ for all $1 \leq i \leq t$. Let $a_i \in \mathbb{N}$ such that $2^{a_i} \| ord_{p_i}(q)$. Then a non trivial self dual cyclic code of length n exists if and only if one of the following statements holds:*

(i) *There exists at least $i_0, 1 \leq i_0 \leq t$ such that $a_{i_0} = 0$.*
(ii) *For all $1 \leq i \leq t$, $a_i \neq 0$, there exist two distinct integers i_1, i_2 with $1 \leq i_1, i_2 \leq t$ such that $a_{i_1} \neq a_{i_2}$.*

Proof. Since $gcd(n, q) = 1$, then q must be an odd integer. Hence for all l in $\mathbb{N}^*$ we have $2 \mid q^l + 1$. If $a_1 = a_2 = ... = a_t = a$, and $a \neq 0$, by Lemma 12, we know that there exists l in $\mathbb{N}^*$ such that $q^l \equiv -1 \mod \prod_{i=1}^t p_i^{k_i}$. Therefore, $q^l \equiv -1 \mod n$. Hence, there do not exist non trivial self dual codes on R by Lemma 15.

Conversely, assume (i) holds. Thus, from Lemma 8, there is no integer l such that $q^l \equiv -1 \mod p_{i_0}$. Hence, there does not exist integer l in $\mathbb{N}$, such that $q^l \equiv -1 \mod n$. This proves by Lemma 15 that non trivial self dual cyclic codes over R exist.

Assume now that (ii) is satisfied. By Lemma 12, if there exist two distinct integers $i_1, i_2, 1 \leq i_1, i_2 \leq t$ such that $a_{i_1} \neq a_{i_2}$, then there is no integer l such that $q^l \equiv -1 \mod \prod_{i=1}^t p_i^{k_i}$. Even if we have 2 divides $q^l + 1$ for all $l \in \mathbb{N}^*$, we cannot find any integer l such that $q^l \equiv -1 \mod n$. Hence by Lemma 15, non trivial self dual codes over R exist. □

Example 7. Let $R = \mathbb{Z}_9$ and $n = 70 = 2 \cdot 5 \cdot 7$. We have $ord_5(3) = 4$, $ord_7(3) = 6$, and hence $2 \| ord_7(3)$ and $2^2 \| ord_5(3)$. So there exist non trivial self dual cyclic codes of length 70 over $\mathbb{Z}_9$. The factorization of $x^{70} - 1$ over $\mathbb{Z}_9$ is given by

$$x^{70} - 1 = f_1(x)f_2(x)f_3(x)f_4(x)f_5(x)f_6(x)f_7(x)f_7^*(x)f_8(x)f_8^*(x),$$

where

$$\begin{aligned}
f_1(x) =& \quad x + 1,\\
f_2(x) =& \quad x + 8,\\
f_3(x) =& \quad x^4 + x^3 + x^2 + x + 1,\\
f_4(x) =& \quad x^4 + 8x^3 + x^2 + 8x + 1,\\
f_5(x) =& \quad x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,\\
f_6(x) =& \quad x^6 + 8x^5 + x^4 + 8x^3 + x^2 + 8x + 1,\\
f_7(x) =& \quad x^{12} + 4x^{10} + 6x^9 + 8x^8 + x^7 + 3x^6 + 4x^5 + 5x^4 + 7x^3 + 5x^2 + 8x + 1,\\
f_8(x) =& \quad x^{12} + 4x^{10} + 3x^9 + 8x^8 + 8x^7 + 3x^6 + 5x^5 + 5x^4 + 2x^3 + 5x^2 + x + 1.
\end{aligned}$$

Let $x^{70} - 1 = g(x)h(x)h^*(x)$, where $g(x) = f_1(x)f_2(x)f_3(x)f_4(x)f_5(x)f_6(x)$ is a self reciprocal polynomial and $h(x) = f_7(x)f_8(x)$. Thus, for example, the code $\langle g(x)h(x), 3h(x)h^*(x)\rangle$ is self dual.

Example 8. Let $R = \mathbb{Z}_{49}$ and $n = 30 = 2 \cdot 3 \cdot 5$. We have $ord_3(7) = 1$, $ord_5(7) = 4$. We have that $ord_3(7)$ is odd, so there exist non trivial self dual cyclic codes of length 30 over $\mathbb{Z}_{49}$. The factorization of $x^{30} - 1$ over $\mathbb{Z}_{49}$ is given by

$$x^{30} - 1 = f_1(x)f_2(x)f_2^*(x)f_3(x)f_3^*(x)f_4(x)f_5(x)f_6(x)f_7(x)f_7^*(x)f_8(x)f_8^*(x),$$

where

$$\begin{aligned}
&f_1(x) = x + 1, && f_2(x) = x - 19\\
&f_3(x) = x - 18, && f_4(x) = x - 1,\\
&f_5(x) = x^4 + x^3 + x^2 + x + 1, && f_6(x) = x^4 - x^3 + x^2 - x + 1,\\
&f_7(x) = x^4 - 19x^3 + 18x^2 + x - 19, && f_8(x) = x^4 - 18x^3 - 19x^2 - x + 18,
\end{aligned}$$

Let $x^{30} - 1 = g(x)h(x)h^*(x)$, where $g(x) = f_1(x)f_4(x)f_5(x)f_6(x)$ and $h(x) = f_2(x)f_3(x)f_7(x)f_8(x)$. Thus, for example, the code $\langle g(x)h(x), 7h(x)h^*(x)\rangle$ is self dual.

We determine now, necessary and sufficient conditions for the existence of non trivial self dual cyclic codes over R for doubly even lengths.

Theorem 7. *Let R be a finite chain ring with maximal ideal of even index of nilpotency e, and residue field $\mathbb{F}_q$. Let n be a doubly even integer coprime to q, such that the irreducible factorization of n is given by $n = 2^{k_0}p_1^{k_1}p_2^{k_2}...p_t^{k_t}$ where k_i in*

$\mathbb{N}^*$ *for all* $1 \leq i \leq t$ *and* $k_0 \geq 2$*. Let* a_i *in* $\mathbb{N}$ *such that* $2^{a_i} \| ord_{p_i}(q)$*, for* $1 \leq i \leq t$*. The following statements are equivalent:*

(i) *Non trivial self dual cyclic codes over* R *exist.*
(ii) *There exits* i*,* $1 \leq i \leq t$*, such that* $a_i \neq 1$ *or* $2^{k_0} \nmid (q+1)$*.*

Proof. Assume that (ii) is not satisfied. This implies that $a_1 = a_2 = ... = a_t = 1$ and $2^{k_0} \mid (q+1)$. Then from Lemma 12, there is an odd integer l such that $q^l \equiv -1 \mod \prod_{i=1}^{t} p_i^{k_i}$. Since $q \equiv -1 \mod 2^{k_0}$ and l is odd, it follows that $q^l \equiv -1 \mod 2^{k_0}$. Thus $q^l \equiv -1 \mod n$. Lemma 15 shows that non trivial self dual cyclic code over R does not exist.

Conversely, suppose that it does not exist any non trivial self dual cyclic codes of length n over R. Then, by Lemma 15, there exist some positive integer l such that $q^l \equiv -1 \mod n$. Thus, $q^l \equiv -1 \mod 2^{k_0}$. By Lemma 14, we have that $q \equiv -1 \mod 2^{k_0}$ and that the integer l is odd. On the other hand $q^l \equiv -1 \mod n$ implies again that $q^l \equiv -1 \mod p_i$. Lemma 8 gives that $2l = (1+2m_i)ord_{p_i}(q)$, for some integers m_i. Since l is odd, it follows that $2 \| ord_{p_i}(q)$. This means that $a_i = 1$ for each $1 \leq i \leq t$. □

Example 9. Let $R = \mathbb{Z}_{25}$ and $n = 84 = 2^2 \cdot 3 \cdot 7$. We have that $2^2 \nmid (5+1)$. Then there are non trivial self dual cyclic codes of length 84 over $\mathbb{Z}_{25}$. The factorization of $x^{84} - 1$ over $\mathbb{Z}_{25}$ is given by

$$x^{84} - 1 = \prod_{i=1}^{10} f_i(x) \prod_{i=11}^{15} f_i(x) f_i^*(x),$$

where

$$\begin{aligned}
f_1(x) &= x + 1,\\
f_2(x) &= x + 24,\\
f_3(x) &= x^2 + x + 1,\\
f_4(x) &= x^2 + 24x + 1,\\
f_5(x) &= x^6 + 5x^5 + 22x^4 + 2x^3 + 22x^2 + 5x + 1,\\
f_6(x) &= x^6 + 20x^5 + 22x^4 + 23x^3 + 22x^2 + 20x + 1,\\
f_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,\\
f_8(x) &= x^6 + 6x^5 + 8x^4 + 9x^3 + 8x^2 + 6x + 1,\\
f_9(x) &= x^6 + 24x^5 + x^4 + 24x^3 + x^2 + 24x + 1,\\
f_{10}(x) &= x^6 + 19x^5 + 8x^4 + 16x^3 + 8x^2 + 19x + 1,\\
f_{11}(x) &= x + 7,\\
f_{12}(x) &= x^2 + 7x + 24,\\
f_{13}(x) &= x^6 + 10x^5 + 3x^4 + 11x^3 + 22x^2 + 10x + 24,\\
f_{14}(x) &= x^6 + 17x^5 + 17x^4 + 12x^3 + 8x^2 + 17x + 24,\\
f_{15}(x) &= x^6 + 7x^5 + 24x^4 + 18x^3 + x^2 + 7x + 24.
\end{aligned}$$

Let $x^{84}-1=g(x)h(x)h^*(x)$ where $g(x)=\prod_{i=1}^{10} f_i(x)$ and $h(x)=\prod_{i=11}^{15} f_i(x)$. Thus for example the code $\langle g(x)h(x),\ 5h(x)h^*(x)\rangle$ is self dual.

Example 10. Let $R=\mathbb{Z}_{81}$ and $n=140=2^2\cdot 5\cdot 7$. We have that $2^2 \mid (3+1)$, $ord_7(3)=6$ and $ord_5(3)=4$. Thus $2^1\|ord_7(3)$ and $2^2\|ord_5(3)$. Therefore, there exist non trivial self dual cyclic codes of length 140 over $\mathbb{Z}_{81}$. The factorization of $x^{140}-1$ over $\mathbb{Z}_{81}$ is given by

$$\begin{aligned} x^{140}-1= \quad & f_1(x)f_2(x)f_3(x)f_4(x)f_4^*(x)f_5(x)f_6(x)f_7(x)f_8(x)f_9(x) \\ & f_{10}(x)f_{11}(x)f_{11}^*(x)f_{12}(x)f_{12}^*(x)f_{13}(x)f_{13}^*(x)f_{14}(x)f_{14}^*(x), \end{aligned}$$

where

$$\begin{aligned} f_1(x)= \quad & x+1, \\ f_2(x)= \quad & x-1, \\ f_3(x)= \quad & x^2+1, \\ f_4(x)= \quad & x^4-20x^3-3x^2+20x+1, \\ f_5(x)= \quad & x^4+x^3+x^2+x+1, \\ f_6(x)= \quad & x^4-x^3+x^2-x+1, \\ f_7(x)= \quad & x^6+13x^5+3x^4+13x^3+3x^2+13x+1, \\ f_8(x)= \quad & x^6+x^5+x^4+x^3+x^2+x+1, \\ f_9(x)= \quad & x^6-13x^5+3x^4-13x^3+3x^2-13x+1, \\ f_{10}(x)= \quad & x^6-x^5+x^4-x^3+x^2-x+1, \\ f_{11}(x)= \quad & x^{12}-24x^{11}+9x^{10}-17x^9+5x^8+31x^7-4x^6+11x^5-12x^4+4x^3 \\ & -8x^2+37x+1, \\ f_{12}(x)= \quad & x^{12}+24x^{11}+9x^{10}+17x^9+5x^8+50x^7-4x^6-11x^5-12x^4-4x^3 \\ & -8x^2+44x+1, \\ f_{13}(x)= \quad & x^{12}-9x^{11}+4x^{10}+15x^9+53x^8+19x^7+12x^6+49x^5+23x^4-2x^3 \\ & -13x^2+8x+1, \\ f_{14}(x)= \quad & x^{12}+9x^{11}+4x^{10}-15x^9+53x^8-19x^7+12x^6+32x^5+23x^4+2x^3 \\ & -13x^2-8x+1. \end{aligned}$$

Let $x^{140}-1=g(x)h(x)h^*(x)$ where $g(x)=\prod_{i=1}^{10} f_i(x)f_4^*(x)$ and $h(x)=\prod_{i=11}^{14} f_i(x)$. Thus the code $\langle g(x)h(x),\ 9h(x)h^*(x)\rangle$ is self dual.

5. Construction of new isodual cyclic codes over finite chain rings

In this section and according to different factorizations of the polynomial x^n-1, we give some new constructions of isodual cyclic codes over finite chain rings as a generalization of those obtained in [1]. First, we recall the structure of cyclic codes of length $2^a m$ given in [1].

Lemma 17. *[1, Lemma 4] Let R be a finite chain ring with residue field $\mathbb{F}_q$ such that q is an odd prime power, and let m an odd integer coprime to q. Then there is a primitive 2^a-th root of unity ξ in R^* if and only if $q \equiv 1 \mod 2^a$. Further,*

1. *$x^{2^a} - 1 = \prod_{k=1}^{2^a}(x - \xi^k)$ in $R[x]$,*
2. *ξ^m is also a primitive 2^a-th root of unity,*
3. *$\prod_{k=1}^{2^a} \xi^k = 1$, if $a \geqslant 2$.*

Proposition 1. *If R^* contains a primitive 2^a-th root of unity ξ, and $x^m - 1 = \prod_{i=1}^{l} f_i(x)$, where $f_i(x)$, $1 \leq i \leq l$, are monic basic irreducible pairwise coprime factors in $R[x]$, then*

$$x^{2^a m} - 1 = \prod_{k=1}^{2^a} \prod_{i=1}^{l} f_i(\xi^k x).$$

Proof. Assume that $x^m - 1 = \prod_{i=1}^{l} f_i(x)$. Let ξ be a primitive 2^a-th root of unity. Then $(\xi^k x)^m - 1 = \prod_{i=1}^{l} f_i(\xi^k x)$. Thus $x^m - \xi^{-km} = \xi^{-km} \prod_{i=1}^{l} f_i(\xi^k x)$. Since ξ is a primitive 2^a-th root of unity and $\prod_{k=1}^{2^a} \xi^{-km} = 1$, we get

$$\begin{aligned} x^{2^a m} - 1 &= (x^m)^{2^a} - 1 = \prod_{k=1}^{2^a}(x^m - \xi^k) = \prod_{k=1}^{2^a}(x^m - \xi^{-km}) \\ &= \prod_{k=1}^{2^a}(\xi^{-km} \prod_{i=1}^{l} f_i(\xi^k x)) = \prod_{k=1}^{2^a} \prod_{i=1}^{l} f_i(\xi^k x)) \quad \square \end{aligned}$$

For the construction of isodual codes we need the following result given in [1]

Lemma 18. *[1, Theorem 3] Let R be a finite chain ring, C a free cyclic code of length n over R generated by a polynomial $g(x)$ and δ a unit in R such that $\delta^n = 1$. Then the following holds:*

(i) C is equivalent to the cyclic code generated by $g^*(x)$.
(ii) C is equivalent to the cyclic code generated by $g(\delta x)$.
(iii) C is equivalent to the cyclic code generated by $g^*(\delta x)$ or $(g(\delta x))^*$.
(iv) If n is even, then C is equivalent to the cyclic code generated by $g(-x)$.

Proposition 2. *Let n be a positive integer. If $f(x)$ and $g(x)$ are polynomials in $R[x]$ such that $x^n - 1 = g(x)f(x)$, then the cyclic code generated by $g(x)$ is equivalent to the dual of the code generated by $f(x)$.*

Proof. Let C be a cyclic code generated by $g(x)$ and C' a cyclic code generated by $f(x)$. We have that the dual of C' is generated by $g^*(x)$. By Lemma 18, C is equivalent to $C'^{\perp}$. $\square$

The following theorem gives a natural construction for free cyclic isodual codes.

Proposition 3. *Let n be a positive integer such that there exists δ in R^* verifying $\delta^n = 1$. If $x^n - 1 = \alpha g(x)g(\delta x)$ or $x^n - 1 = \alpha g(x)g(\delta x)^*$ for some α in R^*, then the code generated by $g(x)$ is isodual.*

Proof. Assume that $x^n - 1 = \alpha g(x)g(\delta x)^*$. Let C be a code generated by the polynomial $g(x)$. From Theorem 4, C is free code. From Proposition 2, C is equivalent to the dual of the cyclic code C' generated by $\alpha g(\delta x)^*$. Up to normalization and since $\delta^n = 1$ and α in R^*, we obtain that the code C' is equivalent to the code generated by $g(x)$ which is C itself. Therefore C is isodual. With the same argument, we get the result for the second part. □

In the following, we take q is an odd prime power such that $q \equiv 1 \mod 2^a$ with $a \geq 1$ and m an odd integer with $\gcd(m, q) = 1$. We next give new construction of isodual cyclic codes of length $2^a m$ over R.

Theorem 8. *Assume that $x^m - 1 = f_1(x)f_2(x)$. Then the free cyclic codes of length $2^a m$ generated by*

$$\prod_{k=1}^{2^{a-1}} f_i(\xi^{2k}x) \prod_{k=0}^{2^{a-1}-1} f_j(\xi^{2k+1}x),\ i{,}j \in \{1,2\}, i \neq j,$$

or

$$\prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}x)f_2(\xi^{2k}x),$$

or

$$\prod_{k=0}^{2^{a-1}-1} f_1(\xi^{2k+1}x)f_2(\xi^{2k+1}x)$$

are isodual, where ξ is a primitive 2^a-th root of unity.

Proof. Let $x^m - 1 = f_1(x)f_2(x)$. From Proposition 1, we have

$$x^{2^a m} - 1 = \prod_{k=1}^{2^a} f_1(\xi^k x)f_2(\xi^k x) = \prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}x)f_2(\xi^{2k}x) \prod_{k=0}^{2^{a-1}-1} f_1(\xi^{2k+1}x)f_2(\xi^{2k+1}x).$$

Let

$$g(x) = \prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}x) \prod_{k=0}^{2^{a-1}-1} f_2(\xi^{2k+1}x).$$

Table 1
List of isodual codes obtained of length 36 over $\mathbb{Z}_{25}$.

Polynomial generator $g(x)$ of the isodual code C
$g(x) = x^9 + (\xi - \xi^2)x^6 + (\xi^2 - \xi^3)x^3 - 1$
$g(x) = \xi^3 x^9 + (\xi - 1)x^6 + (\xi^3 - \xi^2)x^3 - 1$
$g(x) = \xi^3 x^9 - (\xi^2 - \xi)x^8 + (\xi^3 - 1)x^7 - (\xi^2 - 1)x^6 + (\xi^2 - \xi^3)x^5 - (\xi - 1)x^4 + (\xi - \xi^3)x^3 + (\xi^3 - 1)x^2 + (\xi - \xi^2)x - 1$
$g(x) = x^9 - (\xi^2 - \xi^3)x^8 - (\xi - \xi^2)x^7 + (\xi^2 - 1)x^6 + (\xi - 1)x^5 - (\xi^3 - 1)x^4 + (\xi^2 - 1)x^3 - (\xi^2 - \xi^3)x^2 - (\xi - \xi^2)x - 1$
$g(x) = \xi^2 x^9 - (\xi - 1)x^8 - (\xi^3 - 1)x^7 - (\xi^2 - \xi^3)x^6 - (\xi - \xi^2)x^5 + (\xi - 1)x^4 - (\xi^3 - 1)x^3 - (\xi^2 - \xi^3)x^2 - (\xi - \xi^2)x - 1$
$g(x) = \xi x^9 + (\xi^3 - 1)x^8 + (\xi - \xi^2)x^7 + (\xi^3 - 1)x^6 + (\xi - \xi^2)x^5 + (\xi^3 - 1)x^4 + (\xi - \xi^2)x^3 + (\xi^3 - 1)x^2 + (\xi - \xi^2)x - 1$
$g(x) = \xi^2 x^9 - 1$
$g(x) = \xi x^9 - 1$

Knowing that $\xi^{2^a} = 1$, we get

$$g(\xi x) = \prod_{k=1}^{2^{a-1}} f_1(\xi^{2k+1}x) \prod_{k=0}^{2^{a-1}-1} f_2(\xi^{2k+2}x) = \prod_{k=0}^{2^{a-1}-1} f_1(\xi^{2k+1}x) \prod_{k=1}^{2^{a-1}} f_2(\xi^{2k}x).$$

In other words, we have that $x^{2^a m} - 1 = g(x)g(\xi x)$. Since $\xi^{2^a m} = 1$, then from Theorem 3 the code generated by $g(x)$ is isodual. A similar argument is employed to prove that codes generated by

$$\prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}x) f_2(\xi^{2k}x)$$

or

$$\prod_{k=0}^{2^{a-1}-1} f_1(\xi^{2k+1}x) f_2(\xi^{2k+1}x)$$

are also isodual. □

Example 11. Let $R = \mathbb{Z}_{25}$ and $n = 36 = 2^2 \cdot 3^2$, $q = 5 \equiv 1 \mod 2^2$. We have

$$x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1).$$

Thus, we get the isodual codes given in Table 1, where ξ is a primitive 4-th root of unity.

Corollary 3. *Let p^k be a prime power. Assume that $x^{p^k} - 1 = f_1(x)f_2(x)$. Then the cyclic codes generated by*

$$f_1(x)f_2(-x) \text{ or } f_1(-x)f_2(x) \text{ or } x^{p^k} - 1 \text{ or } x^{p^k} + 1$$

Table 2
List of LCD-isodual codes obtained of length 50 over $\mathbb{Z}_9$.

Polynomial generator $g(x)$ of LCD-isodual code C
$g(x) = x^{25} - 2x^{20} + 2x^{15} - 2x^{10} + 2x^5 - 1$
$g(x) = x^{25} + 2x^{20} + 2x^{15} + 2x^{10} + 2x^5 + 1$
$g(x) = -x^{25} - 2x^{24} - 2x^{23} - 2x^{22} - 2x^{21} + 2x^{19} + 2x^{18} + 2x^{17} + 2x^{16} - 2x^{14} - 2x^{13} - 2x^{12} - 2x^{11} + 2x^9 + 2x^8 + 2x^7 + 2x^6 - 2x^4 - 2x^3 - 2x^2 - 2x - 1$
$g(x) = x^{25} - 2x^{24} + 2x^{23} - 2x^{22} + 2x^{21} - 2x^{19} + 2x^{18} - 2x^{17} + 2x^{16} - 2x^{14} + 2x^{13} - 2x^{12} + 2x^{11} - 2x^9 + 2x^8 - 2x^7 + 2x^6 - 2x^4 + 2x^3 - 2x^2 + 2x - 1$
$g(x) = x^{25} - 2x^{24} + 2x^{23} - 2x^{22} + 2x^{21} - 2x^{20} + 2x^{19} - 2x^{18} + 2x^{17} - 2x^{16} + 2x^{15} - 2x^{14} + 2x^{13} - 2x^{12} + 2x^{11} - 2x^{10} + 2x^9 - 2x^8 + 2x^7 - 2x^6 + 2x^5 - 2x^4 + 2x^3 - 2x^2 + 2x - 1$
$g(x) = x^{25} + 2x^{24} + 2x^{23} + 2x^{22} + 2x^{21} + 2x^{20} + 2x^{19} + 2x^{18} + 2x^{17} + 2x^{16} + 2x^{15} + 2x^{14} + 2x^{13} + 2x^{12} + 2x^{11} + 2x^{10} + 2x^9 + 2x^8 + 2x^7 + 2x^6 + 2x^5 - 2x^4 + 2x^3 + 2x^2 + 2x + 1$
$g(x) = x^{25} - 1$
$g(x) = x^{25} + 1$

are isodual codes of length $2p^k$. Further, if $ord_p(q)$ is even, then these codes are LCD-isodual codes.

Proof. The result follows from Theorem 1 and Theorem 8 for $a = 1$, $m = p^k$ and $\xi = -1$. □

Example 12. Let $R = \mathbb{Z}_9$ and $n = 50 = 2 \cdot 5^2$. We have

$$x^{25} - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)(x^{20} + x^{15} + x^{10} + x^5 + 1).$$

Further $ord_5(3) = 4$. So we get the LCD isodual codes shown in Table 2.

Corollary 4. *Let m be an odd integer such that the irreducible factorization of m is given by $m = p_1^{k_1} p_2^{k_2} ... p_t^{k_t}$ and $x^m - 1 = f_1(x)f_2(x)$. Assume that there exists a in $\mathbb{N}^*$ such that $2^a \| ord_{p_i}(q)$, for all $1 \leq i \leq t$. Then, the cyclic codes generated by*

$$f_1(x)f_2(-x) \text{ or } f_1(-x)f_2(x) \text{ or } x^m - 1 \text{ or } x^m + 1$$

are LCD-isodual codes of length $2m$.

Proof. The result follows immediately from Theorem 2 and Theorem 8 with $\xi = -1$. □

Another construction of isodual cyclic codes is given by the following theorem.

Theorem 9. *Assume that we have the factorization $x^m - 1 = f_1(x)f_2(x)f_2^*(x)$, such that the polynomial f_1 is self reciprocal. Then the cyclic codes of length $2^a m$ over R generated by*

$$\prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}x)\prod_{k=1}^{2^a} f_2(\xi^k x)$$

or

$$\prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}x)\prod_{k=1}^{2^a} f_2^*(\xi^k x)$$

are isodual, where ξ is a primitive 2^a-th root of unity.

Proof. Let $x^m-1=f_1(x)f_2(x)f_2^*(x)$ then

$$x^{2^a m}-1=\prod_{k=1}^{2^a} f_1(\xi^k x)f_2(\xi^k x)f_2^*(\xi^k x)=\prod_{k=1}^{2^{a-1}} f_1(\xi^{2k})\prod_{k=0}^{2^{a-1}-1} f_1(\xi^{2k+1})\prod_{k=1}^{2^a} f_2(\xi^k x)f_2^*(\xi^k x)$$

Let $g(x)=\prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}x)\prod_{k=1}^{2^a} f_2(\xi^k x)$. Since $\xi^{2^a}=1$, we get

$$g(\xi x)=\prod_{k=1}^{2^{a-1}} f_1(\xi^{2k+1}x)\prod_{k=1}^{2^a} f_2(\xi^{k+1}x)=\prod_{k=0}^{2^{a-1}-1} f_1(\xi^{2k+1}x)\prod_{k=1}^{2^a} f_2(\xi^k x).$$

Since the polynomial f_1 is self reciprocal, we obtain the factorization $x^{2^a m}-1=g(x)g(\xi x)^*$. The desired result follows from Theorem 3. The same result is obtained for the codes generated by

$$\prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}x)\prod_{k=1}^{2^a} f_2^*(\xi^k x). \quad \square$$

Example 13. Let $R=\mathbb{Z}_{25}$ and $n=132=2^2\cdot 33$. We have $5\equiv 1 \mod 2^2$ and

$$\begin{aligned} x^{33}-1= \quad & (x-1)(x^2+x+1)(x^5-8x^4-x^3+x^2-9x-1)\\ & (x^5+9x^4-x^3+x^2+8x-1)\\ & (x^{10}-9x^9+7x^8+11x^7+9x^6-4x^5-7x^4-6x^3-10x^2+8x+1)\\ & (x^{10}+8x^9-10x^8-6x^7-7x^6-4x^5+9x^4+11x^3+7x^2-9x+1) \end{aligned}$$

Let $x^{33}-1=f_1(x)f_2(x)f_2^*(x)$, where $f_1(x)=(x-1)(x^2+x+1)$ and $f_2(x)=(x^5-8x^4-x^3+x^2-9x-1)(x^{10}-9x^9+7x^8+11x^7+9x^6-4x^5-7x^4-6x^3-10x^2+8x+1)$. Thus, for example, the codes generated by

$$\left\langle f_1(x)f_1(\xi^2x)f_2(x)f_2(\xi^2x)f_2(\xi^3x)\right\rangle$$

or

$$\left\langle f_1(x)f_1(\xi^2x)f_2^*(x)f_2^*(\xi x)f_2^*(\xi^2x)f_2^*(\xi^3x)\right\rangle$$

are isodual, where ξ is a primitive 4-th root of unity.

Corollary 5. *Let p be an odd prime number and k in $\mathbb{N}$ such that $x^{p^k}-1=f_1(x)f_2(x)f_2^*(x)$. Assume that $ord_p(q)$ is even. Then the cyclic codes of length $2p^k$ generated by*

$$f_1(x)f_2(x)f_2(-x) \text{ or } f_1(x)f_2^*(x)f_2^*(-x)$$

are LCD-isodual codes.

Proof. The result follows from Theorem 1 and Theorem 9 with $\xi=-1$. □

Corollary 6. *Let m be an odd integer such that the irreducible factorization of m is given by $m=p_1^{k_1}p_2^{k_2}...p_t^{k_t}$ and $x^m-1=f_1(x)f_2(x)f_2^*(x)$. Assume that there exists a in $\mathbb{N}^*$ such that $2^a\|ord_{p_i}(q)$, for all $1\leq i\leq t$. Then the cyclic codes of length $2m$ generated by*

$$f_1(x)f_2(x)f_2(-x) \text{ or } f_1(x)f_2^*(x)f_2^*(-x)$$

are LCD-isodual codes.

Proof. The result follows immediately from Theorem 2 and Theorem 9 with $\xi=-1$. □

Example 14. Let $R=\mathbb{Z}_{27}$ and $n=70=2\cdot5\cdot7$. We have $x^{35}-1=f_1(x)f_2(x)f_2^*(x)$, where

$$f_1(x)=(x-1)(x^4+x^3+x^2+x+1)(x^6+x^5+x^4+x^3+x^2+x+1)$$
$$f_2(x)=(x^{12}-9x^{11}+4x^{10}-12x^9-3x^8-7x^7+12x^6-5x^5-4x^4-2x^3+14x^2+8x+1).$$

So the cyclic codes of length 70 over $\mathbb{Z}_{27}$ generated by

$$g(x)=f_1(x)f_2(x)f_2(-x)$$

or

$$h(x)=f_1(x)f_2^*(x)f_2^*(-x)$$

are isodual.

6. Conclusion

In this work, cyclic codes over finite chain rings were studied. Conditions for which all these codes are LCD were given. In addition, necessary and sufficient conditions were given for the existence of non trivial self dual cyclic codes. Further, new constructions of isodual codes were presented and investigated when these codes are LCD-isodual codes.

References

[1] A. Batoul, K. Guenda, T.A. Gulliver, N. Aydin, On isodual cyclic codes over finite chain rings, in: S. El Hajji, A. Nitaj, E. Souidi (Eds.), Codes, Cryptology, and Information Security C2SI-Carlet, in: Lecture Notes in Computer Science, vol. 10194, 2017, pp. 176–194.

[2] A. Batoul, K. Guenda, T.A. Gulliver, Constacyclic codes over finite principal ideal rings, in: S. El Hajji, A. Nitaj, E. Souidi (Eds.), Codes, Cryptology, and Information Security C2SI-Carlet, in: Lecture Notes in Computer Science, vol. 10194, 2017, pp. 161–175.

[3] A. Batoul, K. Guenda, T.A. Gulliver, Repeated-root isodual cyclic codes over finite fields, in: S. El Hajji, A. Nitaj, C. Carelet, E. Souidi (Eds.), Codes, Cryptology, and Information Security C2SI-Carlet, in: Lecture Notes in Computer Science, vol. 9084, 2015, pp. 119–132.

[4] F. Benahmed, K. Guenda, A. Batoul, T.A. Gulliver, Some new constructions of isodual and LCD codes over finite fields, Adv. Math. Commun. 13 (2) (2019) 281–296.

[5] N. Benbelkacem, J. Borges, S.T. Dougherty, C. Fernandez-Cordoba, On $\mathbb{Z}_2\mathbb{Z}_4$-additive complementary dual codes and related LCD codes, Finite Fields Appl. 62 (2020).

[6] D.J. Bernstein, J. Buchmann, E. Dahmen, Post-Quantum Cryptography. Library of Congress Control Number: 2008937466. Mathematics Subject Classification Numbers (2000): 94A60.

[7] S. Bhowmick, A. Fotue-Tabue, E. Martinez-Moro, R. Bandi, S. Bagchi, Do non-free LCD codes over finite commutative Frobenius rings exist?, Des. Codes Cryptogr. 88 (2020) 825–840.

[8] H.Q. Dinh, S.R. Lopez-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inf. Theory 50 (8) (2004) 1728–1744.

[9] V. Dragoiy, T. Richmondz, D. Bucerzan, A. Legayz, Code-Based Cryptography: from Theoretical to Physical Cryptanalysis. Published in: 2018 7th International Conference on Computers Communications and Control (ICCCC).

[10] K. Guenda, T.A. Gulliver, MDS and self-dual codes over rings, Finite Fields Appl. 18 (2012) 1061–1075.

[11] A.R. Hammons, J.P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inf. Theory 40 (2) (1994) 301–319.

[12] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York, 1982.

[13] C. Li, C. Ding, S. Li, LCD cyclic codes over finite fields, IEEE Trans. Inf. Theory 63 (2017) 4344–4356.

[14] E.R. Lina, E.G. Nocon, On the construction of some LCD codes over finite fields, Manila J. Sci. 9 (2016) 67–82.

[15] X. Liu, H. Liu, LCD codes over finite chain rings, Finite Fields Appl. 34 (2015) 1–19.

[16] Z. Liu, J. Wang, Linear complementary dual codes over rings, Des. Codes Cryptogr. 87 (2019) 3077–3086.

[17] J.L. Massey, Linear codes with complementary duals, Discrete Math. 106/107 (1992) 337–342.

[18] B.R. McDonald, Finite Rings with Identity, Pure and Applied Math., vol. 28, Marcel Dekker, New York, NY, 1974.

[19] G.H. Norton, A. Salagean, On the structure of linear and cyclic codes over a finite chain ring, Appl. Algebra Eng. Commun. Comput. 10 (6) (2000) 489–506.

[20] X. Yang, J.L. Massey, The condition for a cyclic code to have a complementary dual, Discrete Math. 126 (1994) 391–393.