Scientific Annals of Computer Science vol. 34 (1), 2024, pp. 23–38
doi: 10.47743/SACS.2024.1.23

Classification of Certain Cyclic LCD Codes

Seth Gannon[1] and Hamid Kulosman[2]

Abstract

We show that a necessary and sufficient condition for a cyclic code $\mathcal{C}$ of length N over a finite chain ring R (whose maximal ideal has nilpotence 2) to be an LCD code is that $\mathcal{C} = (f(x))$, where $f(X)$ is a self-reciprocal monic divisor of $X^N - 1$ in $R[X]$ and $x = X + (X^N - 1)$ in $R[X]/(X^N - 1)$. A similar, but slightly different, theorem was proved in 2019 by Z. Liu and J. Wang for general finite chain rings (Theorem 25 in [5]). We provide two proofs, both completely different than the proof of Liu and Wang.

Keywords: Complementary dual (LCD) code, cyclic codes, codes over rings.

1 Introduction

A finite commutative ring is called a *finite chain ring* if its ideals are linearly ordered by inclusion. A finite chain ring is clearly a local ring. It is well-known that a commutative ring is a finite chain ring if and only if it is a finite local principal ideal ring. Let γ be a generator of the maximal ideal of a finite chain ring R. Then γ is nilpotent and let ν be its nilpotency index, i.e., the smallest positive integer such that $\gamma^\nu = 0$. We will denote by κ the residue field $R/(\gamma)$. A *linear code* $\mathcal{C}$ of length N overa finite commutative ring R is any R-submodule of the R-module R^N. A code is

[1]Department of Mathematics & Computer Science, Sewanee: The University of the South, 723 University Avenue, Sewanee, TN 37375,USA, Email: dsgannon@sewanee.edu

[2]Department of Mathematics, University of Louisville, 2301 South 3rd St, Louisville, KY 40292, USA, Email: hamid.kulosman@louisville.edu

said to be *cyclic* if a cyclic shift of any codeword is a codeword. If we denote $R_N = \frac{R[X]}{X^{N-1}}$, then, as usual we identify $(R^N, +)$ and $(R_N, +)$ via the map $c_1c_2 \dots c_N \mapsto c_1 + c_2x + \dots + c_Nx^{N-1}$ from R^N to R_N, where $x = X + (X^{N-1})$. With that identification, a linear code over R of length N is cyclic if and only if it is an ideal of R_N. Let R be a finite commutative ring. We define the *inner product* of elements $\mathbf{x} = x_1x_2 \dots x_N$ and $\mathbf{y} = y_1y_2 \dots y_N$ in R^N by $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{N} x_iy_i$. If $\mathcal{C}$ is a code over R of length N, we define the *dual* $\mathcal{C}^\perp$ of $\mathcal{C}$ by

$$\mathcal{C}^\perp = \{\mathbf{x} \in R^N | \mathbf{x} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}$$

A *linear code with a complemenatry dual* (an LCD code) is defined to be a linear code $\mathcal{C}$ satisfying $\mathcal{C} \cap \mathcal{C}^\perp = \{\mathbf{0}\}$.

LCD codes (and, more generally, the hulls of linear codes) are recently being of considerable interest since there are several applications of them, including, for example, the recently found applications in Quantum Coding Theory. It was defined in [6], where a necessary and sufficient for a linear code over a field to be an LCD code was given in terms of the generator matrix. Later in [8] the authors gave a necessary and sufficient condition for a cyclic code over a field to be an LCD code.

Theorem 1 *[8] If $g(X)$ is the generator polynomial of a cyclic code $\mathcal{C}$ over $\mathbf{F}_q$ of length N, then $\mathcal{C}$ is an LCD code if and only if $g(X)$ is self-reciprocal and all the monic irreducible factors of $g(X)$ have the same multiplicity in $g(X)$ and in $X^N - 1$.*

Recently in [2] we provided a necessary and sufficient condition for a cyclic code over $\mathbb{Z}_4$, to be an LCD code by using a theorem from [4] where a formula for the number of elements in $\text{Hull}(C) = C \cap C^\perp$ was given in terms of the generators of a cyclic code C of odd length N over $\mathbb{Z}_4$.

Theorem 2 *[2, Theorem 2.1] A cyclic code C over $\mathbb{Z}_4$ of odd length N is an LCD code if and only if $C = (f(x))$, where $f(X)$ is a self-reciprocal monic divisor of $X^N - 1 \in \mathbb{Z}_4[X]$.*

In this paper we generalize the results from [8] and our results in [2] by using results from [3] and [7] to produce a condition for a cyclic code C over a finite chain ring with nilpotency 2 to be an LCD code.

2 Classification of Cyclic Codes over R

2.1 Preliminaries

$\mathbb{F}_2+u\mathbb{F}_2$ and $\mathbb{Z}_4$ are special cases of finite chain rings. The ring $A=\frac{\mathbb{F}_2[X]}{(X^2)}=\mathbb{F}_2[u]=\mathbb{F}_2+u\mathbb{F}_2$, where $u=X+(X^2)$, so that $A=\{a+bu\ :\ a,b\in\mathbb{F}_2\}=\{0,1,u,1+u\}$ is known as the ring of dual numbers over $\mathbb{F}_2$ (note: $u^2=0$). The ring A is a chain ring with the ideals $A\supseteq\{0,u\}\supseteq\{0\}$. It is one of the four commutative rings with four elements: $\mathbb{F}_2\times\mathbb{F}_2,\mathbb{F}_4,\mathbb{Z}_4,A=\mathbb{F}_2+u\mathbb{F}_2$. The units in A are 1 and $1+u$ and the ideals of A are $(0)=\{0\}$, $(1)=(1+u)=A$, and $(1)=\{0,u\}$. A is a local ring (i.e. has unique maximal ideal, namely (u)). The maximal ideal $\mathfrak{m}=(u)$ has nilpotency index 2 as $(u)^2=(u^2)=(0)$. The ring A is of characteristic 2, i.e., $x+x=0$ for every $x\in A$. A is an extension of the field $\mathbb{F}_2$, as the elements $0,1$ from A form a subfield $\mathbb{F}_2$ of the ring A and $A/\mathfrak{m}\cong\mathbb{F}_2$ (the residue field of A). The natural map $\pi:A\to A/\mathfrak{m}\cong\mathbb{F}_2$ is given by

$$\pi(0)=0,\ \pi(1)=1,\ \pi(u)=0,\ \pi(1+u)=1.$$

Let $C\subseteq A^n$ be a linear code over $A=\mathbb{F}_2+u\mathbb{F}_2$. Then $\overline{C}=\{\overline{\mathbf{w}}=\overline{w_1w_2}\dots\overline{w_n}|\mathbf{w}=w_1w_2\dots w_n\}$ will be the projection of C onto a code over $\overline{A}^n=\mathbb{F}_2^n$. The projection is a map $\pi:C\to\mathbb{F}_2^n$. The same notation π is used for the projection $\pi:A=\mathbb{F}_2+u\mathbb{F}_2\to\mathbb{F}_2$, as well as for $\pi:A^n\to\mathbb{F}_2^n$.

Let R be a finite chain ring with maximal ideal $\mathfrak{m}=(\gamma)$. All elements of $\mathfrak{m}$ are nilpotent and $R^*=R\backslash\mathfrak{m}$. The notation $R=(R,\mathfrak{m},\kappa)$ means that R is a local ring with maximal ideal $\mathfrak{m}$ and residue field $\kappa=\frac{R}{\mathfrak{m}}$. The notation $(R,\mathfrak{m})$ is used when there is no need to specify κ The phrase "finite chain ring $(R,(\gamma),\kappa)$ or $(R,(\gamma))$" means that the maximal ideal of R is generated by γ and $\kappa=\frac{R}{(\gamma)}$. The rings $\mathbb{Z}_4$ and $A=\mathbb{F}_2+u\mathbb{F}_2$ are examples of finite chain rings $(R,(\gamma))$ with $\nu(\gamma)=2$. where $\nu(\gamma)$ denotes the index of nilpotency of γ. Similar to the previously mentioned projection the following can be defined for codes over $R=(R,\mathfrak{m},\kappa)$. Let $C\subseteq R^n$ be a linear code over R. Then $\overline{C}=\{\overline{\mathbf{w}}=\overline{w_1w_2}\dots\overline{w_n}|\mathbf{w}=w_1w_2\dots w_n\}$ will be the projection of C onto a code over $\overline{R}^N=\kappa^N$. The projection is a map $\pi:C\to\kappa^N$. The same notation π is used for the projection $\pi:R\to\kappa$, as well as for $\pi:R^N\to\kappa^N$. If R is a commutative ring, the cyclic codes over R of length N are the ideals of the quotient ring $R_N=\frac{R[X]}{(X^N-1)}$. We denote the elements of $R[X]$ by $f(X)$, or shortly by f, while the elements of $\frac{R[X]}{(X^N-1)}$ are denoted by $f(x)$ (so that $x=X+(X^N-1)$) and $f(x)=f(X)+(X^N-1)$).

The following theorem describes the unique factorization of a polynomial in $R[X]$ and will be used throughout the rest of this chapter.

Theorem 3 *[7, Theorem 4.4] Suppose $N \geq 1$ is an integer that $char(\kappa) \nmid N$. Then for every ideal I of R_N there exists two unique monic polynomials $f_0(X)$ and $f_1(X)$ from $R[X]$ with $f_1(X)|f_0(X)|X^N - 1$ such that $I = \big(f_0(x), \gamma f_1(x)\big)$.*

We will now define a reciprocal polynomial over R in the same we way we previously defined a reciprocal polynomial over $\mathbb{Z}_4$. Any monic factor g of $X^N - 1 \in R[X]$ factors uniquely (up to the order of factors) into a product of monic pairwise coprime basic irreducible polynomials from $R[X]$ and those monic irreducibles are from the set $\mathrm{Fact}(X^N - 1)$. We will denote by $Fact(g)$ the set of those factors of g.

Definition 4 *Let $f(X) = a_0 + a_1X + ... + a_{n-1}X^{n-1} + X^n$ be a monic polynomial in R whose constant term a_0 is a unit in R. The reciprocal polynomial f^* of f is defined by*

$$f^*(X) = a_0^{-1} X^{deg(f)} f(\frac{1}{X}).$$

The following is the monic version of Hensel's Lemma which shows how one can get from a factorization in $\kappa[X]$ to a factorization in $R[X]$.

Corollary 5 *[7, Theorem 2.6] Let $R = \big(R, \mathfrak{m}, \kappa\big)$ be a finite local ring and $f \in R[X]$ be a monic polynomial. Assume there are $g_1, g_2, \ldots, g_k \in \kappa[X]$ monic, pairwise relatively prime and such that $\overline{f} = g_1 g_2 \cdots g_k$. Then there are $f_1, f_2, \ldots, f_k \in R[X]$ monic, pairwise relatively prime, such that $f = f_1 f_2 \cdots f_k$ and $\overline{f_i} = g_i$ for $i = 1, 2, \ldots k$.*

2.2 Results

The following are standing assumptions for this section:

1. $R = (R, \mathfrak{m} = (\gamma), \kappa = \frac{R}{\mathfrak{m}})$ is a finite chain ring with $\nu(\gamma) = 2$.
2. $N \geq 1$ is an integer such that $\mathrm{char}(\kappa) \nmid N$.
3. $R_N = \frac{R[X]}{X^N - 1}$ and $\kappa_N = \frac{\kappa[X]}{X^N - 1}$.

Theorem 6 *For every cyclic code C over R of length N there are unique, monic, pairwise coprime polynomials $f(X)$, $g(X)$, and $h(X)$ in $R[X]$ such that $X^N - 1 = f(X)g(X)h(X)$ and $C = \big(f(x)g(x), \gamma f(x)\big)$.*

Proof: By Theorem 3, there are unique monic polynomials $f_0(X)$ and $f_1(X)$ in $R[X]$ such that $f_1(X)|f_0(X)|x^N - 1$ and $C = \big(f_0(x), \gamma f_1(x)\big)$. Let $f_0(X) = f_1(X)g_1(X)$ and $h_1(X) = \frac{X^N-1}{f_0(X)} = \frac{X^N-1}{f_1(X)g_1(X)}$. Then f_1, g_1 and h_1 are monic, pairwise coprime polynomials (since the assumed condition $\mathrm{char}(\kappa) \nmid N$) such that $X^N - 1 = f_1(X)g_1(X)h_1(X)$ and $C = \big(f_1(x)g_1(x)$, $\gamma f_1(x)$. The polynomials f_1, g_1 and h_1 are unique, otherwise the pair f_0, f_1 from [7, Theorem 4.4], would not be unique. Replacing the notation f_1, g_1 and h_1 by f, g and h we get the statement of the theorem. □

Proposition 7 *The polynomial $f = X^N - 1 \in R[X]$ has a unique decomposition into distinct monic basic irreducible factors in $R[X]$.*

Proof: Since $\mathrm{char}(\kappa) \nmid N$, $\overline{f} = X^N - 1 \in \kappa[X]$ is square free in $\kappa[X]$ hence by [7, Theorem 2.7], $\overline{f} = X^N - 1 \in R[X]$ factors uniquely into monic pairwise coprime basic irreducibles. □

We will denote the set of all monic pairwise coprime basic irreducibles into which $X^N - 1 \in R[X]$ factors in $R[X]$ by $\mathrm{Fact}(X^N - 1)$. Any monic factor g of $X^N - 1 \in R[X]$ factors uniquely (up to the order of factors) into a product of monic pairwise coprime basic irreducible polynomials from $R[X]$ and those monic irreducibles are from the set $\mathrm{Fact}(X^N - 1)$. We will denote by $Fact(g)$ the set of those factors of g.

Proposition 8 *Any monic factor $g(X)$ of $X^N - 1 \in R[X]$ factors uniquely (up to the order of factors) into a product of monic pairwise coprime basic irreducible polynomials from $R[X]$ and those monic irreducibles are from the set $Fact(X^N - 1)$.*

Proof: Since $X^N - 1 \in \kappa[X]$ is square-free, $\bar{g}(X) \in \kappa[X]$ is also square-free. Now the statement follows from [7, Theorem 2.7], and Proposition 4.7. □

Proposition 9 *[3, Pages 5-6] The polynomial $X^N - 1 \in \mathbb{F}_q[X]$ can be decomposed in $\mathbb{F}_q[X]$ into a product of monic irreducible factors in the following way:*

$$X^N - 1 = h_1(X) \dots h_s(X) k_1(X) k_1^*(X) \dots k_t(X) k_t^*(X), \tag{1}$$

where the polynomials $h_i(X)$ are self-reciprocal and the pairs $\big(k_j(X), k_j^*(X)\big)$ are reciprocal pairs. This decomposition is unique on the right-hand side of the above equality are pairwise coprime.

Proposition 10 *Let $\kappa = \mathbb{F}_q$. Taking into account Proposition 9, the polynomial $X^N - 1 \in R[X]$ can be decomposed in $R[X]$ into a product of monic, basic irreducible factors in the following way:*

$$X^N - 1 = g_1(X) \dots g_s(X) f_1(X) f_1^*(X) \dots f_t(X) f_t^*(X), \tag{2}$$

where the polynomials $g_i(X)$ are self-reciprocal, the pairs $\big(f_j(X), f_j^*(X)\big)$ are reciprocal pairs, and $\bar{g}_i = h_i$, $\bar{f}_i = k_i$, $\bar{f_i^*} = k_i^*$. The decomposition of $X^N - 1$ into monic basic irreducible is unique up to the order of the factors and the polynomials that appear on the right-hand side the above equality are pairwise coprime.

Proof: The decomposition (2) can be obtained by the Hensel lifting, given by Corollary 5, of the decomposition (1). The uniqueness follows from Proposition 7. The uniqueness, together with Proposition 11, implies that the polynomials g_j are self-reciprocal and that the pairs $\big(f_j(X)$, $f_j^*(X)\big)$ are reciprocal pairs. The pairwise coprimeness in (2) follows from the pairwise coprimeness in (1).

□

Proposition 11 *Let $f \in R[X]$ be a monic polynomial with invertible constant term. Then $\overline{f^*} = \overline{f}^*$*

Proof:

Let $f = a_0 + a_1 X \cdots + a_{n-1} X^{n-1} + X^N$. Then $\overline{f^*} = \overline{a_0^{-1}(1 + a_{n-1}X + \dots + a_1 X^{n-1} + X^n)} = \overline{a_0^{-1}}(1 + \overline{a_{n-1}}X + \cdots + \overline{a_1}X^{n-1} + \overline{a_0}X))$. On the other side, $\overline{f}^* = (\overline{a_0} + \overline{a_1}X + \cdots + \overline{a_{n-1}}X^{n-1} + X^n)^* = \overline{a_0}^{-1}(1 + \overline{a_{n-1}}X + \cdots + \overline{a_1}X^{n-1} + \overline{a_0}X) = \overline{a_0^{-1}}(1 + \overline{a_{n-1}}X + \cdots + \overline{a_1}X^{n-1} + \overline{a_0}X)$. □

We will denote by $\mathrm{Fact}(g)$ the set of monic basic irreducible factors of g that appears in the decomposition from Proposition 8. Note that here g is a monic factor of $X^N - 1 \in R[X]$.

Lemma 12 *Let $p(X)$ and $q(X)$ be two polynomials in $R[X]$ monic divisors of $X^N - 1$. Suppose that $p(X)q(X) = 0$ and let $q'(X) = \frac{X^N - 1}{q(X)}$. Then $q'(X) | p(X)$.*

Proof: The condition $p(X)q(X) = 0$ implies $p(X)q(X) \in (X^N - 1)$, hence $p(X)q(X) = t(X)(X^N - 1)$ for some $t(X)$. Hence $p(X)q(X) = t(X)q(X)q'(X)$, which implies $q(X)\big(p(X) - t(X)q'(X)\big) = 0$. Since $q(X)$ is monic, it is a regular element of $R[X]$, so that $p(X) - t(X)q'(X) = 0$. Hence $q'(X)|p(X)$. □

Lemma 13 *[4, Lemma 3.1] Let* $\boldsymbol{u} = (u_0, u_1, \ldots, u_{N-1})$ *and* $\boldsymbol{v} = (v_0, v_1, \ldots, v_{N-1})$ *be vectors in* R^N *with corresponding polynomials* $u(X)$ *and* $v(X)$. *Then* $\boldsymbol{u}$ *is orthogonal to* $\boldsymbol{v}$ *and all its shifts if and only if* $u(x)v^*(x) = 0$ *in* R_N.

Lemma 14 *Let* $a(X)$, $b(X)$ *be monic divisors of* $X^N - 1$ *in* $R[X]$. *Then*

$$X^N - 1 = lcm\big(a(X), b(X)\big) \cdot gcd\big(\frac{X^N - 1}{a(X)}, \frac{X^N - 1}{b(X)}\big).$$

Proof: The statement follows from the relation
$\mathrm{Fact}(a) \cup \mathrm{Fact}(b) \cup \big(\mathrm{Fact}(X^N - 1) \setminus \mathrm{Fact}(a)\big) \cap \big(\mathrm{Fact}(X^N - 1) \setminus \mathrm{Fact}(b)\big)$
$= \mathrm{Fact}(X^N - 1)$. □

Corollary 15 *Let* $f(X)$, $g(X)$ *and* $h(X)$ *be monic divisors of* $X^N - 1$ *in* $R[X]$ *such that* $f(X)g(X)h(X) = X^N - 1$. *Then:*

$$X^N - 1 = lcm\big(f(X)g(X), h^*(X)g^*(X)\big) \cdot gcd\big(h(X), f^*(X)\big)$$

and

$$\frac{lcm\big(f(X)g(X), h^*(X)g^*(X)\big)}{lcm\big(f(X), h^*(X)\big)} = \frac{X^N - 1}{gcd\big(h(X), f^*(X)\big) \cdot lcm\big(f(X), h^*(X)\big)}.$$

Proof: The first relation follows from Lemma 13 since $f(X)g(X)h(X) = X^N - 1$ and $f^*(X)g^*(X)h^*(X) = X^N - 1$, The second relation follows from the first relation. □

The following theorem extends [4, Theorem 3.2] from cyclic codes over $\mathbb{Z}_4$ to cyclic codes over R.

Theorem 16 *Let* $C = \big(f(x)g(x), \gamma f(x)\big)$ *be a cyclic code over* R *of length* N, *where* $f(X)$, $g(X)$ *are monic divisors of* $X^N - 1$ *in* $R[X]$ *such that* $f(X)g(X)h(X) = X^N - 1$. *Then*

$$Hull(C) = \big(lcm\big(f(X)g(X), h^*(X)g^*(X)\big)\ ,\ \gamma\ lcm\big(f(X), h^*(X)\big)\big)$$

Furthermore,

$$|Hull(C)| = 4^{deg(H(X))}2^{deg(G(X))},$$

where

$$H(X) = gcd\big(h(X), f^*(X)\big)$$

and

$$G(X) = \frac{X^N - 1}{gcd\big(h(X), f^*(X)\big)\, lcm\big(f(X), h^*(X)\big)}.$$

Proof: By [7, Theorem 4.9], we have

$$C^{\perp} = \big(h^*(x)g^*(x), \gamma h^*(x)\big).$$

Let C' be a cyclic code of length N over R give by

$$C' = \big(F(x)G(x), \gamma F(x)\big),$$

where

$$F(X) = \mathrm{lcm}\big(f(X), h^*(X)$$

and by Lemma 14 and Corollary 15 we have that

$$G(X) = \frac{\big(\mathrm{lcm}\big(f(X)g(X), h^*(X)g^*(X)\big)}{\mathrm{lcm}\big(f(X), h^*(X)\big)}$$

$$= \frac{X^N - 1}{\gcd\big(h(X), f^*(X)\big) \cdot \mathrm{lcm}\big(f(X), h^*(X)\big)},$$

and

$$H(X) = \frac{X^N - 1}{\big(\mathrm{lcm}\big(f(X)g(X), h^*(X)g^*(X)\big)} = \gcd\big(h(X), f^*(X)\big)$$

.

The polynomials $F(X)$, $G(X)$ and $H(X)$ are monic pairwise coprime and $X^N - 1 = F(X)G(X)H(X)$. since

$$\big(F(x)G(x), \gamma F(x)\big) \subseteq \big(f(x)g(x), \gamma f(x)\big)$$

and

$$\big(F(x)G(x), \gamma F(x)\big) \subseteq \big(h^*(x)g^*(x), \gamma h^*(x)\big)$$

we have

$$C' \subseteq \mathrm{Hull}(C).$$

Now the opposite inclusion is shown. Since Hull(C) is a cyclic code of length N over R, we have

$$C' = \big(A(x)B(x), \gamma A(x)\big),$$

where $A(X)$, $B(X)$ and $C(X)$ are pairwise coprime polynomials in $R[X]$ such that $A(X)B(X)C(X) = X^N - 1$. Since Hull$(C) \subseteq C^\perp$ is orthogonal to C, by Lemma 13, we have

$$A(X)B(X) \cdot \gamma f^*(X) = 0$$

and

$$\gamma A(X) \cdot f^*(X)g^*(X) = 0$$

which implies by Lemma 12 that

$$h^*(X)g^*(X)|A(X)B(X)$$

and

$$h^*(X)|A(X).$$

Similarly, Hull$(C) \subseteq C$ is orthogonal to $C^\perp$ which implies by Lemma 13 that

$$A(X)B(X) \cdot \gamma h(X) = 0$$

and

$$\gamma A(X) \cdot h(X)g(X) = 0$$

It follows By Lemma 12 that

$$f(X)g(X)|A(X)B(X)$$

and

$$f(X)|A(X)$$

Consequently,

$$\mathrm{lcm}\big(f(X)g(X), h^*(X)g^*(X)\big)\,(|A(X)B(X))$$

and

$$\mathrm{lcm}\big(h^*(X), f(X)\big)|A(X)$$

which implies that

$$F(X)H(X)|A(X)B(X)$$

and

$$F(X)|A(X).$$

Hence $\mathrm{Hull}(C) \subseteq C'$. Therefore $\mathrm{Hull}(C) = C'$

Assuming that

$$f_0(X) = \mathrm{lcm}\big(f(X)g(X), h(X)^*g(X)^*\big)$$

and

$$f_1(X) = \mathrm{lcm}\big(f(X)g^*(X)\big)$$

it follows from [7, Theorem 4.5], that $|\mathrm{Hull}(C)| = 4^{\deg(H(X))}2^{\deg(G(X))}$ as

$$H(X) = \frac{X^N - 1}{f_0(X)}$$

such that

$$\deg(H(X)) = N - \deg(f_0(X)),$$

and

$$G(X) = \frac{f_0(X)}{f_1(X)}$$

so that

$$\deg(G(X)) = \deg(f_0(X)) - \deg(f_1(X))$$

□

The following is the condition for a cyclic code over R to be an LCD code and extends the result of [8] and our results in [2].

Theorem 17 *A cyclic code C over R of length N is an LCD code if and only if $C = \big(f(x)\big)$, where $f(X)$ is a self-reciprocal monic divisor of $X^N - 1$ in $R[X]$.*

We now provide two proofs for the above theorem.

Proof: (First Proof) Let C be a cyclic code over R of length N. Suppose that C is an LCD code. It follows from 6 and 16 that there are unique polynomials $f(X)$, $g(X)$, $h(X)$ in $R[X]$ such that $C = \big(f(x)g(x), \gamma f(x)\big)$ with the following conditions satisfied:

$$f(X)g(X)h(X) = X^N - 1 \tag{3}$$

$$f, g, h \text{ are pairwise coprime} \tag{4}$$

$$\gcd(h(X), f^*(X)) = 1 \tag{5}$$

$$\operatorname{lcm}(f(X), h^*(X)) = X^N - 1 \tag{6}$$

The relations (5), respectively (6), are true because $H(X) = 1$, respectively, $G(X) = 1$, in the formula for $|\mathrm{Hull}(C)|$ in Theorem 16. It follows from (5) that:

$$\gcd(f(X), h^*(X)) = 1$$

which, together with (6) implies then following relations:

$$\mathrm{Fact}(f) \cap \mathrm{Fact}(h^*) = \emptyset \tag{7}$$

$$\mathrm{Fact}(f) \cup \mathrm{Fact}(h^*) = \mathrm{Fact}(X^N - 1). \tag{8}$$

The conditions (3) and (4) can be reformulated as

$$\mathrm{Fact}(f) \cup \mathrm{Fact}(g) \cup \mathrm{Fact}(h) = \mathrm{Fact}(X^N - 1) \tag{9}$$

$$\mathrm{Fact}(f),\ \mathrm{Fact}(g),\ \mathrm{Fact}(h) \text{ are pairwise disjoint.} \tag{10}$$

Now from (7), (8), (9), and (10) we can conclude that

$$\mathrm{Fact}(h^*) = \mathrm{Fact}(g) \cup \mathrm{Fact}(h) \tag{11}$$

Since $\mathrm{Fact}(g)$ and $\mathrm{Fact}(h)$ are disjoint, $\mathrm{Fact}(h)$ and $\mathrm{Fact}(h^*)$ have the same number of elements, we conclude that

$$\mathrm{Fact}(g) = \emptyset, \tag{12}$$

or, equivalently, that

$$g = 1. \tag{13}$$

Then (11) and (12) imply that h is self-reciprocal, and, since due to (13) $X^N - 1 = f(X)h(X)$ we have f is also self-reciprocal.

Also again using (13), we have $C = (f(x)g(x), \gamma f(x)) = (f(x), \gamma f(x)) = (f(x))$ Conversely, let $C = (f(x))$, where $f(X)$ is a monic self-reciprocal divisor of $X^N - 1$ in $R[X]$. Then $g(X) = 1$ and $h(X) = \frac{X^N-1}{f(X)}$ are the unique monic divisors of $X^N - 1$ such that $f(X)g(X)h(X) = X^N - 1$ and $C = (f(x)g(x), \gamma f(x))$. Since $f(X)$ and $h(X)$ are relatively prime and self-reciprocal, then in Corollary 15 we have $H(X) = 1$ and $G(X) = 1$. Hence, by Corollary 15, $|\text{Hull}(C)| = 1$, i.e., C is an LCD code. $\square$ For the second proof we will need the following definitions:

Definition 18 *C is a free code if it is a free R-module. In other words, if C has a basis.*

Definition 19 *Let C be a linear code over R. Define a linear code $(C : \gamma) = \{\boldsymbol{w} \in R^n : \gamma \boldsymbol{w} \in C\}$.*

Definition 20 *Let*

$$k_0(C) = dim_\kappa \overline{C},$$

$$k_1(C) = dim_\kappa \overline{(C : \gamma)} - dim_\kappa \overline{C}.$$

We say C is of type $\big(k_0(C), k_1(C)\big)$ and $k(C) = k_0(C) + k_1(C)$.

Proof: (Second Proof) Suppose that C is an LCD cyclic code of length N over R. Then by [1, Proposition 4.1]. C is free. Let $C = \big(f(x)g(x), \gamma f(x)\big)$ for some monic divisors f, g, and h of $X^N - 1$ in $R[X]$ such that $f(X)g(X)h(X) = X^N - 1$. Assuming that $f_0 = fg$ and $f_1 = f$, we have by [7, Theorem 4.5], that $k_0(C) = n - \deg(f_0) = \deg(h)$ and $k_1(C) = n - \deg(f_0) - \deg(f_1) = \deg(g)$. By [7, Proposition 3.13], C is free if and only if $k_1(C) = 0$, i.e., if and only if $g = 1$. Hence $C = \big(f(x), \gamma f(x)\big) = \big(f(x)\big)$. It remains to show that f is self-reciprocal. Note that by Theorem 4.14 that when $g = 1$, then

$$\text{Hull}(C) = \big(\text{lcm}(f, h^*)\big)$$

and we need to see when is $\big(\text{lcm}(f, h^*)\big) = X^N - 1$, i.e., $\text{Hull}(C) = \big(0\big)$. Taking into account Proposition 10 and the fact that f and h are pairwise coprime monic divisors of $X^N - 1$ such that $f(X)h(X) = X^N - 1$. Let Γ_f (respectively Γ_h) be the set of the elements from $\{g_1(X) \dots g_s(X)\}$ that participate in the factorization of f (respectively h). Let Φ_f (respectively Φ_h) be the set of all $f_j(X), f_j^*(X)$ which both participate in the factorization of f (respectively h). Finally, let Δ_f be the set of all $f_j(X)$ which participate in

the factorization of f, but where $f_j^*(X)$ participate in the factorization of h and those $f_j^*(X)$ form Δ_h. Then

$$f = \Pi\, \Gamma_f \cdot \Pi\Phi_f \cdot \Pi\Delta_f$$

$$h = \Pi\, \Gamma_h \cdot \Pi\Phi_h \cdot \Pi\Delta_h$$

so that

$$\operatorname{lcm}\big(f, h^*\big) = \Pi\, \Gamma_f \cdot \Pi\, \Gamma_h \cdot \Pi\Delta_f$$

Since $\operatorname{lcm}\big(f, h^*\big) = X^N - 1$, we have $\Delta_h = \emptyset$, hence $\Delta_f = \emptyset$, hence f is self-reciprocal. The converse can be proved in the same way as the first proof. □

We again denote by $\varphi(n)$ the Euler function and define the following two functions:

$$\gamma(n, q) = \frac{\varphi(n)}{\operatorname{ord}_{\mathbb{Z}_n^*}(q),}$$

and

$$\beta(n, q) = \frac{\varphi(n)}{2\operatorname{ord}_{\mathbb{Z}_n^*}(q)}$$

where $q = p^r$, p prime, and $p \nmid n$. In order to give the number of cyclic LCD codes of length N over R we again define good and bad pairs and give a decomposition of $X^N - 1$ over R.

Definition 21 *Let n and r be positive integers. We say that the pair (n, r) is good if $n|(r^k + 1)$ for some integer $k \geq 1$. Otherwise we say that the pair (n, r) is bad.*

Proposition 22 *([6, Page 5]) The polynomial $X^n - 1 \in \mathbb{F}_q[X]$ can be decomposed in $\mathbb{F}_q[X]$ into a product of monic irreducible factors in the following way:*

$$X^N - 1 = \prod_{\substack{n|N \\ (n,q)\ good}} \left(\prod_{i=1}^{\gamma(n,q)} h_{i,n} \right) \prod_{\substack{n|N \\ (n,q)\ bad}} \left(\prod_{i=1}^{\beta(n,q)} k_{i,n} k_{i,n}^* \right), \qquad (14)$$

where the polynomials $h_{i,n}$ are self-reciprocal and the pairs $(k_{i,n}, k_{i,n}^*)$ are reciprocal pairs. This decomposition is unique up to the order of factors, and the polynomials that appear on the right-hand side of the above equality are pairwise coprime.

Proposition 23 *Let $k = F_q$. Taking into account Proposition 22, the polynomial $X^N - 1 \in R[X]$ can be decomposed in $R[X]$ into a product of monic, basic irreducible factors in the following way:*

$$X^N - 1 = \prod_{\substack{n|N \\ (n,q) \text{ good}}} \left(\prod_{i=1}^{\gamma(n,q)} g_{i,n} \right) \prod_{\substack{n|N \\ (n,q) \text{ bad}}} \left(\prod_{i=1}^{\beta(n,q)} f_{i,n} f_{i,n}^* \right), \qquad (15)$$

where the polynomials g_{in} are self-reciprocal and the pairs $(f_{i,n}, f_{i,n}^*)$ are reciprocal pairs, and $\overline{g_{i,n}} = h_{i,n}$, $\overline{f_{i,n}} = f_{i,n}$, $\overline{f_{i,n}^*} = k_{i,n}^*$. The decomposition of $X^N - 1$ into monic basic irreducible is unique up to the order of factors, and the polynomials that appear on the right-hand side of the above equality are pairwise coprime.

Proof: This proposition follows from Proposition 22 in the same way in which Proposition 10 follows from Proposition 9. □

Theorem 24 *The number of cyclic LCD codes of length N over R is 2^{nmsrf}, where $\kappa = \mathbb{F}_q$ and*

$$\text{nmsrf} = \sum_{\substack{n|N \\ (n,q) \text{ good}}} \frac{\varphi(n)}{\text{ord}_{\mathbb{Z}_n^*}(q)} + \frac{1}{2} \sum_{\substack{n|N \\ (n,q) \text{ bad}}} \frac{\varphi(n)}{\text{ord}_{\mathbb{Z}_n^*}(q)}.$$

Proof: Let $\Gamma = \{g_{i,n} : i, n\}$ The number of $g_{i,n}$'s is

$$|\Gamma| = \sum_{\substack{n|N \\ (n,q) \text{ good}}} \gamma(n,q)$$

Let Φ be the set consisting of exactly one element from each pair $\{f_{i,n}, f_{i,n}^*\}$

$$|\Phi| = \sum_{\substack{n|N \\ (n,q) \text{ bad}}} \beta(n,q)$$

The total number of elements in $\Gamma \cup \Phi$ is

$$\text{nmsrf} = \sum_{\substack{n|N \\ (n,q) \text{ good}}} \gamma(n,q) \; + \sum_{\substack{n|N \\ (n,q) \text{ bad}}} \beta(n,q)$$

which is equal to

$$\text{nmsrf} = \sum_{\substack{n|N \\ (n,q) \text{ good}}} \frac{\varphi(n)}{\text{ord}_{\mathbb{Z}_n^*}(q)} + \frac{1}{2} \sum_{\substack{n|N \\ (n,q) \text{ bad}}} \frac{\varphi(n)}{\text{ord}_{\mathbb{Z}_n^*}(q)}.$$

Every self-reciprocal monic divisors of $X^N - 1$ is uniquely determined by a subset of $\Gamma \cup \Phi$. Namely if $A \subseteq \Gamma \cup \Phi$, then $A = B \cup C$, where $B \subseteq \Gamma$ and $C \subseteq \Phi$, and the monic divisor corresponding to A can be written as

$$\Pi\{g \in B\} \cdot \Pi\{ff^* \; : \; f \in C\}.$$

Hence the number of self-reciprocal monic divisors of $X^N - 1$ is 2^{nmsrf}. By Theorem 17, the number of cyclic LCD codes of length n is 2^{nmsrf}. □

References

[1] Yilmaz Durgun. On LCD codes over finite chain rings. *Bulletin of the Korean Mathematical Society*, 57(1):37–50, 2020. doi:10.4134/BKMS.b181173.

[2] Seth Gannon and Hamid Kulosman. The condition for a cyclic code over $\mathbb{Z}_4$ of odd length to have a complementary dual. *CoRR*, abs/1905.12309, 2019. arXiv:1905.12309.

[3] Yan Jia, San Ling, and Chaoping Xing. On self-dual cyclic codes over finite fields. *IEEE Transactions on Information Theory*, 57(4):2243–2251, 2011. doi:10.1109/TIT.2010.2092415.

[4] Somphong Jitman, Ekkasit Sangwisut, and Patanee Udomkavanich. Hulls of cyclic codes over $\mathbb{Z}_4$. *Discrete Mathematics*, 343(1):111621, 2020. doi:10.1016/j.disc.2019.111621.

[5] Zihui Liu and Jinliang Wang. Linear complementary dual codes over rings. *Designs, Codes and Cryptography*, 87(12):3077–3086, 2019. doi:10.1007/S10623-019-00664-3.

[6] James L Massey. Linear codes with complementary duals. *Discrete Mathematics*, 106-107:337–342, 1992. doi:10.1016/0012-365X(92)90563-U.

[7] Graham H Norton and Ana Sălăgean. On the structure of linear and cyclic codes over a finite chain ring. *Applicable algebra in engineering, communication and computing*, 10(6):489–506, 2000. doi:10.1007/PL00012382.

[8] Xiang Yang and James L. Massey. The condition for a cyclic codes to have a complementary dual. *Discrete Mathematics*, 126(1-3):391–393, 1994. doi:10.1016/0012-365X(94)90283-6.