CONTRACTION OF CYCLIC CODES OVER FINITE CHAIN RINGS

ALEXANDRE FOTUE TABUE AND CHRISTOPHE MOUJAHA

ABSTRACT. Let $R$ be a commutative finite chain ring of invariants $(q, s)$, and $\Gamma(R)$ the Teichmüller’s set of $R$. In this paper, the trace representation cyclic $R$-linear codes of length $\ell$, is presented, when $\gcd(\ell, q) = 1$. We will show that the contractions of some cyclic $R$-linear codes of length $u\ell$ are $\gamma$-constacyclic $R$-linear codes of length $\ell$, where $\gamma \in \Gamma(R) \setminus \{0_R\}$ and the multiplicative order of $\gamma$ is $u$.

1. INTRODUCTION

Let $R$ be finite chain ring with invariant $(q, s)$, $\pi : R \to \mathbb{F}_q$ be the natural ring epimorphism, and $\ell$ a positive integer such that $\gcd(q, \ell) = 1$. Let $R^\times$ be the group of units of $R$, and $\gamma \in R^\times$. An $R$-linear code $C$ of length $\gamma$ is $\gamma$-constacyclic if $\tau_\gamma(C) = C$, where $\tau_\gamma : R^s \to R^t$, is the $\gamma$-constashift operator, defined by $\tau_\gamma(c_0, c_1, \cdots, c_{\ell-1}) = (\gamma c_{\ell-1}, c_0, \cdots, c_{\ell-2})$. Especially, cyclic and negacyclic linear codes correspond to $\gamma = 1_R$ and $\gamma = -1_R$, respectively (see [4]). The residue code of $R$-linear code $C$ is the $\mathbb{F}_q$-linear code $\pi(C) := \{(\pi(c_0), \pi(c_1), \cdots, \pi(c_{\ell-1})) : (c_0, c_1, \cdots, c_{\ell-1}) \in C\}$. The equality $\pi(\tau_\gamma(C)) = \tau_{\pi(\gamma)}(\pi(C))$, enables to see that the residue code of any $\gamma$-constacyclic $R$-linear code, is an $\pi(\gamma)$-constacyclic $\mathbb{F}_q$-linear code. In the literature [3, 5, 10, 11, 12], the class of $\gamma$-constacyclic $R$-linear codes, which are studied, have the following property $\gamma \in 1_R + R\theta$.

In this paper, on the one hand, we will describe each $\gamma$-constacyclic $R$-linear code of length $\ell$, as contraction of a cyclic $R$-linear code of length $u\ell$, and on the other hand, we will investigate on the structure of $\gamma$-constacyclic $R$-linear codes, where $\gamma \in \Gamma(R) \setminus \{0_R\}$.

The present paper is organized as follows. In Sect. 2 we present results which will be used in the following sections. Sect. 3 studies the subring subcode and trace code of a linear codes over finite chain rings. In Sect. 4 the trace-description of cyclic linear codes over finite chain rings is presented. For any $\gamma \in \Gamma(R)$, we proceed to investigate on the structural properties of $\gamma$-constacyclic codes of arbitrary length $\ell$, in Sect. 5.

2. BACKGROUND ON FINITE CHAIN RINGS

Throughout of this section, $R$ is a commutative ring with identity and $J(R)$ denoted the Jacobson radical of $R$, and $R^\times$ denotes the multiplicative group of units of $R$. The definitions and results on the finite chain rings are extracted in monographs [6, 8].

Definition 2.1. We say that $R$ is a finite chain ring of invariants $(q, s)$, if:

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

The map $\pi : R \to \mathbb{F}_q$ denotes the canonical projection.

Lemma 1. Let $R$ be a finite chain ring of invariants $(q, s)$, and $\theta$ be a generator of $J(R)$. Then

1. $R^\times = R \setminus J(R)$, and the ideals of $R$ are precisely $J(R)^t = R\theta^t$, where $t \in \{0, 1, \cdots, s\}$;
2. $|R^\times| = q^{(s-1)(q-1)}$ and $|J(R)^t| = q^{q-t}$, for every $t \in \{0, 1, \cdots, s\}$.

Theorem 1. Let $R$ be a finite chain ring of invariants $(q, s)$, and $\theta$ be a generator of $J(R)$. Then
(1) \( R^* = \Gamma(R)^* \cdot (1 + R\theta) \), and \( \Gamma(R)^* \cong \mathbb{F}_q \setminus \{0\} \) (as multiplicative group) where \( \Gamma(R)^* := \{ b \in R : b \neq 0, b\theta = b \} \); 
(2) \( \Gamma(R)^* \) is a cyclic subgroup of \( R^* \), of order \( q - 1 \) and \( |1_R + R\theta| = q^{s-1} \); 
(3) for every element \( a \in R \), there exists a unique \( (a_0, a_1, \cdots, a_{s-1}) \in \Gamma(R)^s \), such that \( a = a_0 + a_1 \theta + \cdots + a_{s-1} \theta^{s-1} \).

**Definition 2.2.** Let \( R \) be a finite chain ring of invariants \( (q, s) \), and \( \theta \) be a generator of \( J(R) \). The set \( \Gamma(R) = \Gamma(R)^* \cup \{0\} \) 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 \( R \) is a subring of \( S \) and \( 1_R = 1_S \). We denote by \( \text{rank}_R(S) \), the rank of \( R \)-module \( S \). We denote by \( \text{Aut}_R(S) \), the group of ring automorphisms of \( S \) which fix the elements of \( R \).

**Definition 2.3.** Let \( R \) be a finite chain ring of invariants \( (q, s) \). We say that the finite chain ring \( S \) is the Galois extension of \( R \) of degree \( m \), if

1. \( S|R \) is unramified, i.e. \( J(S) = J(R)|S \);
2. \( S|R \) is normal, i.e. \( R := \{ a \in S : \varphi(a) = a \ for \ all \ \varphi \in \text{Aut}_R(S) \} \).

**Proposition 1.** Let \( R \) be a finite chain ring of invariants \( (q, s) \). Let \( S \) be the Galois extension of \( R \) of degree \( m \). Then

1. \( S \) is a free \( R \)-module of rank \( m \);
2. \( \text{Aut}_R(S) \) is cyclic of order \( m \);
3. \( S = R[\xi] \) where \( \xi \) is a generator of \( \Gamma(S) \).

**Definition 2.4.** Let \( S|R \) be the Galois extension of finite chain rings of degree \( m \) and \( \sigma \) be a generator of \( \text{Aut}_R(S) \). The map \( \text{Tr}_R^S := \sum_{i=0}^{m-1} \sigma_i \), is called the trace map of the Galois extension \( S|R \).

**Proposition 2.** [6 Chap. XIV] Let \( S|T \) and \( R|T \) be Galois extensions of finite chain rings. Then

1. \( R = \{ a \in S : \sigma(a) = a \ for \ all \ \sigma \in \text{Aut}_R(S) \} \);
2. the bilinear form \( \varphi : (a, b) \rightarrow \text{Tr}_R^S(ab) \) is nondegenerate;
3. \( \text{Tr}_R^S \) is a generator of \( S \)-module \( \text{Hom}_R(S, R) \), and \( \text{Tr}_T^S \circ \text{Tr}_R^S = \text{Tr}_T^S \).

3. **Linear codes over finite chain rings**

Recall that an \( R \)-linear code of length \( \ell \) is an \( R \)-submodule of \( R^\ell \). We say that an \( R \)-linear code is free if it is a free as \( R \)-module.

3.1. **Type and rank of a linear code.** A matrix \( G \) 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 the other rows of \( G \). We say that \( G \) is a generator matrix in standard form if

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

where \( U \) is a suitable permutation matrix. The \( s \)-tuple \( (k_0, k_1, \cdots, k_{s-1}) \) is called type of \( G \) and \( \text{rank}(G) := k_0 + k_1 + \cdots + k_{s-1} \) is the rank of \( G \).

**Proposition 3.** ([9 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 \( \mathcal{C} \).

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

**Definition 3.1.** Let \( \mathcal{C} \) be an \( R \)-linear code.
Proof. Delsarte’s celebrated result (see [7, Theorem 3.10]) Let \( \mathcal{C} \) be an \( R \)-linear code of length \( \ell \) and 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 \( \ell \), define by: 
\[
\mathcal{C}^\perp := \{ \mathbf{a} \in R^\ell : \mathbf{a} \cdot \mathbf{b}^T = 0 \text{ for all } \mathbf{c} \in \mathcal{C} \}. 
\]
A generator matrix of \( \mathcal{C}^\perp \), is called parity-check matrix of \( \mathcal{C} \).

**Proposition 4.** (\cite{7} Theorem 3.10) Let \( \mathcal{C} \) be an \( R \)-linear code of length \( \ell \) and of type \((k_0, k_1, \ldots, k_{s-1})\).

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

### 3.2 Galois closure of a linear code over a finite chain ring

Let \( \mathcal{B} \) be an \( S \)-linear codes of length \( \ell \). Then
\[
\sigma(\mathcal{B}) := \{(\sigma(\mathbf{c}_0), \ldots, \sigma(\mathbf{c}_{\ell-1})) : (\mathbf{c}_0, \ldots, \mathbf{c}_{\ell-1}) \in \mathcal{B} \}
\]
is also an \( S \)-linear codes of length \( \ell \). We say that the \( S \)-linear code \( \mathcal{B} \) is call \( \sigma \)-invariant if \( \sigma(\mathcal{B}) = \mathcal{B} \). The subring subcode of \( \mathcal{B} \) to \( R \), is \( R \)-linear code \( \text{Res}_R(\mathcal{B}) := \mathcal{B} \cap R^\ell \), and the trace code of \( \mathcal{B} \) over \( R \), is the \( R \)-linear code
\[
\text{Tr}_R(\mathcal{B}) := \{(\text{Tr}_R^S(\mathbf{c}_0), \ldots, \text{Tr}_R^S(\mathbf{c}_{\ell-1})) : (\mathbf{c}_0, \ldots, \mathbf{c}_{\ell-1}) \in \mathcal{B} \}.
\]
It is clear that \( \text{Tr}_R^S(\mathcal{B}) = \text{Tr}_R^S(\mathcal{B})^\perp \). The extension code of an \( R \)-linear code \( \mathcal{C} \) to \( S \), is the \( S \)-linear code \( \text{Ext}_S(\mathcal{C}) \), formed by taking all combinations of codewords of \( \mathcal{C} \). The following theorem generalizes Delsarte’s celebrated result (see \cite{13} Ch.7, S.8, Theorem 11.1).

**Theorem 2.** (\cite{7} Theorem 3). Let \( \mathcal{B} \) be an \( S \)-linear code then \( \text{Tr}_R^S(\mathcal{B}^\perp) = \text{Res}_R(\mathcal{B})^\perp \), where \( \mathcal{B}^\perp \) is the dual to \( \mathcal{B} \) with respect to the usual scalar product, and \( \text{Res}_R(\mathcal{B})^\perp \) is the dual of \( \text{Res}_R(\mathcal{B}) \) in \( R^\ell \).

**Definition 3.2.** Let \( \mathcal{B} \) be an \( S \)-linear code. The \( \sigma \)-closure of \( \mathcal{B} \), is the smallest \( \sigma \)-invariant \( S \)-linear code \( \mathcal{\overline{B}} \), containing \( \mathcal{B} \).

**Proposition 5.** Let \( \mathcal{B} \) be an \( S \)-linear code. Then \( \mathcal{\overline{B}} = \sum_{i=0}^{m-1} \sigma^i(\mathcal{B}) \) and \( \text{Tr}_R^S(\mathcal{B}) = \text{Tr}_R^S(\mathcal{\overline{B}}) \).

**Proof.** We have \( \mathcal{B} \subseteq \mathcal{\overline{B}} \) and \( \sigma(\mathcal{B}) = \mathcal{\overline{B}} \), by Definition 3.2 of \( \mathcal{\overline{B}} \). So \( \sigma^i(\mathcal{B}) \subseteq \mathcal{\overline{B}} \), for all \( i \in \{0, 1, \ldots, m-1\} \). Hence \( \sum_{i=0}^{m-1} \sigma^i(\mathcal{B}) \subseteq \mathcal{\overline{B}} \). 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 \( \mathcal{\overline{B}} \) is the smallest \( S \)-linear code containing \( \mathcal{B} \), which is \( \sigma \)-invariant, it follows \( \mathcal{\overline{B}} \subseteq \sum_{i=0}^{m-1} \sigma^i(\mathcal{B}) \). Hence \( \mathcal{\overline{B}} = \sum_{i=0}^{m-1} \sigma^i(\mathcal{B}) \). Thanks to \cite{7} Proposition 1., \( \text{Tr}_R^S(\mathcal{\overline{B}}) = \text{Tr}_R^S(\mathcal{B}) \).

The following Theorem summarizes the obtained results in \cite{7}.

**Theorem 3.** 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.

**Proof.** Let \( \mathcal{B} \) be an \( S \)-linear code.
1. $\Leftrightarrow$ 2. : Thanks to [2] Theorem 2.
1. $\Leftrightarrow$ 3. : Since any $R$-basis of $Res_R(\mathcal{B})$ is also an $S$-basis of $Ext_S(Res_R(\mathcal{B}))$. Thanks to [2] Theorem 1, we deduce that $\mathcal{B} = Ext_S\left(Tr_{R}^{s}(\mathcal{B})\right)$ if and only if $\mathcal{B}$ and $Res_R(\mathcal{B})$ have the same type.

4. CYCLIC LINEAR CODES OVER FINITE CHAIN RINGS

Let $\ell$ be a positive integer such that $gcd(q, \ell) = 1$. Then the remainder $q \pmod{\ell}$ of $q$ by $\ell$, belongs to $\mathbb{Z}_{\ell}^{*}$, the positive integer $m$ denotes the multiplicative order of $q \pmod{\ell}$. Let $\Sigma_{\ell} := \{0, 1, \cdots, \ell-1\}$ be the underlying set of $\mathbb{Z}_{\ell}$.

4.1. CYCLOMATIC COSETS. Let $u$ be a positive integer. The set of multiples of $u$ in $A$ is $uA := \{uz \pmod{\ell} : z \in A\}$.

The $q$-closure of $A$ is $C_{q}(A) := \bigcup_{i \in \mathbb{N}} q^{i}A$.

**Definition 4.1.** Let $z \in \Sigma_{\ell}$. The $q$-cyclotomic coset modulo $\ell$, containing $z$, the Galois closure of $\{z\}$. We simply write $C_{q}(z) := C_{q}(\{z\})$.

It denotes by $Gal(q)$ the set of $q$-closure subsets of $\Sigma_{\ell}$. Obviously, the $q$-cyclotomic cosets modulo $\ell$, form a partition of $\Sigma_{\ell}$. Let $\Sigma_{q}(\ell)$ be a set of representatives of each $q$-cyclotomic cosets modulo $\ell$.

**Proposition 6.** [1] Proposition 5.2 We have $|\Sigma_{q}(\ell)| = \sum_{d | \ell} \phi(d)/ord_{d}(q)$, where $\phi(.)$ is the Euler totient function and $ord_{d}(q) := \min\{i \in \mathbb{N} : q^{i+1} \equiv 1 \pmod{\ell}\}$.

**Notation 1.** Let $z \in \Sigma_{\ell}$ and $A$ be a subset of $\Sigma_{\ell}$ and $u \in \mathbb{N}$, with $gcd(u,q) = 1$.

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

**Remark 1.** Let $A$ be a subset of $\Sigma_{\ell}$. Then $C_{q}(\overline{A}) = \overline{C_{q}(A)}$ and $-C_{q}(A) = C_{q}(-A)$. Moreover $(A^{\circ})^{\circ} = A$.

**Example 4.1.** We take $\ell = 20, q = 3$. The $q$-cyclotomic cosets modulo $\ell$, are: $C_{q}(\{0\}) = \{0\}, C_{q}(\{5\}) = \{5, 15\}, C_{q}(\{10\}) = \{10\}$, and

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

So $\Sigma_{q}(20) = \{0, 1, 2, 4, 5, 10, 11\}$. We remark that $C_{q}(\{-z\}) = C_{q}(\{z\})$, for every $z \in \{0, 2, 4, 5, 10\}$. We set $I := [0, 10]$. We have $A := C_{q}(I) = C_{q}(\{0, 1, 2, 4, 5, 10\})$, $A = C_{q}(\{2, 4, 5, 10, 11\})$, and $A^{\circ} := C_{q}(\{1\})$.

4.2. Likewise Reed-Solomon 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 $A := \{a_{1}, a_{2}, \cdots, a_{k}\}$ be a subset of $\Sigma_{\ell}$. One denotes by $P(S; A)$, the free $S$-module with $S$-basis $\{X^{a} : a \in A\}$. Since $m$ is the smallest positive integer with $q^{m} \equiv 1 \pmod{\ell}$, we can write $\eta := \xi^{-m / \ell}$ and the multiplicative order of $\eta$ is $\ell$. The evaluation

$$ev_{\eta} : \quad P(S; A) \rightarrow S^{\ell} \rightarrow (f(1), f(\eta), \cdots, f(\eta^{\ell - 1})),$$

is an $S$-modules monomorphism. We see that if $A := \{0, 1, \cdots, k - 1\}$, then for any $\ell^{th}$-primitive root of unity $\eta$ in $\Gamma(S)$, the $S$-linear code $ev_{\eta}(P(S; A))$ is a primitive Reed-Solomon code. For this reason, we define Likewise Reed-Solomon codes which are a family of codes defined over large finite chain rings as follows.

**Definition 4.2.** Let $A$ be a subset of $\Sigma_{\ell}$, and $S$ be a finite chain ring such that $|\Gamma(S)| \geq \ell$. Let $\eta \in \Gamma(S)$ and the multiplicative order of $\eta$ is $\ell$. The $S$-submodule $ev_{\eta}(P(S; A))$ is called likewise Reed-Solomon code over $S$, with defining pair $(\eta, A)$.
We remark that $L_\eta(S; A) := ev_\eta(P(S; A))$ is the free $S$-linear code with free $S$-basis $\{ev_\eta(X^a) : a \in A\}$, where $A$ is a subset of $\Sigma_\ell$. We remark that $L_\eta(S; \emptyset) = \{0\}$, $L_\eta(S; \{\emptyset\}) = 1$ and $L_\eta(S; \Sigma_\ell) = S^\ell$.

**Proposition 7.** Let $A, B$ be two subsets of $\Sigma_\ell$. Then

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

**Proof.** Consider the codeword $c_i = (1, \eta^a, \ldots, \eta^{a(\ell-1)})$. Then the shift of $c_i$ is $\eta^{-a}c_i$. Since $L_\eta(S; A)$ is $S$-linear, we have $\eta^{-a}c_i \in L_\eta(S; A)$. Hence $L_\eta(S; A)$ is cyclic. It is clear that $L_\eta(S; A \cup B) \supseteq L_\eta(S; A) + L_\eta(S; B)$. The set $\{ev_\eta(X^a) : a \in A \cup (B \setminus A)\}$ is a free $R$-basis of $L_\eta(S; A \cup B)$ and $L_\eta(S; A) + L_\eta(S; B)$. Hence, $L_\eta(S; A \cup B) = L_\eta(S; A) + L_\eta(S; B)$. We leave the last equality as an exercise.

**Proposition 8.** Let $A$ be a subset of $\Sigma_\ell$ and $u$ be a positive integer such that $\gcd(\ell, u) = 1$. Then

1. $L_\eta^u(S; A) = L_\eta(S; uA)$;
2. $L_\eta(S; A) = L_\eta(S; A^\ell)$;
3. $L_\eta(S; A)$ is the $\sigma$-closure of $L_\eta(S; A)$.

**Proof.** Assume that $\gcd(\ell, u) = 1$. Then $\eta$ and $\eta^u$ are $\ell$th-primitive roots of unity. Since $\{ev_\eta(X^a) : a \in uA\}$ is a free $R$-basis of $L_\eta(S; A)$, we have $L_\eta^u(S; A) = L_\eta(S; uA)$.

A free $S$-basis of $L_\eta(S; A^\ell)$ is $\{c_i : -a \in A\}$ where $c_i := (1, \eta^{-a}, \ldots, \eta^{-a(\ell-1)}) \in L_\eta(S; A^\ell)$. Then for all $b \in A$, $c_b := (1, \eta^b, \ldots, \eta^{b(\ell-1)}) \in L_\eta(S; A)$. We have $c_i c_b^{\text{tr}} = \sum_{j=0}^{\ell-1} \eta^{ij}$. 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 $c_b c_a^{\text{tr}} = 0$. So $L_\eta(S; A^\ell) \subseteq L_\eta(S; A^\ell)$. Comparison of cardinality yields $L_\eta(S; A^\ell) = L_\eta(S; A^\ell)$. Finally, $\sigma(L_\eta(S; A)) = L_\eta(S; A)$. So by Proposition 5 we have $L_\eta(S; A) = \bigcup_{i=0}^{m-1} L_\eta(S; q^iA) = L_\eta(S; A^\ell)$. Since $\text{ev}_q(A) = \bigcup_{i=0}^{m-1} q^iA$, we obtain $L_\eta(S; A) = L_\eta(S; \text{ev}_q(A))$. 

4.3. **Trace representation of free cyclic linear codes.** We introduce the map trace-evaluation $\text{Tr}_S^R \circ ev_\eta : P_\eta(S; A) \to R^\ell$, defined by:

$$\text{Tr}_S^R \circ ev_\eta(X^a) := \text{Tr}_R^S \left(1, \eta^a, \ldots, \eta^{a(\ell-1)}\right),$$

for all $a \in A$. In the sequel, we write: $C_\eta(R; A) := \text{Tr}_S^R \left(L_\eta(S; A)\right)$, and $C_\eta(R; A)$ is a free cyclic $R$-linear code of length $\ell$. The immediate properties of trace representation of free cyclic linear codes over finite chain ring are given in the following.

**Proposition 9.** Let $A, B$ be two empty subsets of $\Sigma_\ell$. Then

1. $C_\eta(R; A) = C_\eta(R; \text{ev}_q(A))$;
2. $\text{rank}_S(L_\eta(S; \text{ev}_q(A))) = |\text{ev}_q(A)|$ and $C_\eta(R; A) = C_\eta(R; A^\ell)$;
3. $C_\eta(S; A \cup B) = C_\eta(S; A) + C_\eta(S; B)$ and $C_\eta(S; A \cap B) = C_\eta(S; A) \cap C_\eta(S; B)$.

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

1. From Proposition 5, $C_\eta(R; A) = \text{Tr}(L_\eta(S; A)) = \text{Tr}(L_\eta(S; \text{ev}_q(A))) = C_\eta(R; \text{ev}_q(A))$.
2. Theorem 3 yields $C_\eta(R; A) = \text{Tr}(L_\eta(S; \text{ev}_q(A))) = \text{Res}_S(L_\eta(S; \text{ev}_q(A)))$. So $\text{rank}_R(C_\eta(R; A)) = \text{rank}_S(L_\eta(S; \text{ev}_q(A))) = |\text{ev}_q(A)|$.

From Proposition 8, $C_\eta(R; A^\ell) = C_\eta(R; A^\ell)$. 

The following theorem gives the number of cyclic codes and free cyclic codes over finite chain rings.
Lemma 3. Let $G$ be a finite chain ring of invariants $(q, s)$ and $S$ be the Galois extension of $G$ of degree $m$. Let $z \in \Sigma_s$. Set $S = R[\xi]$, $m_z := [c_0(z)]$, $\eta := \frac{\xi^{m_z} - 1}{\eta - z}$. Then the map

$$
\psi_z : R[\xi^{m_z}] \to C_0(R; \{z\}),
$$

$$
a \mapsto \text{Tr}_R^S(\text{ev}_\eta(aX^z)),
$$

is an $G$-module isomorphism. Further $R[\xi^{m_z}]$ is the Galois extension of $G$ of degree $m_z$ and $\psi_z \circ \tau_0 = \tau_1 \circ \psi_z$, where $\tau_1(a) = a_{2},$ for all $a \in R[q].$

Proof. It is clear that $a \in \text{Ker}(\psi_z)$ if and only if $a \in R[\xi^{m_z}] \cap R[\xi^{m_z}]$, where duality is with respect to trace form. As the trace bilinear form is nondegenerate, we have $S = R[\xi^{m_z}] \cap R[\xi^{m_z}]$ and Ker$(\psi_z) = \{0\}$. Hence $\psi_z$ is an $G$-module monomorphism. We remark that, $C_0(R, \{z\})$ is cyclic, if and only if $\psi_z \circ \tau_0 = \tau_1 \circ \psi_z$, for all $a \in R[q]$. Finally, we have $S = R[\xi]$, so $R[\xi^{m_z}]$ is the Galois extension of $G$ of degree $m_z$. Hence, $\psi_z$ is an $G$-module isomorphism.

Definition 4.3. A non-trivial cyclic $G$-linear code $C$ is said to be irreducible, if for all $G$-linear cyclic subcodes $C_1$ and $C_2$ of $C$, such that, $C = C_1 \oplus C_2$, implies $C_1 = \{0\}$ or $C_2 = \{0\}$.

Proposition 10. The irreducible cyclic $G$-linear codes are precisely $\theta^t C_0(R; \{z\})$, where $t \in \{0, 1, \cdots, s - 1\}$ and $z \in \Sigma_s(q)$.

Proof. By Lemma 3 the cyclic $G$-linear code $C_0(R; \{z\})$ and all the cyclic $G$-linear subcodes are irreducible. Let $C$ be an irreducible cyclic $G$-linear code. Then the $G$-linear code $\text{Quo}\theta_{s-1}(C) := \{c \in R^s : \theta^t c \in C\}$ is cyclic and free, and so $\text{Quo}\theta_{s-1}(C) = C_0(R; A)$ for some $A \subset \Sigma_s(q)$ and $A \neq \emptyset$. Assume that $|A| > 1$. Then $C_0(R; A) = C_0(R; A_1) \oplus C_0(R; A_2)$ where $A_1 \cap A_2 = \emptyset$, $A_1 \neq \emptyset$ and $A_2 \neq \emptyset$. We have $C_0(R; A_1) \neq \{0\}$ and $C_0(R; A_2) \neq \{0\}$. Therefore $C = (C_0(R; A_1)) \oplus (C_0(R; A_2))$. It is impossible, because $C$ be an irreducible. So $|A| = 1$. Now, $C \subseteq C_0(R; \{z\})$, it follows that $C = \theta^t C_0(R; \{z\})$, for some $t \in \{0, 1, \cdots, s - 1\}$.

We set $\Sigma_s(q)$ a set of representatives of each $q$-cyclotomic cosets modulo $\ell$. An $(q, s)$-cyclotomic partition modulo $\ell$, is the $(s + 1)$-tuple $(A_0, A_1, \cdots, A_s)$ with the property $A_t = C_q(\lambda^{-1}(\{t\}))$, where $\lambda : \Sigma_s(q) \to \{0, 1, \cdots, s\}$ is a map. Denoted by

$$
\mathcal{M}_t(q, s) := \{(A_0, A_1, \cdots, A_s) : (\exists \lambda \in \{0, 1, \cdots, s\}^{\Sigma_s(q)}) (A_t = \lambda^{-1}(\{t\}))\}
$$

the set of $(q, s)$-cyclotomic partitions modulo $\ell$, and $\text{Cy}(R, \ell)$ the set of cyclic $G$-linear codes of length $\ell$. We have $|\mathcal{M}_t(q, s)| = (s + 1)^{|\Sigma_s(q)|}$.

Example 4.2. We take $\ell = 20, q = 3$ and $s = 2$. Then $|\Sigma_s(q)| = 13$ and $|\mathcal{M}_t(q, s)| = 3^{7}$. An $(q, s)$-cyclotomic partition modulo $\ell$, is $A_t := (C_q(0, 1, 2), C_q(0, 11), C_q(4, 10))$.

Theorem 4. Any cyclic $G$-linear code $C$ there exists a unique $A := (A_0, A_1, \cdots, A_s) \in \mathcal{M}_t(q, s)$ such that $C = C_q(A)$ and $C_q(A) = \bigoplus_{t=0}^{s-1} C_q(R; A_t)$. Moreover, the type of $C_q(A)$ is

$$
(C_q(A_0), C_q(A_1), \cdots, C_q(A_{s-1})),
$$

for some $A_0, A_1, \cdots, A_s \in \mathcal{M}_t(q, s)$.

Proof. Let $C$ be an cyclic $G$-linear code of length $\ell$. From Proposition 9, we have $R[\xi^{m_z}]$ is equal to $C_q(R; \{z\})'s$ are free irreducible cyclic $G$-linear codes. Therefore $C = \bigoplus_{z \in \Sigma_s(q)} C_q(R; \{z\})$, where $C_q(R; \{z\})'$s are free irreducible cyclic $G$-linear codes.
\[C_0(R; \{z\}) \cap \mathcal{C}.\] From Proposition \[10\] \(\mathcal{C}_z = \theta \cdot \mathcal{C}_0(R; \{z\})\), where \(t_z \in \{0, 1, \ldots, s\}\). Hence

\[\mathcal{C} = \bigoplus_{t \in \Sigma(q)} \theta \cdot \mathcal{C}_0(R; \{z\}) \bigoplus_{t=0}^{s-1} \mathcal{C}_0(R; A_t),\]

where \(A_t = \{z \in \Sigma(q) : t_z = t\}\). Since \(\mathcal{N}_r(q, s) = (s + 1)^{\mathcal{N}_r(q, s)}\), by Theorem \[2\] the uniqueness of \(A := (A_0, A_1, \ldots, A_s) \in \mathcal{N}_r(q, s)\) such that \(\mathcal{C} = C_0(A)\) is guaranteed.

Moreover, for every \(t \in \{0, 1, \ldots, s - 1\}\), the cyclic \(R\)-linear code \(C_0(R; A_t)\) is free and \(\text{rank}_R(C_0(R; A_t)) = |\mathcal{C}_0(A_t)|\). Since the direct sum \(\bigoplus \theta \cdot \mathcal{C}_0(R; A_t)\) gives the type of \(C_0(A)\), the type of \(C_0(A)\) is \((k_0, k_1, \ldots, k_s)\), where \(k_i := |\mathcal{C}_0(A_i)|\), for every \(t \in \{0, 1, \ldots, s - 1\}\).

\[\text{Proposition 11.} \text{ Let } A := (A_0, A_1, \ldots, A_s) \in \mathcal{N}_r(q, s) \text{ and } t \in \{0, 1, \ldots, s - 1\}. \text{ Then } C_0(A) \vdash C_0(A^\circ), \text{ where } A^\circ := (-A_s, -A_{s-1}, \ldots, -A_1, -A_0).\]

\[\text{Proof.} \text{ Let } A := (A_0, A_1, \ldots, A_s) \in \mathcal{N}_r(q, s). \text{ We have } C_0(A) \vdash \bigcap_{t=0}^{s-1} \left( \theta \cdot A_t \right) \text{ and } \text{rank}_R(C_0(R; A_t)) = |\mathcal{C}_0(A_t)|, \text{ for every } t \in \{1, 2, \ldots, s\}. \text{ It follows that } C_0(A^\circ) \subseteq C_0(A) \vdash.\]

\[\text{From Propositions } 4 \text{ and Theorem } 4 \text{ C}_0(A^\circ) \text{ and } C_0(A) \vdash \text{ have the same type, we have } C_0(A) \vdash = C_0(A^\circ). \]
Theorem 5. Let $u, ℓ \in \mathbb{N}$ such that $\gcd(u, ℓ, q) = 1$. Let $A$ be a subset of $\{0, 1, \ldots, u ℓ - 1\}$ and $C_q(R; A)$ be a cyclic $R$-linear code of length $u ℓ$. Then $C_q(A)(\text{mod } u) = \{a\}$, if and only if $\mathcal{X} := \varphi^{-1}(C_q(R; A))$ is an $\gamma$-constacyclic $R$-linear code of length $ℓ$, where $\gamma = \frac{\zeta^{q m - 1}}{u \text{ mod } u}$. Moreover, $\mathcal{X} \perp = \varphi^{-1}(C_q(R; A^u))$, where $C_q(A)(\text{mod } u) = \{a\}$, and $A^u := \{a \in A^0 : a \equiv -a(\text{mod } u)\}$, is an $\gamma^{-1}$-constacyclic $R$-linear code of length $ℓ$.

Proof. Let $m$ be the positive integer such that $q^m \equiv 1(\text{mod } u ℓ)$ and $q^m \not\equiv 1(\text{mod } u ℓ)$. Let $S := R[\xi]$ be a Galois extension of $R$ of degree $m$. We set $u := \frac{q - 1}{u ℓ}$ and $η := ξ^w$. Let $Z := C_q(A)$, where $A$ is a subset of $\Sigma_q$. Then $C_q(R; Z) = \oplus_{z \in Z} C_q(R; \{z\})$. It is enough to show that $C_q(R; \{z\}) \subseteq \varphi(R^\ell)$, for all $z \in Z$. Let $z \in Z$, we set $m_z := |C_q(z)|$ and $ζ := η^{m_z}$. From Lemma 1, $C_q(R; \{z\}) = \psi_z C_q(R[ζ^{m_z}]) = Tr^R_S(\psi_q R[ζ^{m_z}])$. Thus for all $c := (c_0, \ldots, c_{u ℓ - 1}) \in C_q(R; \{z\})$, from Lemma 1, there exist a unique $a \in R[ζ^{m_z}]$ and such that $c = Tr^R_S(\psi_q(aX^ζ))$. Since $R[ζ^{m_z}]$ is the Galois extension of $R$ of degree $m_z$, there then exist a unique $(a_0, a_1, \ldots, a_{m_z - 1})$ such that $a := \sum_{h=0}^{m_z - 1} a_h \xi^{h m_z} \in R[ζ^{m_z}]$.

Example 5.1. Let $R$ be a finite chain ring of invariants $(q, s)$ where $q = 3$. Take $ℓ = 28, u = 2$. We set $A_1 := C_q(\{1, 7\}), A_2 := C_q(\{1, \ldots, 11\})$, and $A_3 := C_q(\{1, 5, 7, 11\})$. We have $C_q(A_i)(\text{mod } 2) = \{1\}$. We can set $\mathcal{X}_i := \varphi^{-1}(C_q(R; A_i))$, where $i \in \{1, 2, 3\}$. Since $A_1^2 = A_2$ and $A_2^2 = A_2$, we have $\mathcal{X}_3 = \mathcal{X}_1^\perp$ and $\mathcal{X}_2$ is self-dual.

The Hamming weight of an $R$-linear code $\mathcal{C}$, of length $ℓ$, is defined as: $\text{wt}(\mathcal{C}) := \min\{\text{wt}(c) : c \in \mathcal{C} \setminus \{0\}\}$, where $\text{wt}(c) := |\{j \in \Sigma_q : c_j \neq 0\}|$.

Corollary 2. Let $u, ℓ \in \mathbb{N}$ such that $\gcd(u, ℓ, q) = 1$. Set $A := (A_0, A_1, \ldots, A_s) \in \mathbb{R}_{u ℓ}(q, s)$ and $C_R(A)$ be a cyclic $R$-linear code of length $u ℓ$ such that $\bigcup_{t=0}^{s-1} A_t(\text{mod } u) = \{a\}$. Set $\mathcal{X} := \varphi^{-1}(C_R(A))$. Then

(1) $\mathcal{X}$ is an $\gamma$-constacyclic $R$-linear code of length $ℓ$, where $\gamma = \frac{\zeta^{q m - 1}}{u \text{ mod } u}$,
Example 5.2. Let \( R \) be a finite chain ring of invariants \( (q, s) \) where \( J(R) = R\emptyset \), \( q = 3 \) and \( s = 2 \). We take \( \ell = 10 \), \( u = 2 \). We set \( \mathcal{A} := \{A_0, A_1, A_2\} \), where \( A_0 := \mathbb{C}_q\{\{1\}\} \), \( A_1 := \mathbb{C}_q\{\{5\}\} \), and \( A_2 := \mathbb{C}_q\{\{0, 2, 4, 10, 11\}\} \). We have \( \mathbb{C}_q\{A_0\}(\mod 2) = \mathbb{C}_q\{A_1\}(\mod 2) = \{\emptyset\} \). So the contraction of the cyclic \( R \)-linear code \( \mathbb{C}_R(A) \) of length 20, is the self-dual negacyclic \( R \)-linear code \( \mathcal{C} := \mathfrak{v}^{-1}\left(\mathbb{C}_q(R; A_0)\oplus \theta \mathfrak{v}^{-1}\left(\mathbb{C}_q(R; A_1)\right)\right) \), of length 10.

6. Conclusion

We have seen that in the case \( \gcd(\ell, |R|) = 1 \), and \( \gamma \in \Gamma(R)^* \), the class of \( \gamma \)-constacyclic \( R \)-linear codes of length \( \ell \), is the same as the class of contractions of cyclic \( R \)-linear codes \( \mathbb{C}_R(A_0, A_1, \cdots, A_s) \) of length \( u \ell \), where \( u \) is the multiplicative order of \( \gamma \), and each cyclic \( R \)-linear code \( \mathbb{C}_R(A_0, A_1, \cdots, A_s) \) of this class, satisfies: \( \bigcup_{t=0}^{s-1} A_t (\mod u) \) is a singleton.

References

[1] Batoul A., Guenda K., Guelliver T.A., On the self-dual cyclic codes over finite chain rings, Des. Codes Cryptogr. 70(1) 347-358 (2014)
[2] Bierbrauer J., The Theory of Cyclic Codes and a Generalization to Additive Codes, Des. Codes Cryptogr. 25(2): 189–206 (2002).
[3] Yonglin Cao, On constacyclic codes over finite chain rings, Finite Fields and Their Applications 24 (2013) 124–135.
[4] H. Dinh, S.R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory 50 (8) 1728–1744 (2004).
[5] Kai X., Zhu S., Tang Y., Some constacyclic self-dual codes over the integers modulo \( 2^m \), Finite Fields Appl. 18 (2012) 258–270.
[6] McDonald B. R., Finite Rings with Identity, Marcel Dekker, New York (1974).
[7] Martinez-Moro E., Nicolas A.P., Rua F., On trace codes and Galois invariance over finite commutative chain rings, Finite Fields Appl. Vol. 22, pp. 114–121 (2013).
[8] Alexandr A. Nechaev, Finite rings with applications, in: Handbook of Algebra, vol. 5, Elsevier/North-Holland, Amsterdam, 2008, pp. 213–320.
[9] Norton G.H., Slălăgean A., On the Structure of Linear and Cyclic Codes over a Finite Chain Ring, AAECC Vol. 10, pp. 489–506, (2000).
[10] H. Tapia-Recillas, G. Vega, Some constacyclic codes over \( \mathbb{Z}_p^m \) and binary quasi-cyclic codes, Discrete Appl. Math. 128 (2003) 305–316.
[11] Wolfmann J., Negacyclic and cyclic codes over \( \mathbb{Z}_4 \), IEEE Trans. Inform. Theory 45 (7) (1999) 2527–2532.
[12] Zhu S., Kai X., A class of constacyclic codes over \( \mathbb{Z}_{2^m} \), Finite Fields Appl. 16 (2010) 243–254.
[13] McWilliams F. J. and Sloane N. J. A., The Theory of Error-Correcting Codes, North-Holland Mathematical Library, Vol 16, North-Holland Publishing Co., Amsterdam, (1977).

Department of Mathematics, Faculty of Sciences, University of Yaoundé I, Cameroon
E-mail address: alexfotue@gmail.com

Department of Mathematics, Higher Teachers Training College of Yaoundé, University of Yaoundé I, Cameroon
E-mail address: cmouaha@yahoo.fr