ON THE LATTICE OF CYCLIC LINEAR CODES OVER FINITE CHAIN RINGS

ALEXANDRE FOTUE TABUE AND CHRISTOPHE MOUJAH

ABSTRACT. Let $R$ be a commutative finite chain ring of invariants $(q,s)$. In this paper, the trace representation of any free cyclic $R$-linear code of length $\ell$, is presented, via the $q$-cyclotomic cosets modulo $\ell$, when $\gcd(\ell,q)=1$. The lattice $\langle \text{Cy}(R,\ell); +,\cap \rangle$ of cyclic $R$-linear codes of length $\ell$, is investigated. A lower bound on the Hamming distance of cyclic $R$-linear codes of length $\ell$, is established. When $q$ is even, a family of MDS and self-orthogonal $R$-linear cyclic codes, is constructed.

1. Introduction

Research on linear codes over chain rings can be found in [2][11] and cyclic linear codes were among the first codes practically used and they play a very significant role in coding theory. For instance, cyclic codes can be efficiently encoded using shift registers. Many important codes such as the Golay codes, Hamming codes and BCH codes can be represented as cyclic codes. Cyclic linear codes have been studied for decades and a lot of progress has been made (see, for example, [13]).

Let $R$ be finite chain ring with invariant $(q,s)$, and $\ell$ a positive integer such that $\gcd(q,\ell)=1$. An $R$-linear code of length $\ell$ is an $R$-submodule of $R^\ell$. An $R$-linear code $C$ of length $\ell$ is cyclic if for every codeword $(c_0,c_1,\cdots,c_{\ell-1})$ in $C$ then the word $(c_{\ell-1},c_0,\cdots,c_{\ell-2})$ also belongs to $C$. For example, the zero module $\{0\}$, the trivial $R$-linear code $R^\ell$ and the repetition code $I:=\{(c,c,\cdots,c) : c \in R\}$ are cyclic $R$-linear codes of length $\ell$.

As usual, the $R$-module isomorphism

\begin{equation}
\Psi : R^\ell \\
\rightarrow \ R[X]/(X^\ell-1)
\end{equation}

\begin{equation}
(c_0,c_1,\cdots,c_{\ell-1}) \rightarrow c_0 + c_1 X + \cdots + c_{\ell-1} X^{\ell-1} + (X^\ell-1)
\end{equation}

is used to identify the cyclic $R$-linear codes of length $\ell$ with ideals of the ring $R[X]/(X^\ell-1)$ and $(X^\ell-1)$ is the ideal of $R[X]$ generated by $X^\ell-1$. The $R$-module $\Psi(C)$ is called polynomial representation of the $R$-linear code $C$. This polynomial representation of cyclic linear codes is used by Calderbank and Sloane in [3], by Kanwar and López-Permouth [9], for study the structure of cyclic linear codes over $\mathbb{Z}_p^\ell$. Wan [12] extended these results to cyclic linear codes over Galois rings. Norton and Sălăgean [11] and Dinh and López-Permouth [5], in turn, extended the results of [3] and [9] to cyclic linear codes over finite chain rings.

We denote by $\text{Cy}(R,\ell)$, the set of all cyclic $R$-linear codes of length $\ell$. We equip $\text{Cy}(R,\ell)$ of binary operations as: $+$, and $\cap$. When $s = 1$ and $\gcd(q,\ell)=1$, it is widely known that $\mathbb{F}_q[X]$ is a domain ideal ring. Hence the lattice of ideals of $\mathbb{F}_q[X]/(X^\ell-1)$ is distributive. By the polynomial representation, it follows that for every $C \in \text{Cy}(\mathbb{F}_q,\ell)$, there exists a unique monic divisor $g$ of $X^\ell-1$ in $\mathbb{F}_q[X]$ such that $\Psi(C) = \langle g \rangle$, where $\langle g \rangle := (g)/(X^\ell-1)$, and $g$ is called the generator polynomial of $C$, and

\begin{equation}
\Psi^{-1}(\langle g_1 \rangle) \cap \Psi^{-1}(\langle g_2 \rangle) = \Psi^{-1}(\langle 1 \mathrm{cm}(g_1,g_2) \rangle),
\end{equation}

\begin{equation}
\Psi^{-1}(\langle g_1 \rangle) + \Psi^{-1}(\langle g_2 \rangle) = \Psi^{-1}(\langle g \mathrm{cd}(g_1,g_2) \rangle),
\end{equation}

for all monic divisors $g_1$ and $g_2$ of $X^\ell-1$ in $\mathbb{F}_q[X]$. Hence, the lattice $\langle \text{Cy}(\mathbb{F}_q,\ell); +,\cap\rangle$, $\mathbb{F}_q^\ell$ is distributive. In the general case $s \neq 1$, the lattice $\langle \text{Cy}(R,\ell); +,\cap \rangle$ is little known. In [11], Norton and Sălăgean, describe the generating set in standard form of any cyclic $R$-linear code of length $\ell$. The objective of this paper is to develop another approach of construction of cyclic linear codes in case the

2010 Mathematics Subject Classification. 13B05; 94B15; 06G10; 16P10.

Key words and phrases. Finite Chain Rings, Cyclotomic cosets, Linear Codes, Cyclic Codes, Trace Map, Finite Lattices.
length of the code is coprime to the characteristic of the finite chain ring. Fundamental theory of this approach will be developed, and will be employed to construct any cyclic linear code. BCH-bound of any cyclic linear code will be also established.

The paper is organized as follows: Some definitions and results about the finite chain rings and Galois extension of finite chain rings, are recalled in Section 2. Section 3 discusses the notions of the type of any linear code over a finite chain ring. In Section 4, the set of cyclotomic partitions is investigated. In Section 5, the trace-description of free cyclic linear codes over finite chain rings is presented. A lattice of cyclic linear codes is studied in Section 6.

2. Background on finite chain rings

Throughout of this section, \( R \) is a finite local ring with identity, \( J(R) \) denotes the maximal ideal of \( R \), and \( \mathcal{M}_{u \times \ell}(R) \) denotes the set of all \( u \times \ell \)-matrices over \( R \) for all \( 1 \leq u \leq \ell \).

**Definition 2.1.** A finite local ring \( R \) with identity is called a finite chain ring of invariants \((q,s)\) if

1. \( J(R) \) is principal, \( R/J(R) \cong \mathbb{F}_q \), and;
2. \( R \supseteq R \theta \supseteq \cdots \supseteq R \theta^{s-1} \supseteq R \theta^s = \{0_R\} \) where \( \theta \) is a generator of \( J(R) \).

For example, for every positive integer \( s, n, p \) and \( p \) prime, the ring \( \mathbb{Z}_{p^s} \), is a finite chain ring of invariants \((p,s)\), and the ring \( \mathbb{F}_{p^s}[\theta] \) with \( \theta^s = 0_R \) and \( \theta^{s-1} \neq 0_R \), is a finite chain ring of invariants \((p^n,s)\).

Let \( R \) be a finite chain ring of invariants \((q,s)\) and \( \theta \) be a generator of \( J(R) \). The ring epimorphism

\[
\pi: R \rightarrow \mathbb{F}_q \\
c \mapsto c(\mod \theta)
\]

naturally extends to \( R[X] \), of the following way: \( \pi(\sum a_i X^i) = \sum \pi(a_i) X^i \) and \( \mathcal{M}_{u \times \ell}(R) \) of the following way: \( \pi \) acts on all the coefficients of any polynomial (resp. matrix) over \( R \). Let \( R^\times \) be the multiplicative group of units of \( R \). Obviously, the cardinality of \( R^\times \) is \( q^{s-1}(q-1) \). It follows that \( R^\times \cong \Gamma(R)^s \times (1 + J(R)) \) with \( \Gamma(R)^s = \{b \in R : b \neq 0_R, b^q = b\} \), and \( \Gamma(R)^s \) is a cyclic subgroup of \( R^\times \), of order \( q-1 \). The set \( \Gamma(R) = \Gamma(R)^s \cup \{0_R\} \) is called the Teichmüller set of \( R \).

We say that the ring \( S \) is an extension of \( R \) and we denote it by \( S|R \) if \( R \) a subring of \( S \) and \( 1_R = 1_S \). We denote by \( \text{rank}_R(S) \), the rank of \( R \)-module \( S \). Let \( f \in R[X] \) of degree \( m \) and \( (f) \) is an ideal of \( R[X] \) generated by \( f \). Let \( f \) be a monic polynomial over \( R \) of degree \( m \). We say that \( f \) is basic irreducible (resp. basic primitive) if \( \pi(f) \) is irreducible over \( \mathbb{F}_q \) (resp. primitive).

**Definition 2.2.** Let \( R \) be a finite chain ring of invariants \((q,s)\). A finite ring \( S \) is a Galois extension of \( R \) of degree \( m \), if \( S \cong R[\alpha] \), (as \( R \)-algebras) where \( \alpha \) is a root of a monic basic primitive polynomial over \( R \) of degree \( m \).

**Remark 1.** Let \( R \) be a finite chain ring of invariants \((q,s)\) and \( S \) is a Galois extension of \( R \) of degree \( m \). Let \( \xi \) be a generator of \( \Gamma(S) \setminus \{0_S\} \). Then \( S \) is also a finite chain ring of invariants \((q^m,s)\) and \( S = R[\xi] \).

We denote by \( \text{Aut}_R(S) \), the group of ring automorphisms of \( S \) which fix the elements of \( R \).

**Theorem 1.** [4] Chap III.; Proposition 2.1(1)] Let \( R \) be a finite chain ring of invariants \((q,s)\). The ring \( S \) is a Galois extension of \( R \) of degree \( m \) if and only if \( R = \{a \in S : \sigma(a) = a \text{ for all } \sigma \in \text{Aut}_R(S)\} \) and \( J(S) = S J(R) \).

For example, for positive integers \( p, n, s \) and \( p \) prime, the Galois extension of \( \mathbb{Z}_{p^s} \) of degree \( n \), is the Galois ring \( GR(p^s, n) \cong \mathbb{Z}_{p^s}[X]/(f) \), where \( f \) is a monic basic irreducible over \( R \), of degree \( n \).

**Proposition 1.** [10] Theorem XV.10] Let \( R \) be a finite chain ring of invariants \((q,s)\) and \( S \) be the Galois extension of \( R \) of degree \( m \). Let \( \xi \) be a generator of \( \Gamma(S) \setminus \{0_S\} \). Then

1. \( S \) is a free \( R \)-module with free \( R \)-basis \( \{1, \xi, \ldots, \xi^{m-1}\} \);
2. \( \text{Aut}_R(S) \) is a cyclic group of order \( m \), and a generator of \( \text{Aut}_R(S) \) is given by \( \sigma : \xi \mapsto \xi^q \).
Definition 2.3. Let $\mathcal{S}(R)$ be the Galois extension of finite chain rings of degree $m$ and $\sigma$ be a generator of $\text{Aut}_R(\mathcal{S})$. The map $\text{Tr}_R^\mathcal{S} := \sum_{i=0}^{m-1} \sigma^i$, is called the trace map of $\mathcal{S}(R)$.

Theorem 2. [4] Chap III., Corollary 2.2] Let $\mathcal{S}(R)$ be the Galois extension of finite chain rings. Then $\text{Tr}_R^\mathcal{S}$ is a generator of $\mathcal{S}$-module $\text{Hom}_R(\mathcal{S}, R)$.

Proposition 2. Let $R$ be a finite chain ring of invariants $(q,s)$ and $S$ be the Galois extension of $R$ of degree $m$. Then for every positive integer $z$, for every generator $\xi$ of $\Gamma(S)$, the ring $R[\xi^z]$ is the Galois extension of $R$ of degree $m_z$, where $m_z := \min\{i \in \mathbb{N} \setminus \{0\} : zq^i \equiv 1 \pmod{(q^m - 1)}\}$.

Proof. We set $f := (X - \xi^z q)(X - \xi^{zq}) \cdots (X - \xi^{zq^m})$. Since $\mathcal{S}(R)$ is Galois extension, we deduce by Theorem[1] that $f \in R[X]$ and $\pi(f)$ is irreducible. Hence $f$ is a basic irreducible polynomial over $R$ and the degree of $f$ is $m_z$. It follows that $R[\xi^z]$ is a Galois extension of $R$ of degree $m_z$, because by Definition[2,2] $\xi^z$ is a root of a basic irreducible polynomial over $R$ of degree of $m_z$. □

3. Linear codes over finite chain rings

For this section, a finite chain ring of invariants $(q,s)$, and $\theta$ is a generator of maximal ideal $\mathfrak{J}(R)$. The ring epimorphism $\pi : R \to \mathbb{F}_q$ naturally extends to $R'$ of the following way: $\pi(\mathfrak{c}) := (\pi(c_0), \pi(c_1), \ldots, \pi(c_{s_1}))$, for every $\mathfrak{c} := (c_0, c_1, \ldots, c_{s_1}) \in R'$. Recall that an $R$-linear code of length $\ell$ is an $R$-submodule of $R'$.

We say that an $R$-linear code is free if it is free as $R$-module.

3.1. Type and rank of a linear code. An $k \times \ell$-matrix $G$ over $R$, is called a generator matrix for $\mathcal{C}$ if the rows of $G$ span $\mathcal{C}$ and none of them can be written as an $R$-linear combination of other rows of $G$. We say that $G$ is a generator matrix in standard form if

$$
G = \left( \begin{array}{cccc} I_{k_0} & G_{0,1} & G_{0,2} & \cdots & G_{0,s-1} & G_{0,s} \\ 0 & \theta I_{k_1} & \theta G_{1,2} & \cdots & \theta G_{1,s-1} & \theta G_{1,s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \theta^{s-1} I_{k_{s-1}} & \theta^{s-1} G_{s-1,s} \end{array} \right) \mathcal{U},
$$

where $\mathcal{U}$ is a suitable permutation matrix and $G_{t,j} \in \mathbb{M}_{k_t \times k_j}(R)$. The $s$-tuple $(k_0, k_1, \ldots, k_{s-1})$ is called type of $G$ and $\text{rank}(G) = k_0 + k_1 + \cdots + k_{s-1}$ is the rank of $G$.

Proposition 3. (5) Proposition 3.2, Theorem 3.5] Each $R$-linear code $\mathcal{C}$ admits a generator matrix $G$ standard form. Moreover, the type is the same for any generator matrix in standard form for $\mathcal{C}$.

Definition 3.1. Let $\mathcal{C}$ be an $R$-linear code and $G$ be a generator matrix $G$ standard form. The rows of $G$ form an $R$-basis for $\mathcal{C}$, so-called standard $R$-basis for $\mathcal{C}$.

So the type and the rank are the invariants of $\mathcal{C}$, and henceforth we have the following definition.

Definition 3.2. Let $\mathcal{C}$ be an $R$-linear code.

(1) The type of $\mathcal{C}$ is the type of a generator matrix of $\mathcal{C}$ in standard form.

(2) The rank of $\mathcal{C}$, denoted $\text{rank}_R(\mathcal{C})$, is the rank of a generator matrix of $\mathcal{C}$ in standard form.

Obviously, any $R$-linear code $\mathcal{C}$ of length $\ell$ of type $(k_0, k_1, \ldots, k_{s-1})$ is free if and only if the rank of $\mathcal{C}$ is $k_0$, and $k_1 = k_2 = \cdots = k_{s-1} = 0$. It defines the scalar product on $R^\ell$ by: $\mathbf{a} \cdot \mathbf{b}^T := \sum_{i=0}^{\ell-1} a_i b_i$, where $\mathbf{b}^T$ is the transpose of $\mathbf{b}$. Let $\mathcal{C}$ be an $R$-linear code of length $\ell$. The dual code of $\mathcal{C}$, denoted $\mathcal{C}^\perp$, is an $R$-linear code of length $\ell$, is defined by: $\mathcal{C}^\perp := \{ \mathbf{a} \in R^\ell : \mathbf{a} \cdot \mathbf{b}^T = 0_R \text{ for all } \mathbf{b} \in \mathcal{C} \}$. A generator matrix of $\mathcal{C}^\perp$, is called parity-check matrix of $\mathcal{C}$. We recall that an $R$-linear code $\mathcal{C}$ is self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^\perp$. An $R$-linear code $\mathcal{C}$ is self-dual if $\mathcal{C} = \mathcal{C}^\perp$.

Proposition 4. (7) Theorem 3.1] Let $\mathcal{C}$ and $\mathcal{C}'$ be $R$-linear codes of length $\ell$. Then $(\mathcal{C} + \mathcal{C}')^\perp = \mathcal{C}^\perp \cap \mathcal{C}'^\perp$, $(\mathcal{C} \cap \mathcal{C}')^\perp = \mathcal{C}^\perp + \mathcal{C}'^\perp$, and $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. 


Proposition 5. ([11] Theorem 3.10) Let $C$ be an $R$-linear code of length $\ell$, of type $(k_0, k_1, \ldots, k_{s-1})$. Then

1. the type of $C^\perp$ is $(\ell - k, k_{s-1}, \ldots, k_1)$, where $k := k_0 + k_1 + \cdots + k_{s-1}$.
2. $|C| = q^{\sum_{i=0}^{s-1} (s-i)k_i}$, where $|C|$ denotes the number of elements of $C$.

Definition 3.3. Let $R$ be a finite chain ring of invariants $(q, s)$ and $\theta$ be a generator of $J(R)$. Let $C$ be an $R$-linear code of rank $k$.

1. The $R$-linear subcode $\text{Annih}_C(\theta) := \{\mathbf{c} \in C : \theta \mathbf{c} = \mathbf{0}\}$, of $C$, is called the annihilator of $C$.
2. The residue code of $C$ is the $\mathbb{F}_q$-linear code $\pi(C) := \{\mathbf{c} : \mathbf{c} \in C\}$.  

Remark 2. Let $C$ be an $R$-linear code with generator matrix $G$, as in (3). Then a generator matrix of $\text{Annih}_C(\theta)$ is

$$\theta^{s-1} \begin{pmatrix} I_{k_0} & G_{0,1} & G_{0,2} & \cdots & G_{0,s-1} & G_{0,s} \\ 0 & I_{k_1} & G_{1,2} & \cdots & G_{1,s-1} & G_{1,s} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & I_{k_{s-1}} & G_{s-1,s} \end{pmatrix} U.$$ 

The Hamming distance of an $R$-linear code $C$ of length $\ell$, is defined as:

$$\text{wt}(C) := \min\{\text{wt}(\mathbf{c}) : \mathbf{c} \in C, \mathbf{c} \neq \mathbf{0}\},$$

where $\text{wt}(\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\ell-1}) := \{|j \in \sum_{j} : c_j \neq 0_R|\}$.

Theorem 3. Let $C$ be an $R$-linear code. Then $\text{wt}(C) = \text{wt}(\text{Annih}_C(\theta))$.

Proof. We set $\mathcal{A} := \text{Annih}_C(\theta)$. Let $\mathbf{c}$ in $C$ with $\text{wt}(\mathbf{c}) = \text{wt}(C)$. Let $t$ be the least positive integer such that $\theta^t \mathbf{c} = \mathbf{0}$. Then $t \neq 0$ and $\theta^t \mathbf{c} \in \mathcal{A} \setminus \{\mathbf{0}\}$. Hence we must have: $\text{wt}(\mathcal{A}) \leq \text{wt}(\theta^t \mathbf{c}) \leq \text{wt}(\mathbf{c}) = \text{wt}(\mathcal{A})$. Hence the equality $\text{wt}(C) = \text{wt}(\mathcal{A})$.

Corollary 1. Let $C$ be a free $R$-linear codes with generator matrix in standard form $G$, and $G \in \mathcal{M}_{k \times \ell}(\Gamma(R))$. Then $\text{wt}(\pi(C)) = \text{wt}(C)$ and $\pi(G)$ is a generator matrix in standard form for $\pi(C)$.

Example 3.1. Let $C$ be the $\mathbb{Z}_8$-linear code with generator matrix

$$\begin{pmatrix} 1 & 1 & 3 & 4 & 0 & 5 \\ 0 & 2 & 2 & 6 & 4 & 0 \\ 0 & 0 & 4 & 0 & 4 & 4 \end{pmatrix}.$$  

The matrix $G$ is in standard form. So the type of $C$ is $(1,1,1)$. By Remark 2, a generator matrix in standard form of $\mathcal{A} := \text{Annih}_C(2)$ is

$$\begin{pmatrix} 4 & 0 & 0 & 4 & 0 & 4 \\ 0 & 4 & 0 & 4 & 4 & 4 \\ 0 & 0 & 4 & 0 & 4 & 4 \end{pmatrix}.$$  

So by Theorem 3, we have $\text{wt}(C) = 3$.

3.2. Galois closure of a linear code over a finite chain ring. Let $B$ be an $S$-linear code of length $\ell$. Then $\sigma(B) := \{(\sigma(c_0), \ldots, \sigma(c_{\ell-1})) : (c_0, \ldots, c_{\ell-1}) \in B\}$ is also an $S$-linear code of length $\ell$. We say that the $S$-linear code $B$ is called $\sigma$-invariant if $\sigma(B) = B$. The subring subcode of $B$ to $R$, is an $R$-linear code $\text{Res}_R(B) := B \cap R_\ell$, and the trace code of $B$ over $R$, is the $R$-linear code

$$\text{Tr}_R^S(B) := \left\{(\text{Tr}_R^S(c_0), \ldots, \text{Tr}_R^S(c_{\ell-1})) : (c_0, \ldots, c_{\ell-1}) \in B\right\}.$$  

It is clear that $\text{Tr}_R^S(\sigma(B)) = \text{Tr}_R^S(B)$. The extension code of an $R$-linear code $C$ to $S$, is the $S$-linear code $\text{Ext}_S(C)$, formed by taking all combinations of codewords of $C$. The following theorem generalizes Delsarte’s celebrated result (see [13] Ch.7.$\S$8. Theorem 11.]).

Theorem 4. ([9] Theorem 3). Let $B$ be an $S$-linear code then $\text{Tr}_R^S(B^\perp) = \text{Res}_R(B^\perp)$, where $B^\perp$ is the dual to $B$ with respect to the usual scalar product, and $\text{Res}_R(B^\perp)$ is the dual of $\text{Res}_R(B)$ in $R_\ell$.

Definition 3.4. Let $B$ be an $S$-linear code. The $\sigma$-closure of $B$, is the smallest $\sigma$-invariant $S$-linear code $\overline{B}$, containing $B$.  

Proposition 6. Let $\mathcal{B}$ be an $S$-linear code. Then $\widetilde{\mathcal{B}} = \sum_{i=0}^{m-1} \sigma^i(\mathcal{B})$ and $\text{Tr}_{R}^S(\mathcal{B}) = \text{Tr}_{R}^S(\widetilde{\mathcal{B}})$.

Proof. We have $\mathcal{B} \subseteq \widetilde{\mathcal{B}}$ and $\sigma(\mathcal{B}) = \mathcal{B}$, by Definition 3.3 of $\mathcal{B}$. So $\sigma^i(\mathcal{B}) \subseteq \widetilde{\mathcal{B}}$, for all $i \in \{0, 1, \ldots, m - 1\}$. Hence $\sum_{i=0}^{m-1} \sigma^i(\mathcal{B}) \subseteq \widetilde{\mathcal{B}}$. Since $\sigma \left( \sum_{i=0}^{m-1} \sigma^i(\mathcal{B}) \right) = \sum_{i=0}^{m-1} \sigma^i(\mathcal{B})$ and $\mathcal{B} \subseteq \sum_{i=0}^{m-1} \sigma^i(\mathcal{B})$, as $\widetilde{\mathcal{B}}$ is the smallest $S$-linear code containing $\mathcal{B}$, which is $\sigma$-invariant, it follows $\widetilde{\mathcal{B}} \subseteq \sum_{i=0}^{m-1} \sigma^i(\mathcal{B})$. Hence $\widetilde{\mathcal{B}} = \sum_{i=0}^{m-1} \sigma^i(\mathcal{B})$. Thanks to Proposition 1.], $\text{Tr}_{R}^S(\mathcal{B}) = \text{Tr}_{R}^S(\widetilde{\mathcal{B}})$. □

The following Theorem summarizes the obtained results in [9].

Theorem 5. Let $\mathcal{B}$ be an $S$-linear code and $\sigma$ be a generator of $\text{Aut}_R(S)$. Then the following statements are equivalent:

1. $\mathcal{B}$ is $\sigma$-invariant;
2. $\text{Tr}_{R}^S(\mathcal{B}) = \text{Res}_{R}(\mathcal{B})$;
3. $\mathcal{B}$, and $\text{Res}_{R}(\mathcal{B})$ have the same type;
4. $\text{Res}_{R}(\mathcal{B})^\perp = \text{Res}_{R}(\mathcal{B}^\perp)$.

Proof. Let $\mathcal{B}$ be an $S$-linear code.

1. $\Leftrightarrow$ 2.: Thanks to Theorem 2.]
2. $\Leftrightarrow$ 3.: Since any $R$-basis of $\text{Res}_{R}(\mathcal{B})$ is also an $S$-basis of $\text{Ext}_S(\text{Res}_{R}(\mathcal{B}))$. Thanks to Theorem 1, we deduce that $\mathcal{B} = \text{Ext}_S\left(\text{Tr}_{R}^S(\mathcal{B})\right)$ if and only if $\mathcal{B}$ and $\text{Res}_{R}(\mathcal{B})$ have the same type.
3. $\Leftrightarrow$ 4.: By Delsarte’s Theorem, we have $\text{Res}_{R}(\mathcal{B}^\perp) = \text{Tr}_{R}^S(\mathcal{B})^\perp$. Thus, $\text{Tr}_{R}^S(\mathcal{B}) = \text{Res}_{R}(\mathcal{B})$ is equivalent to $\text{Res}_{R}(\mathcal{B}^\perp) = \text{Res}_{R}(\mathcal{B})^\perp$.

□

4. Cyclotomic partitions

Let $\ell$ be a positive integer and $q$ a power of a prime number with the property $\gcd(\ell, q) = 1$.

Consider $\mathbb{Z}_\ell$, the ring of integers modulo $\ell$ and the underlying set $\Sigma_\ell := \{0, 1, \ldots, \ell - 1\}$ of $\mathbb{Z}_\ell$. Let $A$ be a subset of $\Sigma_\ell$. The set of multiples of $u$ in $A$ is $uA := \{uz \mod \ell : z \in A\}$. The $q$-closure of a subset $A$ of $\Sigma_\ell$, is $\ell_q(A) := \bigcup_{i \in \mathbb{N}} q^iA$. We remark that $\ell_q(0) = 0$.

Definition 4.1. Let $z \in \Sigma_\ell$. The $q$-cyclotomic coset modulo $\ell$, containing $z$, denoted $\ell_q(z)$, is the Galois closure of $\{z\}$.

One denotes by $\mathcal{R}_\ell(q)$ the set of $q$-closure subsets of $\Sigma_\ell$, and by $2^{\Sigma_\ell}$ the set of subsets of $\Sigma_\ell$. Obviously, the $q$-cyclotomic cosets modulo $\ell$, form a partition of $\Sigma_\ell$. Let $\Sigma_\ell(q)$ be a set of representatives of each $q$-cyclotomic cosets modulo $\ell$.

Proposition 7. [2 Proposition 5.2] We have $|\Sigma_\ell(q)| = \sum_{d | \ell} \phi(d) \phi_{\ell}(q)$, where $\phi(.)$ is the Euler function and $\phi_{\ell}(q) := \min\{ i \in \mathbb{N} \setminus \{0\} : q^i \equiv 1 \mod \ell \}$.

We introduce the binary and unary operations on $\Sigma_\ell$. These operations are necessary in the following section, for the construction of cyclic linear codes.

Definition 4.2. Let $z \in \Sigma_\ell$ and $A, B$ be two subsets of $\Sigma_\ell$.

1. The opposite of $A$ is $-A := \{z - z : z \in A\}$.
2. The complementary of $A$ is $\overline{A} := \{z \in \Sigma_\ell : z \notin A\}$.
3. The dual of $A$ is $A^\circ := -A$. 

Let $L$ be a nonempty set. We recall that the quintuple $\langle L; \lor, \land; 0, 1 \rangle$ is a bounded lattice if the following identities are satisfied:

1. for all $x, y \in L$: $x \lor y = y \lor x$ and $x \land y = y \land x$;
2. for all $x, y, z \in L$: $(x \lor y) \lor z = x \lor (y \lor z)$ and $(x \land y) \land z = x \land (y \land z)$;
3. for every $x \in L$: $x \lor 0 = x$ and $x \land 1 = x$;
4. for every $x \in L$: $x \lor (x \land y) = x$ and $x = x \land (x \lor y)$;
5. for every $x \in L$, $x \land 0 = 0$ and $x \lor 1 = 1$.

Moreover, a lattice $\langle L; \lor, \land \rangle$ is distributive if for all $x, y, z \in L$, $(x \lor y) \land z = (x \land y) \lor (y \land z)$, and a lattice $\langle L; \lor, \land \rangle$ is modular if for all $x, y, z \in L$, $x \land (y \lor z) = (x \land y) \lor (x \land z)$. A more general and detailed treatment of the topic can be found in textbooks on Lattices such as [3].

**Example 4.1.** The lattice $\langle 2^E; \lor, \cap; \emptyset, E \rangle$ is distributive and bounded, where $2^E$ is the power set of a set $E$. The lattice $\langle L_\ell(R); +, \cap; \{0\}, R^\ell \rangle$ is modular and bounded, where $L_\ell(R)$ is the set of all $R$-linear codes of length $\ell$.

The relationships among these operations, are given in the following:

**Proposition 8.** The lattice $\langle \mathfrak{N}_\ell(q); \lor, \cap; \emptyset, \Sigma_\ell(q) \rangle$ is bounded and distributive. Moreover, the map

$$\mathfrak{C}_q : 2^{\Sigma_\ell} \rightarrow \mathfrak{N}_\ell(q)$$

$$A \mapsto \bigcup_{i \in \mathbb{N}} q^i A$$

is a lattices epimorphism with $\mathfrak{C}_q(-A) = -\mathfrak{C}_q(A)$, $\mathfrak{C}_q(A) = \overline{\mathfrak{C}_q(A)}$, and $A \subseteq B$ implies $\mathfrak{C}_q(A) \subseteq \mathfrak{C}_q(B)$.

**Definition 4.3.** The $(s+1)$-tuple $(A_0, A_1, \ldots, A_s)$ is an $(q, s)$-cyclotomic partition modulo $\ell$, if there exists a unique map $\lambda : \Sigma_\ell(q) \rightarrow \{0, 1, \ldots, s\}$, such that $A_t = \mathfrak{C}_q(\lambda^{-1}(\{t\}))$, for every $0 \leq t \leq s$.

We denote by $\mathfrak{N}_\ell(q, s)$ the set of $(q, s)$-cyclotomic partitions modulo $\ell$. It is easy to see that

$$\mathfrak{N}_\ell(q, s) := \{(A_0, A_1, \ldots, A_s) : \exists \lambda \in \{0, 1, \ldots, s\}^\Sigma_\ell(q) \left( A_t = \lambda^{-1}(\{t\}) \right) \}$$

By Definition 4.3, we see that $|\mathfrak{N}_\ell(q, s)| = (s+1)^{\Sigma_\ell(q)}$.

**Example 4.2.** We take $\ell = 20, q = 3$, and $s = 2$. The $q$-cyclotomic cosets modulo $\ell$, are:

$$\mathfrak{C}_q(\{0\}) = \{0\}, \mathfrak{C}_q(\{3\}) = \{5, 15\}, \mathfrak{C}_q(\{10\}) = \{10\},$$

and

$$\mathfrak{C}_q(\{1\}) = \{1, 3, 9, 7\}; \quad \mathfrak{C}_q(\{2\}) = \{2, 6, 18, 14\};$$
$$\mathfrak{C}_q(\{4\}) = \{4, 12, 16, 8\}; \quad \mathfrak{C}_q(\{11\}) = \{11, 13, 19, 17\}.$$

So $\Sigma_\ell(q) = \{0, 1, 2, 4, 5, 10, 11\}$. We remark that $\mathfrak{C}_q(-z) = \mathfrak{C}_q(\{z\})$, for every $z \in \{0, 2, 4, 5, 10\}$. We set $I := \{0; 1; 2; \ldots; 10\}$. We have $A := \mathfrak{C}_q(I) = \mathfrak{C}_q(\{0, 1, 2, 4, 5, 10\})$, $-A := \mathfrak{C}_q(\{2, 4, 5, 10, 11\})$, and $A^c := \mathfrak{C}_q(\{1\})$.

We remark that the maps

$$\psi : \mathfrak{N}_\ell(q) \rightarrow \mathfrak{N}_\ell(q, s)$$
$$A \mapsto (A, 0, 0, \ldots, A)$$

and

$$\varphi : \mathfrak{N}_\ell(q, s) \rightarrow \mathfrak{N}_\ell(q)$$
$$A_0 \mapsto (A_0, A_1, \ldots, A_s)$$

satisfy $\varphi \psi(A) = A$, and $\psi \varphi(A_0, A_1, \ldots, A_s) = (A_0, 0, \ldots, 0, A_0)$ for every $A \in \mathfrak{N}_\ell(q)$, for every $(A_0, A_1, \ldots, A_s) \in \mathfrak{N}_\ell(q, s)$.

5. **Free Cyclic linear codes over finite chain rings**

Let $R$ be a finite chain ring of invariants $(q, s)$ and $\ell$ be a positive integer such that $\gcd(q, \ell) = 1$. Then there exists a positive integer $m$ such that $q^m \equiv 1 \pmod{\ell}$ and $q^{m-1} \not\equiv 1 \pmod{\ell}$. In this section, we give the trace representation of cyclic $R$-linear codes of length $\ell$. 
5.1. **Cyclic polynomial codes over finite chain rings.** Let $S$ be the Galois extension of $R$ of degree $m$ and $\xi$ be a generator of $\Gamma(S)\setminus\{0\}$. Let $A := \{a_1, a_2, \ldots, a_k\}$ be a subset of $\Sigma_\ell$. One denotes by $P(S; A)$, the free $S$-submodule of $S[X]$ with free $S$-basis $\{X^a : a \in A\}$. Since $m$ is the smallest positive integer with $q^m \equiv 1 \pmod{\ell}$, we can write $\eta := \xi^\frac{\ell-1}{m}$ and the multiplicative order of $\eta$ is $\ell$. The evaluation

$$
\text{ev}_{\eta} : P(S; A) \to S^\ell
$$

is a bijective lattice homomorphism. The following result extends [Proposition 9.](#)

\[\text{Proposition 10.}\]

\[\text{Proof.}\]

We set $\Sigma := \ell \cdot \{1, \eta^a, \ldots, \eta^{(\ell-1)a}\}$. Then the shift of $c_a$ is $\eta^{-a}c_a$. Since $L_\eta(S; A)$ is $S$-linear, we have $\eta^{-a}c_a \in L_\eta(S; A)$. Hence $L_\eta(S; A)$ is cyclic.

\[\text{Proposition 9.}\]

Let $A$ be a subset of $\Sigma_\ell$. Then $L_\eta(S; A)$ is cyclic.

**Proof.** Consider the codeword $c_a = (1, \eta^a, \ldots, \eta^{(\ell-1)a})$. Then the shift of $c_a$ is $\eta^{-a}c_a$. Since $L_\eta(S; A)$ is $S$-linear, we have $\eta^{-a}c_a \in L_\eta(S; A)$. Hence $L_\eta(S; A)$ is cyclic.

\[\text{Proposition 10.}\]

Let $A, B$ be subsets of $\Sigma_\ell$. The following assertions holds:

1. $L_\eta(S; A)^\perp = L_\eta(S; A^\perp)$;
2. $L_\eta(S; A \cup B) = L_\eta(S; A) + L_\eta(S; B)$ and $L_\eta(S; A \cap B) = L_\eta(S; A \cap B) \cap L_\eta(S; B)$.

**Proof.** Let $A, B$ be subsets of $\Sigma_\ell$.

1. An $S$-basis of $L_\eta(S; A^\perp)$ is $\{c_a : -a \in \overline{A}\}$ where $c_a := (1, \eta^{-a}, \ldots, \eta^{-(\ell-1)a}) \in L_\eta(S; A^\perp)$. Then for all $b \in A$, $c_b := (1, \eta^b, \ldots, \eta^{b(\ell-1)}) \in L_\eta(S; A)$, we have $c_b c_a^T = \sum_{j=0}^{\ell-1} \eta^{(b-a)j}$, where $c_a^T$ is the transpose of $c_a$. It is easy to check that $\sum_{j=0}^{\ell-1} \eta^{ij} = 0$, when $i \not\equiv 0 \pmod{\ell}$. Since $0 < b-a < \ell$, we have $c_b c_a^T = 0$. So $L_\eta(S; A^\perp) \subseteq L_\eta(S; A)^\perp$. Comparison of cardinality yields $L_\eta(S; A)^\perp = L_\eta(S; A^\perp)$.

2. We have $L_\eta(S; A) \perp L_\eta(S; A \cup B)$, $L_\eta(S; B) \perp L_\eta(S; A \cup B)$. Therefore $L_\eta(S; A)^\perp L_\eta(S; B) \subseteq L_\eta(S; A \cap B)$ and $L_\eta(S; A) \cap L_\eta(S; B) \subseteq L_\eta(S; A \cap B)$. Since an $S$-basis of $L_\eta(S; A) + L_\eta(S; B)$, is $\{c_a : a \in A \cup (B \setminus A)\}$ and an $S$-basis of $L_\eta(S; A) \cap L_\eta(S; B)$, is $\{c_a : a \in A \cap B\}$. We have the equalities.

We set $L_\ell(S)$ the set of all cyclic polynomial codes of length $\ell$, over $S$. Then the quintuple $\langle L_\ell(S) ; +, \cap, \{\emptyset\}, S^\ell \rangle$, is a lattice and the map

$$
L_\eta(S; -) : 2_{\Sigma_\ell}^2 \to L_\ell(S)
$$

is a bijective lattices homomorphism. The following result extends [1] Theorem 5] to finite chain rings.
Definition 5.2. A subset $I$ of $\Sigma_\ell$ is an interval of length $\delta$ if there exists $(a, u) \in \Sigma_\ell \times \Sigma_\ell$ such that $\gcd(u, \ell) = 1$ and $I := \{ua, u(a + 1), \ldots, u(a + \delta - 1)\}$.

Theorem 6. If $A^\circ$ contains an interval of length $\delta$ then $\wt(L_\eta(S; A)) \geq \delta + 1$.

Proof. Let $I = \{ua, u(a + 1), \ldots, u(a + \delta - 1)\}$ be an interval containing in $A^\circ$, for some integer $u \in \Sigma_\ell$ such that $(u, \ell) = 1$. Then $\zeta := \eta^u$ is also a primitive root of $X^\ell - 1$. Suppose that $c$ is a nonzero codeword of $L_\eta(S; u^{-1}A)$ with $\wt(c) = \wt(L_\eta(S; u^{-1}A))$ and $\wt(L_\eta(S; u^{-1}A)) = \wt(L_\eta(S; A))$. Since $W_\delta$ is a parity-check matrix of $L_\eta(S; A)$ and $B := A^\circ$, it follows that $W_\delta c^T = 0$. Assume that $\text{Supp}(c) := \{j : c_j \neq 0\} \subseteq \{j_1, j_2, \ldots, j_\delta\}$. Consider $m := (c_{j_1}, c_{j_2}, \ldots, c_{j_\delta})$ where $c_{j_1}, c_{j_2}, \ldots, c_{j_\delta}$ are the first $\delta$ entries of $c = (\ldots, 0, c_{j_1}, 0, \ldots, 0, c_{j_2}, \ldots, 0, c_{j_\delta}, \ldots)$. Thus the equality $W_\delta c^T = 0$ becomes $Wm^T = 0$, where

$$W_\delta := \begin{pmatrix} \zeta^{j_1\delta} & \ldots & \zeta^{j_\delta\delta} \\ \vdots & \ddots & \vdots \\ \zeta^{(j_1+\delta-1)\delta} & \ldots & \zeta^{(j_\delta+\delta-1)\delta} \end{pmatrix}.$$ 

We have $\det(W_\delta) = -\zeta^\delta \prod_{1 \leq u < w \leq \delta} (\zeta^j - \zeta^w)$ is invertible since $\zeta \in \Gamma(S) \setminus \{0\}$. Therefore $m = 0$ which is a contradiction because $c \neq 0$. Hence $\wt(L_\eta(S; A)) \geq \delta + 1$. \hfill $\square$

Proposition 11. Let $S$ be a finite chain ring of invariants $(2^n, s)$ and $\ell := 2^s n - 1$, $A := \{1, 2, \ldots, d - 1\}$ where $d := 2^{s^n - 1}$. Then $L_\eta(S; A^\circ)$ is MDS and self-orthogonal.

Proof. We have $A$ is an interval of length $d - 1$ and $A^\circ := A \cup \{0\}$. So We have $L_\eta(S; A^\circ) = L_\eta(S; A) \oplus 1$. Thus $L_\eta(S; A^\circ)$ is self-orthogonal and $A^\circ$ is also an interval of length $d$. Thanks to BCH-bound of Theorem[6] we see that $L_\eta(S; A^\circ)$ is MDS. \hfill $\square$

5.2. Trace representation of free cyclic linear codes. We consider the trace-evaluation $\text{Tr}_R^S \circ \text{ev}_\eta : P_\eta(S; A) \to R'$, defined by:

$$\text{Tr}_R^S \circ \text{ev}_\eta(bX^n) := \left(\text{Tr}_R^S(b), \text{Tr}_R^S(b\eta^a), \ldots, \text{Tr}_R^S(b\eta^{a(\ell - 1)})\right),$$

for every $a \in A$ and for every $b \in R$. In the sequel, we write: $C_\eta(R; A) := \text{Tr}_R^S \left(L_\eta(S; A)\right)$, and $C_\eta(R; A)$ is a free cyclic $R$-linear code of length $\ell$. Let $C_\eta(R) := \{C_\eta(R; A) : A \subseteq \Sigma_\ell\}$ be the set of all free cyclic $R$-linear codes of length $\ell$.

Proposition 12. Let $A, B$ be two subsets of $\Sigma_\ell$. Then

1. $L_\eta(S; C_\eta(A))$ is the $\sigma$-closure of $L_\eta(S; A)$ and $C_\eta(R; A) = C_\eta(R; \sigma_\eta(A))$;
2. $\text{rank}_S(L_\eta(S; \sigma_\eta(A))) = |\sigma_\eta(A)|$;
3. $C_\eta(R; A^\perp) = C_\eta(R; A^\circ)$;
4. $C_\eta(R; A \cup B) = C_\eta(R; A) + C_\eta(R; B)$ and $C_\eta(R; A \cap B) = C_\eta(R; A) \cap C_\eta(R; B)$.

Proof. Let $A, B$ be two subsets of $\Sigma_\ell$.

1. On the one hand, it is clear that $\sigma(L_\eta(S; A)) = L_\eta(S; qA)$. So by Proposition[6] we have

$$\overline{L_\eta(S; A)} = \sum_{i=0}^{m-1} L_\eta(S; q^iA) = L_\eta(S; \bigcup_{i=0}^{m-1} q^iA).$$

Since $\overline{C_\eta(A)} = \bigcup_{i=0}^{m-1} q^iA$, we obtain $L_\eta(S; A) = L_\eta(S; \sigma_\eta(A))$ and the other hand, from Proposition[6] $C_\eta(R; A) = \text{Tr}(L_\eta(S; A)) = \text{Tr}(L_\eta(S; \sigma_\eta(A))) = C_\eta(R; \sigma_\eta(A)).$
(2) Theorem 3 yields $C_q(R; A) = \text{Tr}(L_q(S; C_q(A))) = \text{Res}_R(L_q(S; C_q(A)))$. So
\[\text{rank}_R(C_q(R; A)) = \text{rank}_S(L_q(S; C_q(A))) = |C_q(A)|.\]

(3) We have
\[C_q(R; A) = \text{Res}_R \left( L_q(S; C_q(A)) \right),\]
by Theorem 5
\[= \text{Res}_R \left( L_q(S; C_q(A)^c) \right),\]
by Proposition 10
\[= C_q(R; A^c).\]

(4) Thanks to Proposition 10, $C_q(R; A \cup B) = \text{Tr}(L_q(S; A \cup B)) = \text{Tr}(L_q(S; A)) + \text{Tr}(L_q(S; B))$. Since $\cap q(A) \cap q(B) = \emptyset$, we have \(\text{Tr}(L_q(S; A)) \cap \text{Tr}(L_q(S; B)) = \emptyset\).

\[\square\]

**Theorem 7.** Let $\ell, q$ be positive integers such that $q$ is a prime power and $\gcd(q, \ell) = 1$. Then the lattices $\langle C_q(R); +; \cap; \phi, R^\ell \rangle$ and $\langle R(q); \cup; \cap; \emptyset, \Sigma(q) \rangle$ are isomorphic.

**Proof.** It is obvious that the map $C_q(R) : R_q \to C_q(R)$, is a bijective. From Proposition 12 this map is a lattice isomorphism. \(\square\)

**Corollary 2.** Let $\ell, q$ be positive integers such that $q$ is a prime power and $\gcd(q, \ell) = 1$. Then the lattices $\langle \text{Cy}(F_q, \ell); +; \cap; \emptyset, R^\ell \rangle$ and $\langle C_q(R); +; \cap; \phi, R^\ell \rangle$ are isomorphic.

**Proof.** For all finite chain rings $R_1$ and $R_2$ of invariants $(q, s_1)$ and $(q, s_2)$ respectively. By Theorem 7 lattices $\langle C_q(R_1); +; \cap; \emptyset, R^\ell_1 \rangle$ and $\langle C_q(R_2); +; \cap; \emptyset, R^\ell_2 \rangle$ are isomorphic. Since $C_q(R_q) = \text{Cy}(F_q, \ell)$, we have the result. \(\square\)

**Lemma 1.** Let $R$ be a finite chain ring of invariants $(q, s)$ and $S$ be the Galois extension of $R$ of degree $m$. Let $z \in \Sigma_q$. Set $S_q = R[\xi]$, $m_z := |C_q(z)|$, $\eta := \xi^{m_z}$, and $\xi := \eta^{-z}$. Then the map
\[
\psi_z : R[\xi^2] \longrightarrow C_q(R; \{z\})
\]
\[a \longmapsto \text{Tr}_R^2 \left( \phi_{C_q}(aX^z) \right)\]
is an $R$-module isomorphism. Further $\psi_z \circ t_\ell = \tau_1 \circ \psi_z$, where $\tau_1$ is the cyclic shift and $t_\ell(a) = a\xi$, for all $a \in R[\eta]$.

**Proof.** It is clear that $a \in \text{Ker}(\psi_z)$ if and only if $a \in R[\xi^z] \cap R[\xi^z]$, where duality $\perp_{\text{Tr}}$ is with respect to trace form. As the trace bilinear form is nondegenerate, we have $S_q = R[\xi^z] \cap R[\xi^z]$ and $\text{Ker}(\psi_z) = \{0\}$. Hence $\psi_z$ is an $R$-module monomorphism. We remark that, $C_q(R; \{z\})$ is cyclic, if and only if $\psi_z \circ t_\ell = \tau_1 \circ \psi_z$. Finally, we have $S_q = R[\xi]$, and by Proposition 2 the ring $R[\xi^2]$ is the Galois extension of $R$ of degree $m_z$. Hence, $\psi_z$ is an $R$-module isomorphism. \(\square\)

**Definition 5.3.** A non trivial cyclic $R$-linear code $'c$ is said to be irreducible, if for all $R$-linear cyclic subcodes $'c_1$ and $'c_2$ of $'c$, the implication holds: $'c = 'c_1 \oplus 'c_2$, then $'c_1 = \emptyset$, or $'c_2 = \emptyset$.

**Proposition 13.** The irreducible cyclic $R$-linear codes are precisely $\theta^t C_q(R; \{z\})$, where $t \in \{0, 1, \ldots, s-1\}$ and $z \in \Sigma_q(q)$.

**Proof.** By Lemma 1 the free cyclic $R$-linear codes of length $\ell$ are $C_q(R; \{z\})$ where $z \in \{0, 1, \ldots, \ell-1\}$ and all the cyclic $R$-linear subcodes of each cyclic $R$-linear code, are irreducible. Let $'c$ be an irreducible cyclic $R$-linear code. Then $\langle 'c \rangle := \text{Ann}_R('c)$ is also an irreducible cyclic $R$-linear code and the $R$-linear code $\text{Quot}_c(-1, 'c)$ is cyclic and free. Let $\text{Quot}_c(-1, 'c)$ be the free cyclic $R$-linear code such that $\langle 'c \rangle \subset \text{Quot}_c(-1, 'c)$ and $\text{rank}_S('c) = \text{rank}_S(\text{Quot}_c(-1, 'c))$. Assume that $|A| > 1$. Then $C_q(R; A) = C_q(R; A_1) \oplus C_q(R; A_2)$ where $A_1 \cap A_2 = \emptyset$, $A_1 \neq \emptyset$ and $A_2 \neq \emptyset$. We have $'c \cap C_q(R; A_1) \neq \emptyset$, and $'c \cap C_q(R; A_2) \neq \emptyset$. Therefore $'c = ('c \cap C_q(R; A_1)) \oplus ('c \cap C_q(R; A_2))$. It is impossible, because $'c$ be an irreducible. So $|A| = 1$. Now, $'c \subseteq C_q(R; \{z\})$, it follows that $'c = \theta^t C_q(R; \{z\})$, for some $t \in \{0, 1, \ldots, s-1\}$. \(\square\)
Consider the map
\[ C_{\ell, R} : \mathbb{N}_\ell(q, s) \to \text{Cy}(R, \ell) \]
(5)
\[ (A_0, A_1, \cdots, A_s) \to \bigoplus_{t=0}^{s-1} \theta^t C_{\eta}(R; A_t). \]

In this section, on the one hand, we show that the map \( C_{\ell, R} : \mathbb{N}_\ell(q, s) \to \text{Cy}(R, \ell) \) is bijective and the other hand we equop the set \( C_{\ell, R} \) of binary operations \( \lor \) and \( \land \) such that \( C_{\ell, R} : \langle \mathbb{N}_\ell(q, s); \lor, \land \rangle \to \langle \text{Cy}(R, \ell); +, \cap \rangle \) is a lattice homomorphism.

The following theorem gives the number of cyclic codes and free cyclic codes over finite chain rings.

**Lemma 2.** [2] Theorem 5.1] Let \( R \) be a finite chain ring of invariants \( (q, s) \). Then the number of cyclic \( R \)-linear codes of length \( \ell \), is equal to \((s + 1)^{z(q)}\).

**Lemma 3.** [3] Corollary 11.] A finite lattice is distributive if and only if it is isomorphic to \( \langle 2^E; \cup, \cap, \emptyset, E \rangle \), where \( E \) is a finite set.

Lemmas 2 and 3 give the following fact.

**Theorem 8.** Let \( R \) be a finite chain ring of invariants \( (q, s) \) and \( \ell \) be a nonnegative integer such that \( \gcd(\ell, q) = 1 \). Then \( s \neq 1 \) if and only if \( \langle \text{Cy}(R, \ell); +, \cap, \emptyset, \ell^f \rangle \) is not distributive. Moreover, its sublattice \( \langle C(R); +, \cap, \emptyset, \ell^f \rangle \) is distributive.

We show that each cyclic \( R \)-linear code can be written as a direct sum of irreducibles in precisely one way.

**Lemma 4.** Let \( R \) be a finite chain ring of invariants \( (q, s) \). Then the map \( C_{\ell, R} : \mathbb{N}_\ell(q, s) \to \text{Cy}(R, \ell) \) is a bijection and the type of \( C_{\ell, R}(A) \) is \( (|\mathcal{C}_q(A_0)|, |\mathcal{C}_q(A_1)|, \cdots, |\mathcal{C}_q(A_{s-1})|) \), for some \( A := (A_0, A_1, \cdots, A_s) \in \mathbb{N}_\ell(q, s). \)

**Proof.** Let \( \mathcal{C} \) be an cyclic \( R \)-linear code of length \( \ell \). From Proposition 12 we have
\[ R^\ell = C_{\eta}(R; \Sigma_{\ell}(q)) = \bigoplus_{z \in \Sigma_{\ell}(q)} C_{\eta}(R; \{z\}) \]
and \( C_{\eta}(R; \{z\}) \)‘s are free irreducible cyclic \( R \)-linear codes. It follows that \( \mathcal{C} = \bigoplus z \in \Sigma_{\ell}(q) \mathcal{C}_{\eta}(R; \{z\}) \), where \( \mathcal{C}_{\eta}(R; \{z\}) = \mathcal{C}_{\eta}(R; \{z\}) \). By Proposition 13 \( \mathcal{C}_{\eta}(R; \{z\}) = \theta^t C_{\eta}(R; \{z\}) \), where \( t \in \{0, 1, \cdots, s\} \). Thus \( \bigoplus z \in \Sigma_{\ell}(q) \mathcal{C}_{\eta}(R; \{z\}) = C_{\ell, R}(A_0, A_1, \cdots, A_s) \), where \( A_t = \{z \in \Sigma_{\ell} : t = t\} \). Since \( |\mathbb{N}_\ell(q, s)| = (s + 1)^{z(q)} \), by Theorem 2 the uniqueness of \( A := (A_0, A_1, \cdots, A_s) \in \mathbb{N}_\ell(q, s) \) such that \( \mathcal{C} = C_{\ell, R}(A) \) is guaranteed. Moreover, for every \( t \in \{0, 1, \cdots, s - 1\} \), the cyclic \( R \)-linear code \( C_{\eta}(R; A_t) \) is free and \( \text{rank}_R(C_{\eta}(R; A_t)) = |\mathcal{C}_q(A_t)| \). Since the direct sum \( \bigoplus_{t \in \{0, 1, \cdots, s - 1\}} \theta^t C_{\eta}(R; A_t) \) gives the type of \( C_{\ell, R}(A) \), the type of \( C_{\ell, R}(A) \) is \( (k_0, k_1, \cdots, k_{s-1}) \), where \( k_t := |\mathcal{C}_q(A_t)| \), for every \( 0 \leq t < s - 1 \).

**Definition 6.1.** Let \( \mathcal{C} \) be a cyclic \( R \)-linear codes of length \( \ell \). The defining multiset of \( \mathcal{C} \) is the \((q, s)\)-cyclotomic partition \( \Delta \) modulo \( \ell \), such that \( \mathcal{C} = C_{\ell, R}(\Delta) \).

**Proposition 14.** Let \( A := (A_0, A_1, \cdots, A_s) \in \mathbb{N}_\ell(q, s) \) and \( t \in \{0, 1, \cdots, s - 1\} \). Then \( C_{\ell, R}(A)^t = C_{\ell, R}(A^t) \), where \( A^t := (-A_s, -A_{s-1}, \cdots, -A_1, -A_0) \).

**Proof.** Let \( A := (A_0, A_1, \cdots, A_s) \in \mathbb{N}_\ell(q, s) \). We have \( C_{\ell, R}(A)^t \supseteq \bigcap_{u=0}^{s-1} \left( \theta^{s-u} R^\ell + C_{\eta}(R; A_u^\ell) \right) \) and
\[ \theta^{s-t} C_{\eta}(R; -A_t) \subseteq \bigcap_{u=0}^{s-1} \left( \theta^{s-u} R^\ell + C_{\eta}(R; A_u^\ell) \right). \]
for every \( t \in \{1, 2, \cdots, s\} \). It follows that \( C_{\ell,R}(-A_s, -A_{s-1}, \cdots, -A_1, -A_0) \subseteq C_{\ell,R}(A) \). From Proposition\footnote{1} and Theorem\footnote{2} \( C_{\ell,R}(-A_s, -A_{s-1}, \cdots, -A_1, -A_0) \) and \( C_{\ell,R}(A) \) have the same type, we have

\[
C_{\ell,R}(A) = C_{\ell,R}(-A_s, -A_{s-1}, \cdots, -A_1, -A_0).
\]

\[\square\]

**Corollary 3.** Let \( A := (A_0, A_1, \cdots, A_t) \in \mathcal{M}_t(q, s) \). Then \( C_{\ell,R}(A) \) is self-dual if and only if \( A_t = -A_{s-t} \), for every \( t \in \{0, 1, \cdots, s\} \).

**Corollary 4.** Let \( R \) be a finite chain ring of invariants \((q, s)\) and \( s \) is an even integer. Then the following are equivalent.

1. There exists a subset \( A \) of \( \Sigma_t \) such that \( A \neq -A \).
2. The nontrivial self-dual cyclic \( R \)-linear codes of length \( \ell \) exist.

**Proof.** Let \( R \) be a finite chain ring of invariants \((q, s)\) and \( s \) is an even integer.

1. \( \Rightarrow \) 2.: Assume that there exists a subset \( A \) of \( \Sigma_t \) such that \( C_q(A) \neq -C_q(A) \). Set \( u = \frac{s}{2} \), and \( B := A \cup (-A) \). Consider

\[
\mathcal{C} := C_{\ell,R}(\mathcal{C}_q(A) = \cdots \cup A_{u-1} A_u A_{u+1} \cdots),
\]

where \( A_{u-1} = C_q(A) \), \( A_u = C_q(B) \) and \( A_{u+1} = -A_{u-1} \). We have \( A_{u+1} = A_{u-1} = 0 \), \( A = -A \), and \( A_t = -A_{s-t} = 0 \), for every \( t \in \{0, 1, \cdots, s-2\} \). Thanks to Corollary\footnote{3} we can affirm that \( \mathcal{C} \) is self-dual.

2. \( \Rightarrow \) 1.: Now, we assume that \( \mathcal{C} \) is self-dual cyclic \( R \)-linear codes of length \( \ell \) and every subset \( A \) of \( \Sigma_t \) satisfies \( A = -A \). Set \( \mathcal{C} := C_{\ell,R}(A_0, A_1, A_2, \cdots, A_s) \). From Corollary\footnote{3} \( A_t = -A_{s-t} \), for every \( t \in \{0, 1, \cdots, s\} \). Since \( -A_{s-t} = A_{s-t} \), we have \( A_t = -A_{s-t} = 0 \), for every \( t \in \{0, 1, \cdots, s\} \). Therefore, \( \mathcal{C} = C_{\ell,R}(\cdots \cup A_{\ell} q, 0 \cdots) \) is the trivial self-dual code.

\[\square\]

We point out that the number of cyclic self-dual linear codes over finite chain rings has been given in \[2\]. In order to determine the defining multiset of the sum, and the intersection of \( R \)-linear cyclic codes, we extend the binary operation \( \cup \) of \( \mathcal{M}_t(q, s) \) to \( \mathcal{M}_t(q, s) \) as follows:

**Notation 1.** Let \( A := (A_0, A_1, \cdots, A_s) \) and \( B := (B_0, B_1, \cdots, B_s) \) be elements of \( \mathcal{M}_t(q, s) \). Then

1. \( A \cup B := (C_0, C_1, \cdots, C_s) \), where \( C_0 := A_0 \cup B_0 \) and \( C_t := (A_t \cup B_t) \setminus \bigcup_{u=0}^{t-1} C_u \), for every \( 0 < t \leq s \).
2. \( A \cap B := (C_0 \cap B_0, C_1 \cap B_1, \cdots, C_s \cap B_s) \).

**Theorem 9.** The map \( C_{\ell,R} : \mathcal{M}(\mathcal{M}_t(q, s); \cup, \cap, \emptyset, \emptyset, \Sigma_t(q)) \to \left\{ \text{Cy}(\mathbb{R}, \ell); +, \cap, \{\emptyset, \mathbb{R}\} \right\} \) is a lattice isomorphism, where \( \emptyset := (\emptyset, \emptyset, \emptyset, \emptyset, \Sigma_t(q)) \) and \( \Sigma_t(q) := (\Sigma_t(q), 0, 0, 0) \).

**Proof.** Let \( A := (A_0, A_1, \cdots, A_s) \in \mathcal{M}_t(q, s) \), and \( B := (B_0, B_1, \cdots, B_s) \in \mathcal{M}_t(q, s) \). Firstly, we have

\[
C_{\ell,R}(A) \cap C_{\ell,R}(B) = \sum_{t=0}^{s-1} \theta^t \left[ C_q(R; A_t) + C_q(R; B_t) \right], \text{by the associativity of } +,
\]

\[
= C_q(R; A_0 \cup B_0) + \theta C_q(R; A_1 \cup B_1) \setminus (A_0 \cup B_0) + \cdots \]

\[
\cdots + \theta^{s-1} C_q(R; (A_s \cup B_s) \setminus \left( \bigcup_{u=0}^{s-1} (A_u \cup B_u) \right)) + \cdots
\]

\[
= C_{\ell,R}(A \cup B).
\]

From Propositions\footnote{4} and\footnote{3} we deduce that \( C_{\ell,R}(A) \cap C_{\ell,R}(B) = C_{\ell,R}(A \cap B) \). Finally, by Lemma\footnote{4} we have the expected result.

\[\square\]
Proposition 15. (BCH-bound) Let ‘c’ be a cyclic \( R \)-linear code of length \( \ell \) and \( A := (A_0, A_1, \ldots, A_s) \) be the element of \( \mathbb{N}_s(q, s) \) such that ‘c’ := \( C_{d,R}(A) \) and \( C_{d,R} \left( \bigcup_{t=0}^{s-1} (-A_t) \right) \) contains an interval of length \( \delta \). Then

\[
\text{Annih}_{c}(\theta) = C_{d,R} \left( \theta, \ldots, \theta, \bigcup_{t=0}^{s-1} A_t, A_s \right) \text{ and } \text{wt}(c) \geq 1 + \delta.
\]

Proof. By Theorem 3 we have \( \text{Annih}_{c}(\theta) = C_{d,R} \left( \theta, \ldots, \theta, \bigcup_{t=0}^{s-1} A_t, A_s \right) \), and \( \text{wt}(c) = \text{wt} (\text{Annih}_{c}(\theta)) \). By Theorem 3 the lower bound on the minimum Hamming distance is obtained. \( \square \)

Example 6.1. We again pick \( \ell = 7 \), \( s = 2 \) and \( p = 2 \).

| \( C_{A_0,A_1,A_2} \) | BHC-bound | type : \( (|A_0|,|A_1|) \) | Cardinality : \( 2^{|A_0|+|A_1|} \) |
|---------------------|----------|----------------|-----------------|
| \( \mathcal{C}_0 := C_{\mathbb{Z}_2}(\{0,0,\mathbb{Z}_2(\{0,1,3\})} \) | 0 | \( (0,0) \) | 1 |
| \( \mathcal{C}_{26} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{0,1,3\}),0,0\} \) | 1 | \( (7,0) \) | 214 |
| \( \mathcal{C}_{23} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{1,3\}),\mathbb{Z}_2(\{0\}),0\} \) | 1 | \( (6,0) \) | 212 |
| \( \mathcal{C}_{22} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{0,3\}),\mathbb{Z}_2(\{1\}),0\} \) | 1 | \( (4,3) \) | 211 |
| \( \mathcal{C}_{24} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{0,1\}),\mathbb{Z}_2(\{3\}),0\} \) | 1 | \( (4,3) \) | 211 |
| \( \mathcal{C}_{21} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{3\}),\mathbb{Z}_2(\{0,1\}),0\} \) | 1 | \( (3,4) \) | 210 |
| \( \mathcal{C}_{20} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{1\}),\mathbb{Z}_2(\{0,3\}),0\} \) | 1 | \( (3,4) \) | 210 |
| \( \mathcal{C}_{17} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{0\}),\mathbb{Z}_2(\{1,3\}),0\} \) | 1 | \( (1,6) \) | 28 |
| \( \mathcal{C}_{14} := C_{\mathbb{Z}_2}(\{0,\mathbb{Z}_2(\{1,3\}),0\} \) | 1 | \( (0,7) \) | 27 |
| \( \mathcal{C}_{25} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{1,3\}),0,\mathbb{Z}_2(\{0\}) \) | 2 | \( (6,0) \) | 212 |
| \( \mathcal{C}_{19} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{1\}),\mathbb{Z}_2(\{3\}),\mathbb{Z}_2(\{0\}) \) | 2 | \( (3,3) \) | 29 |
| \( \mathcal{C}_{18} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{3\}),\mathbb{Z}_2(\{1\}),\mathbb{Z}_2(\{0\}) \) | 2 | \( (3,3) \) | 29 |
| \( \mathcal{C}_{9} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{1,3\}),\mathbb{Z}_2(\{0\}) \) | 2 | \( (0,6) \) | 26 |
| \( \mathcal{C}_{16} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{0,3\}),0,\mathbb{Z}_2(\{1\}) \) | 3 | \( (4,0) \) | 28 |
| \( \mathcal{C}_{13} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{3\}),\mathbb{Z}_2(\{0\}),\mathbb{Z}_2(\{1\}) \) | 3 | \( (3,1) \) | 27 |
| \( \mathcal{C}_{12} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{1\}),\mathbb{Z}_2(\{0\}),\mathbb{Z}_2(\{3\}) \) | 3 | \( (3,1) \) | 27 |
| \( \mathcal{C}_{8} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{0\}),\mathbb{Z}_2(\{1\}),\mathbb{Z}_2(\{3\}) \) | 3 | \( (1,3) \) | 25 |
| \( \mathcal{C}_{7} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{0\}),\mathbb{Z}_2(\{3\}),\mathbb{Z}_2(\{1\}) \) | 3 | \( (1,3) \) | 25 |
| \( \mathcal{C}_{6} := C_{\mathbb{Z}_2}(\{0,\mathbb{Z}_2(\{0,3\}),\mathbb{Z}_2(\{1\}) \) | 3 | \( (0,4) \) | 24 |
| \( \mathcal{C}_{11} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{1\}),0,\mathbb{Z}_2(\{0,3\}) \) | 4 | \( (3,0) \) | 26 |
| \( \mathcal{C}_{10} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{3\}),0,\mathbb{Z}_2(\{0,1\}) \) | 4 | \( (3,0) \) | 26 |
| \( \mathcal{C}_{4} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{1\}),\mathbb{Z}_2(\{0,3\}) \) | 4 | \( (0,3) \) | 23 |
| \( \mathcal{C}_{3} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{3\}),\mathbb{Z}_2(\{0,1\}) \) | 4 | \( (0,3) \) | 23 |
| \( \mathcal{C}_{15} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{0,1\}),0,\mathbb{Z}_2(\{3\}) \) | 4 | \( (4,0) \) | 28 |
| \( \mathcal{C}_{6} := C_{\mathbb{Z}_2}(\{0,\mathbb{Z}_2(\{0,1\}),\mathbb{Z}_2(\{3\}) \) | 4 | \( (0,4) \) | 24 |
| \( \mathcal{C}_{2} := C_{\mathbb{Z}_2}(\{\mathbb{Z}_2(\{0\}),0,\mathbb{Z}_2(\{1,3\}) \) | 7 | \( (1,0) \) | 22 |
| \( \mathcal{C}_{1} := C_{\mathbb{Z}_2}(\{0,\mathbb{Z}_2(\{0\}),\mathbb{Z}_2(\{1,3\}) \) | 7 | \( (0,1) \) | 21 |

Table 1. Cyclic \( \mathbb{Z}_4 \)-linear codes of length 7.

We have \( \mathcal{C}_8 + \mathcal{C}_{12} = \mathcal{C}_{15}, \mathcal{C}_{19} + \mathcal{C}_{12} = \mathcal{C}_{20}, \mathcal{C}_8^\perp = \mathcal{C}_{19} \) and \( \mathcal{C}_{12}^\perp = \mathcal{C}_{12} \). So \( \mathcal{C}_8 \cap \mathcal{C}_{12} = (\mathcal{C}_8^\perp + \mathcal{C}_{12}^\perp)^\perp = (\mathcal{C}_{19} + \mathcal{C}_{12})^\perp = \mathcal{C}_{20} = \mathcal{C}_6. \)

References

[1] Bierbrauer J., The Theory of Cyclic Codes and a Generalization to Additive Codes. Des.Codes.Cryptogr. 25(2): (2002), pp. 189-206.
[2] Batoul A., Guenda K., Gulliver T.A., On the self-dual cyclic codes over finite chain rings, Des. Codes Cryptogr. 70(1): (2014), pp. 347-358.
[3] Calderbank A.R., Sloane N.J.A., Modular and \( p \)-adic cyclic codes, Des. Codes Cryptogr. 6(1): (1995), pp. 21-35.
[4] DeMeyer F., Ingraham E., Separable Algebras Over Commutative Rings, Springer, 1971.
[5] H. Dinh, S.R. López-Permouthis, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory 50 (8) (2004), pp. 1728-1744.

[6] Grätze G., *Lattices Theory: First Concepts and Distributive Lattices*, Dover Publications, Inc., 2009.

[7] Honold T. and Landjev I., *Linear codes over finite chain rings*, Electron. J. Combinat., vol. 7, no. 1, (2000), pp. R11.

[8] P. Kanwar, S. R. López-Permouthis, *Cyclic codes over the integer modulo $p^m$*, Finite Fields Appl. Vol 3 (1997), pp. 334-352.

[9] Martínez-Moro E., Nicolas A.P., Rua F., *On trace codes and Galois invariance over finite commutative chain rings*, Finite Fields Appl. Vol. 22, (2013), pp. 114-121.

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

[11] Norton G.H., Salagean A., *On the Structure of Linear and Cyclic Codes over a Finite Chain Ring*, AAECC Vol. 10, (2000), pp. 489-506.

[12] Z. Wan, *Cyclic codes over Galois rings*, Alg. Colloq., 6 (1999), pp. 291-304.

[13] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Math. Library, vol. 16, North-Holland, Amsterdam, 1977.

**DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCES, UNIVERSITY OF YAOUNDE I, CAMEROON**

E-mail address: alexfotue@gmail.com

**DEPARTMENT OF MATHEMATICS, HIGHER TEACHERS TRAINING COLLEGE OF YAOUNDE, UNIVERSITY OF YAOUNDE I, CAMEROON**

E-mail address: cmouaha@yahoo.fr