Algebra and Discrete Mathematics
Volume **27** (2019). Number 2, pp. 252–268

RESEARCH ARTICLE

On the lattice of cyclic codes over finite chain rings

Alexandre Fotue-Tabue and Christophe Mouaha

Communicated by V. A. Artamonov

Abstract. In this paper, R is a finite chain ring of invariants (q, s), and ℓ is a positive integer fulfilling $\gcd(\ell, q) = 1$. In the language of q-cyclotomic cosets modulo ℓ, the cyclic codes over R of length ℓ are uniquely decomposed into a direct sum of trace-representable cyclic codes over R and the lattice of cyclic codes over R of length ℓ is investigated.

Introduction

Research on linear codes over chain rings can be found in [8, 13] and cyclic 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 codes have been studied for decades and a lot of progress has been made (see [15]).

Throughout this paper, R is a finite chain ring of invariants (q, s), and ℓ is a positive integer such that $gcd(q, \ell) = 1$. An R-linear code of length ℓ is an R-submodule of R^ℓ. An R-linear code C of length ℓ is cyclic if the shift $(c_{\ell-1}, c_0, \dots, c_{\ell-2})$ of each codeword $(c_0, c_1, \dots, c_{\ell-1})$ in C, also belongs to C. Unless otherwise specified, all cyclic codes are assumed to

2010 MSC: 13B05, 94B05, 94B15, 03G10, 16P10.

Key words and phrases: finite chain rings, cyclotomic cosets, linear code, cyclic code, trace map.

be linear. As usual, any cyclic code C over R of length ℓ is identified to an ideal of $R[X]/\langle X^\ell - 1\rangle$, via the R-module isomorphism

$$\begin{aligned}\Psi : R^\ell &\to R[X]/\langle X^\ell - 1\rangle \\ (c_0, \dots, c_{\ell-1}) &\mapsto \sum_{j=0}^{\ell-1} c_j X^j + \langle X^\ell - 1\rangle\end{aligned} \tag{1}$$

where $\langle X^\ell - 1\rangle$ is the ideal of $R[X]$ generated by $X^\ell - 1$. The ideal $\Psi(C)$ is called the *polynomial representation* of C, and this polynomial representation was used in [3, 5, 10, 13, 14] for studying the algebraic structure of cyclic codes over finite chain rings. Three other general approaches to the design and analysis of cyclic codes are based on generator matrices, generator polynomials and idempotents. These approaches have their advantages and disadvantages in dealing with cyclic codes. The objectives of this paper are to introduce the cyclotomic approach to the study of cyclic codes.

The paper is organized as follows. In Section 1, we collect the basic results needed on finite chain rings as well as the characterization of their Galois extension. Section 2 discusses the notions of the type of any linear code over a finite chain ring and studies Galois-invariant linear codes. In Section 3, we explore the lattice of cyclotomic cosets modulo ℓ in order to obtain new properties of them. In Section 4, we show that any cyclic code can be uniquely decomposed as a direct sum of trace-representable cyclic codes.

1. Background on finite chain rings

In the rest of this paper, R is a finite local ring with maximal ideal $\mathrm{J}(R)$ and $R^\times$ denotes the group of units of R.

Definition 1. A finite local ring R is a chain ring of invariants (q, s), if R is a principal ideal ring such that q is the cardinality of the residue field of R, and s is the nilpotency index of $\mathrm{J}(R)$.

In the rest of this paper, R is a finite chain ring of invariants (q, s), the residue field of R is $\mathbb{F}_q$ and θ is a generator of $\mathrm{J}(R)$. The ring epimorphism

$$\begin{aligned}\pi : R &\to \mathbb{F}_q, \\ c &\mapsto c + \theta R,\end{aligned}$$

naturally extends to $R[X]$, of the following way: π acts on all the coefficients of any polynomial over R. Obviously, the cardinality of $R^\times$ is $q^{s-1}(q-1)$. It follows that $R^\times \simeq \Gamma(R)\backslash\{0_R\}\times(1_R+\mathrm{J}(R))$ with $\Gamma(R) = \{a \in R : a^q = a\}$ and $\Gamma(R) \setminus \{0_R\}$ is a cyclic subgroup of $R^\times$ of order $q-1$. The set $\Gamma(R)$ 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 $\mathrm{rank}_R(S)$, the rank of R-module S. Let f be a monic polynomial over $R[X]$ of degree m, and $\langle f \rangle$ is an ideal of $R[X]$ generated by f. We say that f is basic irreducible (resp. basic primitive) if $\pi(f)$ is irreducible over $\mathbb{F}_q$ (resp. primitive).

Definition 2. The ring S is the *Galois extension* of degree m of R if $S \simeq R[\alpha]$, (as R-algebras) where α is a root of a monic basic primitive polynomial over R of degree m.

Remark 1. Let S be the Galois extension of degree m of R. Let ξ 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 $\mathrm{Aut}_R(S)$, the group of all ring automorphisms of S which fix the elements of R.

Proposition 1 ([4], Chap. III; Proposition 2.1(1))**.** *The ring S is the Galois extension of degree m of R if and only if*

$$R = \{a \in S\colon \sigma(a) = a \textit{ for all } \sigma \in \mathrm{Aut}_R(S)\}$$

and $\mathrm{J}(S) = \theta S$.

For instance, for nonnegative integers p, n, s and p prime, the Galois extension of $\mathbb{Z}_{p^s}$ of degree n, is the Galois ring $\mathrm{GR}(p^s, n) \simeq \mathbb{Z}_{p^s}[X]/\langle f \rangle$, where $\langle f \rangle$ is the ideal generated by a monic basic irreducible polynomial f over $\mathbb{Z}_{p^s}$ of degree n.

Proposition 2 ([12], Theorem XV.10)**.** *Let S be the Galois extension of degree m of R. Let ξ be a generator of $\Gamma(S) \setminus \{0_S\}$. Then*

1) *S is a free R-module and $\{1, \xi, \ldots, \xi^{m-1}\}$ is a free R-basis of S;*
2) *$\mathrm{Aut}_R(S)$ is a cyclic group of order m, and a generator of $\mathrm{Aut}_R(S)$ is given by $\sigma : \xi \mapsto \xi^q$.*

Definition 3. Let S be the Galois extension of degree m of R. Let σ be a generator of $\mathrm{Aut}_R(S)$. The map $\mathrm{Tr}_R^S := \sum_{i=0}^{m-1} \sigma^i$, is called the *trace map* of $S|R$.

Proposition 3 ([4], Chap. III; Corollary 2.2). *Let $S|R$ be the Galois extension of finite chain rings. Then the trace map $\mathrm{Tr}_R^S : S \to R$ is an epimorphism of R-modules.*

Proposition 4. *Let S be the Galois extension of degree m of R. Then for all positive integer z, for all generator ξ of $\Gamma(S) \setminus \{0_R\}$, the ring $R[\xi^{zq}]$ is the Galois extension of R of degree m_z, and*

$$m_z := \min\{i \in \mathbb{N} \setminus \{0\} \colon zq^i \equiv 1 \mod (q^m - 1)\}.$$

Proof. We set $f := (X - \xi^{zq})(X - \xi^{zq^2}) \cdots (X - \xi^{zq^{m_z}})$. Since S is the Galois extension de R, we deduce by Proposition 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 $R[\xi^{zq}]$ is the Galois extension of R of degree m_z, because by Definition 2, ξ^{zq} is a root of a basic irreducible polynomial over R of degree of m_z. □

2. Linear codes over finite chain rings

The ring epimorphism $\pi : R \to \mathbb{F}_q$ naturally extends to R^ℓ of the following way: $\pi(\underline{c}) := (\pi(c_0), \pi(c_1), \ldots, \pi(c_{\ell-1}))$, for all $\underline{c} := (c_0, c_1, \ldots, c_{\ell-1})$ in R^ℓ. Recall that an R-linear code of length ℓ is an R-submodule of the free R-moduleR^ℓ. We say that an R-linear code is *free* if it is free as R-module.

2.1. Type and minimum Hamming weight of a linear code

A $k \times \ell$-matrix G over R, is called a *generator matrix* for C if the rows of G span 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

$$\mathrm{G} = \begin{pmatrix} I_{k_0} & G_{0,1} & G_{0,2} & \ldots & G_{0,s-1} & G_{0,s} \\ 0 & \theta I_{k_1} & \theta G_{1,2} & \ldots & \theta G_{1,s-1} & \theta G_{1,s} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \theta^{s-1} I_{k_{s-1}} & \theta^{s-1} G_{s-1,s} \end{pmatrix} \mathrm{U}, \qquad (2)$$

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

Proposition 5 ([13], Proposition 3.2, Theorem 3.5). *Each R-linear code C admits a generator matrix* G *standard form. Moreover, the type is the same for any generator matrix in standard form for C.*

Let C be an R-linear code and G be a generator matrix in standard form. The rows of G form an R-basis for C, so-called *standard* R-basis for C. So the type and the rank are the invariants of C, and henceforth we have the following definition.

Definition 4. Let C be an R-linear code.

1) The *type* of C is the type of a generator matrix of C in standard form.
2) The *rank* of C, denoted $\operatorname{rank}_R(C)$, is the rank of a generator matrix of C in standard form.

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

Proposition 6 ([8], Theorem 3.1)**.** *Let C and C' be R-linear codes of length ℓ. Then $(C + C')^\perp = C^\perp \cap C'^\perp$, $(C \cap C')^\perp = C^\perp + C'^\perp$, and $(C^\perp)^\perp = C$.*

Proposition 7 ([13], Theorem 3.10)**.** *Let C be an R-linear code of length ℓ, 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) *$|C| = q^{\sum_{t=0}^{s-1}(s-t)k_t}$, where $|C|$ denotes the number of elements of C.*

Definition 5. Let C be an R-linear code of rank k.

1) The R-linear subcode $\operatorname{Soc}(C) := \{\underline{c} \in C \colon \theta\underline{c} = \underline{0}\}$ of C is called the *socle* of C.
2) The *residue code* of C is the $\mathbb{F}_q$-linear code $\pi(C) := \{\pi(\underline{c}) \colon \underline{c} \in C\}$.

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

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

Let $x \in R^\ell$ and C be an R-linear code of length ℓ. The Hamming weight of x is the number of non-zero coordinates in x. It is denoted by $\mathrm{wt_H}(x)$.

The minimum Hamming weight of C is $\mathrm{wt}_{\mathrm{H}}(C) := \min\{\mathrm{wt}_{\mathrm{H}}(x)\colon x \in C \setminus \{0\}\}$.

Proposition 8 ([9], Theorem 3.3). *Let C be a free R-linear code of length ℓ and D be an R-linear subcode of D such that $\mathrm{rank}_R(C) = \mathrm{rank}_R(D)$. Then*

$$\mathrm{wt}_{\mathrm{H}}(C) = \mathrm{wt}_{\mathrm{H}}(D) = \mathrm{wt}_{\mathrm{H}}(\mathrm{Soc}(D))$$

and $\mathrm{wt}_{\mathrm{H}}(C) = \mathrm{wt}_{\mathrm{H}}(\pi(C))$.

2.2. Galois closure of a linear code over a finite chain ring

Let S be a Galois extension of R and σ be a generator of $\mathrm{Aut}_R(S)$. Let B be an S-linear code of length ℓ Then $\sigma(B) := \{(\sigma(c_0), \dots, \sigma(c_{\ell-1}))\colon (c_0, \dots, c_{\ell-1}) \in B\}$ is also an S-linear code of length ℓ. We say that the S-linear code B is called *Galois invariant* if $\sigma(B) = B$. The *restriction* of B to R, is an R-linear code $\mathrm{Res}_R(B) := B \cap R^\ell$, and the *trace code* of B to R, is the R-linear code

$$\mathrm{Tr}_R^S(B) := \{(\mathrm{Tr}_R^S(c_0), \dots, \mathrm{Tr}_R^S(c_{\ell-1}))\colon (c_0, \dots, c_{\ell-1}) \in B\}.$$

It is clear that $\mathrm{Tr}_R^S(\sigma(B)) = \mathrm{Tr}_R^S(B)$. The *extension code* of an R-linear code C to S, is the S-linear code $\mathrm{Ext}_S(C)$, formed by taking all combinations of codewords of C. The following theorem generalizes Delsarte's celebrated result (see [15, Chap. 7, § 8. Theorem 11]).

Theorem 1 ([11], Theorem 3). *Let B be an S-linear code then $\mathrm{Tr}_R^S(B^\perp) = \mathrm{Res}_R(B)^\perp$, where $B^\perp$ is the dual to B with respect to the usual scalar product, and $\mathrm{Res}_R(B)^\perp$ is the dual of $\mathrm{Res}_R(B)$ in R^ℓ.*

Definition 6. Let B be an S-linear code. The *Galois closure* of B is the smallest Galois invariant S-linear code $\mathrm{Cl}(B)$ containing B.

Proposition 9. *Let B be an S-linear code. Then $\mathrm{Cl}(B) = \sum_{i=0}^{m-1} \sigma^i(B)$ and $\mathrm{Tr}_R^S(B) = \mathrm{Tr}_R^S(\mathrm{Cl}(B))$.*

Proof. We have $B \subseteq \mathrm{Cl}(B)$ and $\sigma(\mathrm{Cl}(B)) = \mathrm{Cl}(B)$, by Definition 6 of $\mathrm{Cl}(B)$. So $\sigma^i(B) \subseteq \mathrm{Cl}(B)$, for all $i \in \{0, 1, \dots, m-1\}$. Hence $\sum_{i=0}^{m-1} \sigma^i(B) \subseteq \mathrm{Cl}(B)$. Since $\sigma(\sum_{i=0}^{m-1} \sigma^i(B)) = \sum_{i=0}^{m-1} \sigma^i(B)$ and $B \subseteq \sum_{i=0}^{m-1} \sigma^i(B)$, as $\mathrm{Cl}(B)$ is the smallest S-linear code containing B, which is Galois invariant, it follows $\mathrm{Cl}(B) \subseteq \sum_{i=0}^{m-1} \sigma^i(B)$. Hence $\mathrm{Cl}(B) = \sum_{i=0}^{m-1} \sigma^i(B)$. Thanks to [11, Proposition 1.], $\mathrm{Tr}_R^S(\mathrm{Cl}(B)) = \mathrm{Tr}_R^S(B)$. □

The following theorem summarizes the obtained results in [11].

Theorem 2. *An S-linear code B is Galois invariant if and only if* $\mathrm{Tr}_R^S(B) = \mathrm{Res}_R(B)$.

3. Cyclotomic partitions

Consider $\mathbb{Z}_\ell$, the ring of integers modulo ℓ and $\Sigma_\ell := \{0, 1, \dots, \ell - 1\}$ the underlying set of $\mathbb{Z}_\ell$. Let A be a subset of Σ_ℓ. The set of *multiples* of u in A is $u\mathrm{A} := \{uz \,(\mathrm{mod}\ \ell) \colon z \in \mathrm{A}\}$. The *$q$-closure* of A modulo ℓ is $\mathsf{C}_q(\mathrm{A}) := \underset{i\in\mathbb{N}}{\cup} q^i\mathrm{A}$. We see that $\mathsf{C}_q(\varnothing) = \varnothing$.

Definition 7. Let $z \in \Sigma_\ell$. The *q-cyclotomic coset modulo ℓ,* containing z, denoted $\mathsf{C}_q(z)$, is the q-closure of $\{z\}$.

Denote by $\Re_\ell(q)$ the set of q-closure subsets of Σ_ℓ, and by 2^{Σ_ℓ} the set of subsets of Σ_ℓ. Obviously, the q-cyclotomic cosets modulo ℓ, form a partition of Σ_ℓ. Let $\Sigma_\ell(q)$ be a set of representatives of each q-cyclotomic cosets modulo ℓ.

Proposition 10 ([1], Proposition 5.2)**.** *We have*

$$|\Sigma_\ell(q)| = \sum_{d|\ell} \frac{\phi(d)}{\mathrm{ord}_d(q)},$$

where

$$\phi(d) := |\{j \in \Sigma_d \colon \gcd(j, d) = 1\}|$$

and

$$\mathrm{ord}_d(q) := \min\{i \in \mathbb{N} \setminus \{0\} \colon q^i \equiv 1 \,(\mathrm{mod}\ d)\}.$$

We introduce the binary and unary operations on Σ_ℓ. These operations are necessary in the following section, for the construction of cyclic codes.

Definition 8. Let $z \in \Sigma_\ell$ and A, B be two subsets of Σ_ℓ.

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

Let L be a nonempty set. We recall that the quintuple $\langle \mathrm{L}; \vee, \wedge; 0, 1\rangle$ is a *bounded lattice* if the operations $\vee$ and $\wedge$ are commutative, associative, idempotent and satisfy the following identities $x = x \vee (x \wedge x)$, $x = x \wedge (x \vee x)$, $x \wedge 0 = 0$ and $x \vee 1 = 1$.

Moreover, a lattice $\langle \mathrm{L}; \vee, \wedge\rangle$ is *distributive* if for all $x, y, z \in \mathrm{L}$, $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$, and a lattice $\langle \mathrm{L}; \vee, \wedge\rangle$ is *modular* if for all $x, y, z \in \mathrm{L}$,

$x \wedge (y \vee (x \vee z)) = (x \wedge z) \vee (y \wedge z)$. A more general and detailed treatment of the topic can be found in textbooks on Lattices such as [7].

Example 1. The lattice $\langle 2^{\mathrm{E}}; \cup, \cap; \varnothing, \mathrm{E}\rangle$ is distributive and bounded, where 2^{E} is the power set of a set E. The lattice $\langle L_\ell(R); +, \cap; \{\underline{0}\}, R^\ell\rangle$ is modular and bounded, where $L_\ell(R)$ is the set of all R-linear codes of length ℓ.

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

Proposition 11. *The lattice* $\langle\, \Re_\ell(q); \cup, \cap; \varnothing, \Sigma_\ell(q)\,\rangle$ *is bounded and distributive. Moreover, the map*

$$\begin{aligned} \mathsf{C}_q : 2^{\Sigma_\ell} &\to \Re_\ell(q) \\ \mathrm{A} &\mapsto \bigcup_{i\in\mathbb{N}} q^i \mathrm{A} \end{aligned}$$

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

Definition 9. The $(s+1)$-tuple $(\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s)$ is an (q,s)-*partition cyclotomic* modulo ℓ, if there exists a unique map $\lambda : \Sigma_\ell(q) \to \{0, 1, \ldots, s\}$, such that $\mathrm{A}_t = \mathsf{C}_q(\lambda^{-1}(\{t\}))$, for all $0 \leqslant t \leqslant s$.

Denote by $\Re_\ell(q,s)$ the set of (q,s)-partition cyclotomic modulo ℓ, and notes that

$$\Re_\ell(q,s) := \{(\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s) \colon (\exists \lambda \in \{0,1,\ldots,s\}^{\Sigma_\ell(q)})(\mathrm{A}_t = \lambda^{-1}(\{t\}))\}.$$

By Definition 9, one check that $|\Re_\ell(q,s)| = (s+1)^{|\Sigma_\ell(q)|}$.

Example 2. The 3-cyclotomic cosets modulo 20 are $\mathsf{C}_3(\{0\}) = \{0\}$,

$$\mathsf{C}_3(\{5\}) = \{5; 15\}, \quad \mathsf{C}_3(\{10\}) = \{10\}, \quad \mathsf{C}_3(\{1\}) = \{1; 3; 9; 7\},$$
$$\mathsf{C}_3(\{2\}) = \{2; 6; 18; 14\}, \quad \mathsf{C}_3(\{4\}) = \{4; 12; 16; 8\},$$
$$\mathsf{C}_3(\{11\}) = \{11; 13; 19; 17\}.$$

So $\Sigma_{20}(3) = \{0; 1; 2; 4; 5; 10; 11\}$ and $\mathsf{C}_3(\{-z\}) = \mathsf{C}_3(\{z\})$, for all $z \in \{0; 2; 4; 5; 10\}$. We have $\mathrm{A} := \mathsf{C}_3(\{0; 1; 2; \ldots; 10\}) = \mathsf{C}_3(\{0; 1; 2; 4; 5; 10\})$, $-\mathrm{A} = \mathsf{C}_3(\{2; 4; 5; 10; 11\})$.

4. Trace-representable cyclic codes

Let S be a Galois extension of R such that $|\Gamma(S)| > \ell$ and ξ be a generator of $\Gamma(S) \setminus \{0\}$. Let $\eta := \xi^{\frac{q^m-1}{\ell}}$ be an element in $\Gamma(S)$ such that ℓ is the multiplicative order of η. A cyclic cyclic code C over R is *trace-representable* if there is a free R-linear code D such that $C = \theta^t D$. In this section, we give the trace representation of free cyclic codes over R of length ℓ.

4.1. Cyclic polynomial codes over finite chain rings

Let $\mathrm{A} := \{i_1, i_2, \dots, i_k\}$ be a subset of Σ_ℓ and

$$\mathbf{P}(S;\mathrm{A}) := \{a_1x^{i_1} + a_2x^{i_2} + \cdots + a_kx^{i_k} : (a_1, a_2 \dots, a_k) \in S^k\}$$

be an S-submodule of the free S-module$S[X]$. The evaluation

$$\begin{aligned}\mathbf{ev}_\eta : \mathbf{P}(S;\mathrm{A}) &\to S^\ell \\ f &\mapsto (f(1), f(\eta), \dots, f(\eta^{\ell-1})),\end{aligned}$$

is an S-modules monomorphism.

We see that if $\mathrm{A} := \{0, 1, \dots, k-1\}$ then for any ℓ^{th}-primitive root of unity η in $\Gamma(S)$, the S-linear code $\mathbf{ev}_\eta(\mathbf{P}(S;\mathrm{A}))$ is a cyclic Reed-Solomon code. For this reason, we define cyclic polynomial codes which is a family of codes over large finite chain rings as follows.

Definition 10. Let A be a subset of Σ_ℓ. The *cyclic polynomial code* over S with defining set A, denoted $\mathbf{L}_\eta(S;\mathrm{A})$, is the free S-module $\mathbf{ev}_\eta(\mathbf{P}(S;\mathrm{A}))$.

For every subset set A of Σ_ℓ, and for all positive integer u such that $\gcd(u, \ell) = 1$, we have $\mathbf{L}_{\eta^u}(S;\mathrm{A}) = \mathbf{L}_\eta(S;u\mathrm{A})$ and

$$W_{\mathrm{A}} := \begin{pmatrix} 1 & \eta^{i_1} & \dots & \eta^{(\ell-1)i_1} \\ \vdots & \vdots & & \vdots \\ 1 & \eta^{i_k} & \dots & \eta^{(\ell-1)i_k} \end{pmatrix} \tag{3}$$

is a generator matrix for $\mathbf{L}_\eta(S;\mathrm{A})$. Note that $\mathbf{L}_\eta(S;\varnothing) = \{\underline{0}\}$, $\mathbf{L}_\eta(S;\Sigma_\ell) = S^\ell$, and $\mathbf{L}_\eta(S;\{0\}) = S \cdot \mathbf{1}$, where $\mathbf{1} := (1, 1, \dots, 1)$.

Proposition 12. *Let* A *be a subset of* Σ_ℓ. *Then* $\mathbf{L}_\eta(S;\mathrm{A})$ *is cyclic.*

Proof. Consider the codeword $c_a = (1, \eta^a, \dots, \eta^{a(\ell-1)})$. Then the shift of c_a is $\eta^{-a}c_a$. Since $\mathbf{L}_\eta(S;\mathrm{A})$ is S-linear, we have $\eta^{-a}c_a \in \mathbf{L}_\eta(S;\mathrm{A})$. Hence $\mathbf{L}_\eta(S;\mathrm{A})$ is cyclic. □

Proposition 13. *Let* A, B *be two subsets of* Σ_ℓ. *The following assertions are satisfied:*

1) $\mathbf{L}_\eta(S; \mathrm{A})^\perp = \mathbf{L}_\eta(S; \mathrm{A}^\diamond)$;
2) $\mathbf{L}_\eta(S; \mathrm{A} \cup \mathrm{B}) = \mathbf{L}_\eta(S; \mathrm{A}) + \mathbf{L}_\eta(S; \mathrm{B})$ *and* $\mathbf{L}_\eta(S; \mathrm{A} \cap \mathrm{B}) = \mathbf{L}_\eta(S; \mathrm{A}) \cap \mathbf{L}_\eta(S; \mathrm{B})$.

Proof. Let A, B be subsets of Σ_ℓ.

1) An S-basis of $\mathbf{L}_\eta(S; \mathrm{A}^\diamond)$ is $\{c_a\colon -a \in \overline{\mathrm{A}}\}$ where $c_a := (1, \eta^{-a}, \ldots, \eta^{-a(\ell-1)}) \in \mathbf{L}_\eta(S; \mathrm{A}^\diamond)$. Then for all $b \in \mathrm{A}$, $c_b := (1, \eta^b, \ldots, \eta^{b(\ell-1)}) \in \mathbf{L}_\eta(S; \mathrm{A})$, we have $c_b c_a^{\mathrm{T}} = \sum_{j=0}^{\ell-1} \eta^{(b-a)j}$, 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 $i \not\equiv 0 (\mathrm{mod}\ \ell)$. Since $0 < b - a < \ell$, we have $c_b c_a^{\mathrm{T}} = 0$. So $\mathbf{L}_\eta(S; \mathrm{A}^\diamond) \subseteq \mathbf{L}_\eta(S; \mathrm{A})^\perp$. Comparison of cardinality yields $\mathbf{L}_\eta(S; \mathrm{A})^\perp = \mathbf{L}_\eta(S; \mathrm{A}^\diamond)$.

2) We have $\mathbf{L}_\eta(S; \mathrm{A}) \subseteq \mathbf{L}_\eta(S; \mathrm{A} \cup \mathrm{B})$, $\mathbf{L}_\eta(S; \mathrm{B}) \subseteq \mathbf{L}_\eta(S; \mathrm{A} \cup \mathrm{B})$. Therefore

$$\mathbf{L}_\eta(S; \mathrm{A}) + \mathbf{L}_\eta(S; \mathrm{B}) \subseteq \mathbf{L}_\eta(S; \mathrm{A} \cup \mathrm{B})$$

and

$$\mathbf{L}_\eta(S; \mathrm{A}) \cap \mathbf{L}_\eta(S; \mathrm{B}) \subseteq \mathbf{L}_\eta(S; \mathrm{A} \cup \mathrm{B}).$$

Since an S-basis of $\mathbf{L}_\eta(S; \mathrm{A}) + \mathbf{L}_\eta(S; \mathrm{B})$ is $\{c_a\colon a \in \mathrm{A} \cup (\mathrm{B} \setminus \mathrm{A})\}$ and an S-basis of $\mathbf{L}_\eta(S; \mathrm{A}) \cap \mathbf{L}_\eta(S; \mathrm{B})$ is $\{c_a\colon a \in \mathrm{A} \cap \mathrm{B}\}$. We have the equalities. □

We set $\mathbf{L}_\ell(S)$ to be the set of all cyclic polynomial codes of length ℓ over S. Then the quintuple $\langle\, \mathbf{L}_\ell(S); +,\ \cap;\ \{\underline{\mathbf{0}}\},\ S^\ell \rangle$ is a lattice and the map

$$\begin{aligned} \mathbf{L}_\eta(S; -) : 2^{\Sigma_\ell} &\to \mathbf{L}_\ell(S), \\ \mathrm{A} &\mapsto \mathbf{L}_\eta(S; \mathrm{A}), \end{aligned}$$

is a lattice isomorphism. The following result extends [2, Theorem 5] to finite chain rings.

Definition 11. A subset I of Σ_ℓ is an interval of length δ if there exists $(a, u) \in \Sigma_\ell \times \Sigma_\ell$ such that $\gcd(u, \ell) = 1$ and

$$\mathrm{I} = \{ua,\ u(a+1),\ \ldots, u(a+\delta-1)\}.$$

Theorem 3. *If* $\mathrm{A}^\diamond$ *contains an interval of length* δ *then*

$$\mathrm{wt}_{\mathrm{H}}(\mathbf{L}_\eta(S; \mathrm{A})) = \mathrm{wt}_{\mathrm{H}}(\mathbf{L}_{\pi(\eta)}(\mathbb{F}_{q^m}; \mathrm{A})) \geqslant \delta + 1.$$

Proof. We have $\pi(\mathbf{L}_\eta(S; \mathrm{A})) = \mathbf{L}_{\pi(\eta)}(\mathbb{F}_{q^m}; \mathrm{A})$. From Proposition 8,

$$\mathrm{wt}_{\mathrm{H}}(\mathbf{L}_\eta(S; \mathrm{A})) = \mathrm{wt}_{\mathrm{H}}(\mathbf{L}_{\pi(\eta)}(\mathbb{F}_{q^m}; \mathrm{A})).$$

From [2, Theorem 6], we have $\mathrm{wt}_{\mathrm{H}}(\mathbf{L}_{\pi(\eta)}(\mathbb{F}_{q^m};\mathrm{A})) \geqslant \delta + 1$. □

Proposition 14. *Let S be a finite chain ring of invariants $(2^n, s)$ and $\ell := 2^{sn} - 1$, $\mathrm{A} := \{1, 2, \ldots, d-1\}$ where $d := 2^{sn-1}$. Then $\mathbf{L}_\eta(S;\mathrm{A}^\diamond)$ is MDS and self-orthogonal.*

Proof. We have A is an interval of length $d-1$ and $\mathrm{A}^\diamond := \mathrm{A} \cup \{0\}$. So We have $\mathbf{L}_\eta(S;\mathrm{A})^\perp = \mathbf{L}_\eta(S;\mathrm{A}^\diamond) = \mathbf{L}_\eta(S;\mathrm{A}) \oplus S \cdot \mathbf{1}$. Thus $\mathbf{L}_\eta(S;\mathrm{A}^\diamond)$ is self-orthogonal and $\mathrm{A}^\diamond$ is also an interval of length d. By Theorem 3, we see that $\mathbf{L}_\eta(S;\mathrm{A}^\diamond)$ is MDS. □

4.2. Free cyclic codes over finite chain rings

We consider the trace-evaluation $\mathrm{Tr}_R^S \circ \mathbf{ev}_\eta : \mathbf{P}_\eta(S;\mathrm{A}) \to R^\ell$ defined as follows:

$$\mathrm{Tr}_R^S \circ \mathbf{ev}_\eta(\lambda X^a) := (\mathrm{Tr}_R^S(\lambda), \mathrm{Tr}_R^S(\lambda\eta^a), \ldots, \mathrm{Tr}_R^S(\lambda\eta^{a(\ell-1)})),$$

for all $a \in \mathrm{A}$ and for all $\lambda \in R$. In the sequel, we write: $\mathbf{C}_\eta(R;\mathrm{A}) := \mathrm{Tr}_R^S(\mathbf{L}_\eta(S;\mathrm{A}))$, and $\mathbf{C}_\eta(R;\mathrm{A})$ is a free cyclic code over R of length ℓ. Let $\mathbf{C}_\ell(R) := \{\mathbf{C}_\eta(R;\mathrm{A})\colon \mathrm{A} \subseteq \Sigma_\ell\}$ be the set of all free cyclic linear codes over R of length ℓ.

Proposition 15. *Let* A, B *be two subsets of* Σ_ℓ. *Then*

1) $\mathbf{L}_\eta(S;\mathtt{C}_q(\mathrm{A}))$ *is the Galois closure of* $\mathbf{L}_\eta(S;\mathrm{A})$ *and* $\mathbf{C}_\eta(R;\mathrm{A}) = \mathbf{C}_\eta(R;\mathtt{C}_q(\mathrm{A}))$;
2) $\mathrm{rank}_S(\mathbf{L}_\eta(S;\mathtt{C}_q(\mathrm{A}))) = |\mathtt{C}_q(\mathrm{A})|$;
3) $\mathbf{C}_\eta(R;\mathrm{A})^\perp = \mathbf{C}_\eta(R;\mathrm{A}^\diamond)$;
4) $\mathbf{C}_\eta(R;\mathrm{A}\cup\mathrm{B}) = \mathbf{C}_\eta(R;\mathrm{A}) + \mathbf{C}_\eta(R;\mathrm{B})$ *and* $\mathbf{C}_\eta(R;\mathrm{A}\cap\mathrm{B}) = \mathbf{C}_\eta(R;\mathrm{A}) \cap \mathbf{C}_\eta(R;\mathrm{B})$.

Proof. Let A, B be two subsets of Σ_ℓ.

1) On the one hand, it is clear that $\sigma(\mathbf{L}_\eta(S;\mathrm{A})) = \mathbf{L}_\eta(S;q\mathrm{A})$. So by Proposition 9, we have

$$\mathrm{Cl}(\mathbf{L}_\eta(S;\mathrm{A})) = \sum_{i=0}^{m-1} \mathbf{L}_\eta(S;q^i\mathrm{A}) = \mathbf{L}_\eta\Bigg(S;\bigcup_{i=0}^{m-1} q^i\mathrm{A}\Bigg).$$

Since $\mathtt{C}_q(\mathrm{A}) = \bigcup_{i=0}^{m-1} q^i\mathrm{A}$, we obtain $\mathrm{Cl}(\mathbf{L}_\eta(S;\mathrm{A})) = \mathbf{L}_\eta(S;\mathtt{C}_q(\mathrm{A}))$ and on the other hand, from Proposition 9, $\mathbf{C}_\eta(R;\mathrm{A}) = \mathrm{Tr}(\mathbf{L}_\eta(S;\mathrm{A})) = \mathrm{Tr}(\mathbf{L}_\eta(S;\mathtt{C}_q(\mathrm{A}))) = \mathbf{C}_\eta(R;\mathtt{C}_q(\mathrm{A}))$.

2) Theorem 2 yields

$$\mathbf{C}_\eta(R;\mathrm{A}) = \mathrm{Tr}(\mathbf{L}_\eta(S;\mathtt{C}_q(\mathrm{A}))) = \mathrm{Res}_R(\mathbf{L}_\eta(S;\mathtt{C}_q(\mathrm{A}))).$$

So $\mathrm{rank}_R(\mathbf{C}_\eta(R;\mathrm{A})) = \mathrm{rank}_S(\mathbf{L}_\eta(S;\complement_q(\mathrm{A}))) = |\complement_q(\mathrm{A})|$.

3) We have

$$\begin{aligned}\mathbf{C}_\eta(R;\mathrm{A})^\perp &= \mathrm{Res}_R(\mathbf{L}_\eta(S;\complement_q(\mathrm{A}))^\perp), \quad \text{by Theorem 2;}\\ &= \mathrm{Res}_R(\mathbf{L}_\eta(S;\complement_q(\mathrm{A})^\diamond)), \quad \text{by Proposition 13;}\\ &= \mathbf{C}_\eta(R;\mathrm{A}^\diamond).\end{aligned}$$

4) By Proposition 13,

$$\mathbf{C}_\eta(R;\mathrm{A}\cup\mathrm{B}) = \mathrm{Tr}(\mathbf{L}_\eta(S;\mathrm{A}\cup\mathrm{B})) = \mathrm{Tr}(\mathbf{L}_\eta(S;\mathrm{A})) + \mathrm{Tr}(\mathbf{L}_\eta(S;\mathrm{B})).$$

Since $\complement_q(\mathrm{A})\cap\complement_q(\mathrm{B}) = \varnothing$, we have $\mathrm{Tr}(\mathbf{L}_\eta(S;\mathrm{A}))\cap\mathrm{Tr}(\mathbf{L}_\eta(S;\mathrm{B})) = \{\underline{\mathbf{0}}\}$. □

Theorem 4. *Let ℓ, q be nonnegative integers such that q is a prime power and $\gcd(q,\ell) = 1$. Then the lattices*

$$\langle\, \mathbf{C}_\ell(R);+,\cap;\{\underline{\mathbf{0}}\},R^\ell\,\rangle \quad \textit{and} \quad \langle\, \Re_\ell(q);\cup,\cap;\varnothing,\Sigma_\ell(q)\,\rangle$$

are isomorphic.

Proof. It is obvious that prove that the map $\mathbf{C}_\eta(R\,;-) : \Re_\ell(q) \to \mathbf{C}_\ell(R)$, is a bijective. From Proposition 15, this map is a lattice isomorphism. □

Corollary 1. *Let ℓ, q be nonnegative integers such that q is a prime power and $\gcd(q,\ell) = 1$. Then the lattices*

$$\langle \mathrm{Cy}(\mathbb{F}_q,\ell);+,\cap;\{\underline{\mathbf{0}}\},\mathbb{F}_q^\ell\rangle \quad \textit{and} \quad \langle\, \mathbf{C}_\ell(R);+,\cap;\{\underline{\mathbf{0}}\},R^\ell\,\rangle$$

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 4, lattices $\langle\, \mathbf{C}_\ell(R_1);+,\cap;\{\underline{\mathbf{0}}\},R_1^\ell\,\rangle$ and $\langle\, \mathbf{C}_\ell(R_2);+,\cap;\{\underline{\mathbf{0}}\},R_2^\ell\,\rangle$ are isomorphic. Since $\mathbf{C}_\ell(\mathbb{F}_q) = \mathrm{Cy}(\mathbb{F}_q,\ell)$, we have the result. □

Lemma 1. *Let $z \in \Sigma_\ell$. Set $m_z := |\complement_q(z)|$ and $\zeta := \eta^{-z}$. Then the map*

$$\begin{aligned}\psi_z : R[\xi^z] &\to \mathbf{C}_\eta(R;\{z\})\\ \mathbf{a} &\mapsto \mathrm{Tr}_R^S(\mathrm{ev}_\eta(\mathbf{a}X^z))\end{aligned}$$

is an R-module isomorphism. Further $\psi_z \circ t_\zeta = \tau_1 \circ \psi_z$, where τ_1 is the cyclic shift and $t_\zeta(\mathbf{a}) = \mathbf{a}\zeta$, for all $\mathbf{a} \in R[\eta]$.

Proof. It is clear that $\mathbf{a} \in \mathrm{Ker}(\psi_z)$ if and only if $\mathbf{a} \in R[\xi^z]^{\perp_{\mathrm{Tr}}} \cap R[\xi^z]$, where duality $\perp_{\mathrm{Tr}}$ is with respect to trace form. As the trace bilinear form is nondegenerate, we have $S = R[\xi^z]^{\perp_{\mathrm{Tr}}} \oplus R[\xi^z]$ and $\mathrm{Ker}(\psi_z) = \{0_R\}$. Hence ψ_z is an R-module monomorphism. We remark that, $\mathbf{C}_\eta(R; \{z\})$ is cyclic, if and only if $\psi_z \circ t_\zeta = \tau_1 \circ \psi_z$. Finally, we have $S = R[\xi]$, and by Proposition 4, the ring $R[\xi^z]$ is the Galois extension of R of degree m_z. Hence, ψ_z is an R-module isomorphism. □

Definition 12. A non trivial cyclic code over R C is said to be *indecomposable*, if for all R-linear cyclic subcodes C_1 and C_2 of C, the implication holds: $C = C_1 \oplus C_2$, then $C_1 = \{\underline{\mathbf{0}}\}$ or $C_2 = \{\underline{\mathbf{0}}\}$.

Proposition 16. *The indecomposable cyclic linear codes over R are precisely $\theta^t \mathbf{C}_\eta(R; \{z\})$s, where $t \in \{0, 1, \ldots, s-1\}$ and $z \in \Sigma_\ell(q)$.*

Proof. By Lemma 1, the free cyclic linear codes over R of length ℓ are $\mathbf{C}_\eta(R; \{z\}))$s where $z \in \{0, 1, \ldots, \ell - 1\}$ and all the cyclic and R-linear subcodes of each cyclic code over R, are indecomposable. Let C be an indecomposable, cyclic and R-linear code and $\mathbb{I}(C)$ be the smallest free, cyclic and R-linear code containing C. Then $A := \mathrm{Soc}(C)$ is also an indecomposable, cyclic and R-linear code and $A \subset \mathbb{I}(C)$ with $\mathrm{rank}_R(A) = \mathrm{rank}_R(\mathbb{I}(C))$. Assume that $|\mathrm{A}| > 1$. Then $\mathbf{C}_\eta(R; \mathrm{A}) = \mathbf{C}_\eta(R; \mathrm{A}_1) \oplus \mathbf{C}_\eta(R; \mathrm{A}_2)$ where $\mathrm{A}_1 \cap \mathrm{A}_2 = \varnothing$, $\mathrm{A}_1 \neq \varnothing$ and $\mathrm{A}_2 \neq \varnothing$. We have $C \cap \mathbf{C}_\eta(R; \mathrm{A}_1) \neq \{\underline{\mathbf{0}}\}$ and $C \cap \mathbf{C}_\eta(R; \mathrm{A}_2) \neq \{\underline{\mathbf{0}}\}$. Therefore $C = (C \cap \mathbf{C}_\eta(R; \mathrm{A}_1)) \oplus (C \cap \mathbf{C}_\eta(R; \mathrm{A}_2))$. It is impossible, because C be an indecomposable. So $|\mathrm{A}| = 1$. Now, $C \subseteq \mathbf{C}_\eta(R; \{z\})$, it follows that $C = \theta^t \mathbf{C}_\eta(R; \{z\})$, for some $t \in \{0, 1, \ldots, s-1\}$. □

5. Sum and intersection of cyclic codes

Consider the map

$$\begin{aligned} \mathbf{C}_{\ell,R} : \Re_\ell(q, s) &\to \mathrm{Cy}(R, \ell) \\ (\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s) &\mapsto \bigoplus_{t=0}^{s-1} \theta^t \mathbf{C}_\eta(R; \mathrm{A}_t). \end{aligned} \tag{4}$$

In this section, on the one hand, we show that the map $\mathbf{C}_{\ell,R} : \Re_\ell(q, s) \to \mathrm{Cy}(R, \ell)$ is bijective and on the other hand we equip the set $\Re_\ell(q, s)$ of binary operations $\sqcup$ and $\sqcap$ such that $\mathbf{C}_{\ell,R} : \langle \Re_\ell(q, s); \sqcup, \sqcap \rangle \to \langle \mathrm{Cy}(R, \ell); +, \cap \rangle$ is a lattice homomorphism.

The following Lemma gives the number of cyclic codes over finite chain rings.

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

Lemma 3 ([7], Corollary 11)**.** *A finite lattice is distributive if and only if it is isomorphic to $\langle 2^{\mathrm{E}}; \cup, \cap; \varnothing, \mathrm{E}\rangle$, where E is a finite set.*

Obviously, $\langle\, \mathbf{C}_\ell(R); +, \cap; \{\underline{\mathbf{0}}\}, R^\ell \,\rangle$ is an sublattice of $\langle \mathrm{Cy}(R,\ell); +, \cap; \{\underline{\mathbf{0}}\}, R^\ell \,\rangle$ and by Theorem 4, $\langle\, \mathbf{C}_\ell(R); +, \cap; \{\underline{\mathbf{0}}\}, R^\ell \,\rangle$ is distributive. Thus Lemmas 2 and 3, give the following fact.

Theorem 5. *Let R be a finite chain ring of invariants (q, s) and ℓ be a nonnegative integer such that $\gcd(\ell, q) = 1$. Then $s \neq 1$ if and only if $\langle \mathrm{Cy}(R,\ell); +, \cap; \{\underline{\mathbf{0}}\}, R^\ell \,\rangle$ is not distributive.*

We show that each cyclic code over R can be written as a direct sum of trace-representable cyclic codes in precisely one way.

Lemma 4. *Let R be a finite chain ring of invariants (q, s). Then the map $\mathbf{C}_{\ell,R} : \Re_\ell(q,s) \to \mathrm{Cy}(R,\ell)$ is a bijection and the type of $\mathbf{C}_{\ell,R}(\underline{\mathrm{A}})$ is $(|\mathsf{C}_q(\mathrm{A}_0)|, |\mathsf{C}_q(\mathrm{A}_1)|, \ldots, |\mathsf{C}_q(\mathrm{A}_{s-1})|)$, for some $\underline{\mathrm{A}} := (\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s) \in \Re_\ell(q,s)$.*

Proof. Let C be a cyclic code over R of length ℓ. From Proposition 15, we have

$$R^\ell = \mathbf{C}_\eta(R; \Sigma_\ell(q)) = \bigoplus_{z\in\Sigma_\ell(q)} \mathbf{C}_\eta(R; \{z\})$$

and $\mathbf{C}_\eta(R;\{z\})$'s are free, indecomposable, cyclic codes over R. It follows that $C = \bigoplus_{z\in\Sigma_\ell(q)} C_z$, where $C_z = \mathbf{C}_\eta(R;\{z\}) \cap C$. By Proposition 16, $C_z = \theta^{t_z}\mathbf{C}_\eta(R;\{z\})$, where $t_z \in \{0, 1, \ldots, s\}$. Thus $\bigoplus_{z\in\Sigma_\ell(q)} \theta^{t_z}\mathbf{C}_\eta(R;\{z\}) = \mathbf{C}_{\ell,R}(\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s)$, where $\mathrm{A}_t = \{z \in \Sigma_\ell \colon t_z = t\}$. Since $|\Re_\ell(q,s)| = (s+1)^{|\Sigma_\ell(q)|}$, by Theorem 2, the uniqueness of $\underline{\mathrm{A}} := (\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s) \in \Re_\ell(q,s)$ such that $C = \mathbf{C}_{\ell,R}(\mathrm{A})$ is guaranteed. Moreover, for all $t \in \{0, 1, \ldots, s-1\}$, the cyclic code over R $\mathbf{C}_\eta(R; \mathrm{A}_t)$ is free and $\mathrm{rank}_R(\mathbf{C}_\eta(R;\mathrm{A}_t)) = |\mathsf{C}_q(\mathrm{A}_t)|$. Since the direct sum $\bigoplus_{t=0}^{s-1} \theta^t \mathbf{C}_\eta(R;\mathrm{A}_t)$ gives the type of $\mathbf{C}_{\ell,R}(\underline{\mathrm{A}})$, the type of $\mathbf{C}_{\ell,R}(\underline{\mathrm{A}})$ is $(k_0, k_1, \ldots, k_{s-1})$, where $k_t := |\mathsf{C}_q(\mathrm{A}_t)|$, for all $0 \leqslant t < s-1$. □

Definition 13. Let C be a cyclic code over R of length ℓ. The *defining multiset* of C is the (q,s)-partition cyclotomic $\underline{\mathrm{A}}$ modulo ℓ, such that $C = \mathbf{C}_{\ell,R}(\underline{\mathrm{A}})$.

Proposition 17. *Let*

$$\underline{\mathrm{A}} := (\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s) \in \Re_\ell(q,s) \quad \textit{and} \quad t \in \{0, 1, \ldots, s-1\}.$$

Then

$$\mathbf{C}_{\ell,R}(\underline{\mathrm{A}})^{\perp} = \mathbf{C}_{\ell,R}(\underline{\mathrm{A}}^{\widetilde{\diamond}}),$$

where $\underline{\mathrm{A}}^{\widetilde{\diamond}} := (-\mathrm{A}_s, -\mathrm{A}_{s-1}, \ldots, -\mathrm{A}_1, -\mathrm{A}_0)$.

Proof. Let $\underline{\mathrm{A}} := (\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s) \in \Re_\ell(q,s)$. We have

$$\mathbf{C}_{\ell,R}(\underline{\mathrm{A}})^{\perp} \supseteq \bigcap_{u=0}^{s-1} (\theta^{s-u} R^{\ell} + \mathbf{C}_{\eta}(R; \mathrm{A}_u^{\diamond}))$$

and

$$\theta^{s-t}\mathbf{C}_{\eta}(R; -\mathrm{A}_t) \subseteq \bigcap_{u=0}^{s-1} (\theta^{s-u} R^{\ell} + \mathbf{C}_{\eta}(R; \mathrm{A}_u^{\diamond})),$$

for all $t \in \{1, 2, \ldots, s\}$. It follows that

$$\mathbf{C}_{\ell,R}(-\mathrm{A}_s, -\mathrm{A}_{s-1}, \ldots, -\mathrm{A}_1, -\mathrm{A}_0) \subseteq \mathbf{C}_{\ell,R}(\underline{\mathrm{A}})^{\perp}.$$

From Proposition 7 and Theorem 6, $\mathbf{C}_{\ell,R}(-\mathrm{A}_s, -\mathrm{A}_{s-1}, \ldots, -\mathrm{A}_1, -\mathrm{A}_0)$ and $\mathbf{C}_{\ell,R}(\underline{\mathrm{A}})^{\perp}$ have the same type, we have

$$\mathbf{C}_{\ell,R}(\underline{\mathrm{A}})^{\perp} = \mathbf{C}_{\ell,R}(-\mathrm{A}_s, -\mathrm{A}_{s-1}, \ldots, -\mathrm{A}_1, -\mathrm{A}_0). \qquad \square$$

Corollary 2. *Let* $\underline{\mathrm{A}} := (\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s) \in \Re_\ell(q,s)$. *Then* $\mathbf{C}_{\ell,R}(\underline{\mathrm{A}})$ *is self-dual if and only if* $\mathrm{A}_t = -\mathrm{A}_{s-t}$, *for all* $t \in \{0, 1 \ldots, s\}$.

Corollary 3. *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* Σ_ℓ *such that* $\mathrm{A} \neq -\mathrm{A}$;
2) *the nontrivial self-dual cyclic linear codes over R of length ℓ exist.*

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

1) ⇒ 2). Assume that there exists a subset A of Σ_ℓ such that $\mathsf{C}_q(\mathrm{A}) \neq -\mathsf{C}_q(\mathrm{A})$. Set $u = \frac{s}{2}$, and $\mathrm{B} := \overline{\mathrm{A} \cup (-\mathrm{A})}$. Consider

$$C := \mathbf{C}_{\ell,R}(\ldots, \varnothing, \mathrm{A}_{u-1}, \mathrm{A}_u, \mathrm{A}_{u+1}, \varnothing, \ldots),$$

where $\mathrm{A}_{u-1} := \mathsf{C}_q(\mathrm{A})$, $\mathrm{A}_u := \mathsf{C}_q(\mathrm{B})$ and $\mathrm{A}_{u+1} := -\mathrm{A}_{u-1}$. We have $\mathrm{A}_{s-u+1} = -\mathrm{A}_{u+1}$, $\mathrm{A}_u = -\mathrm{A}_{s-u} = -\mathrm{A}_u$ and $\mathrm{A}_t = -\mathrm{A}_{s-t} = \varnothing$, for all $t \in \{0, 1, \dots, u-2\}$. Thanks to Corollary 2, we can affirm that C is self-dual.

2) $\Rightarrow$ 1) Now, we assume that C is a self-dual cyclic code over R of length ℓ and every subset A of Σ_ℓ satisfies $\mathrm{A} = -\mathrm{A}$. Set $C = \mathbf{C}_{\ell,R}(\mathrm{A}_0, \mathrm{A}_1, \mathrm{A}_2, \dots, \mathrm{A}_s)$. From Corollary 2, $\mathrm{A}_t = -\mathrm{A}_{s-t}$, for all $t \in \{0, 1, \dots, s\}$. Since $-\mathrm{A}_{s-t} = \mathrm{A}_{s-t}$, we have $\mathrm{A}_t = \mathrm{A}_{s-t} = \varnothing$ for all $t \in \{0, 1 \dots, s\} \setminus \{\frac{s}{2}\}$ and $\mathrm{A}_{\frac{s}{2}} = \Sigma_\ell(q)$. Therefore,

$$C = \mathbf{C}_{\ell,R}(\dots, \varnothing, \Sigma_\ell(q), \varnothing, \dots) = \theta^{\frac{s}{2}} R^\ell,$$

which is the trivial self-dual code. □

In order to determine the defining multiset of the sum and the intersection of cyclic codes over R, we extend the binary operations $\cup$ and $\cap$ of $\Re_\ell(q)$ to $\Re_\ell(q, s)$ as follows:

1) $\underline{\mathrm{A}} \sqcup \underline{\mathrm{B}} := (\mathrm{C}_0, \mathrm{C}_1, \dots, \mathrm{C}_s)$, where $\mathrm{C}_0 := \mathrm{A}_0 \cup \mathrm{B}_0$ and $\mathrm{C}_t := (\mathrm{A}_t \cup \mathrm{B}_t) \setminus (\overset{t-1}{\underset{u=0}{\cup}} \mathrm{C}_u)$, for all $0 < t \leqslant s$.

2) $\underline{\mathrm{A}} \sqcap \underline{\mathrm{B}} := (\underline{\mathrm{A}}^{\widetilde{\diamond}} \vee \underline{\mathrm{B}}^{\widetilde{\diamond}})^{\widetilde{\diamond}}$.

for all $\underline{\mathrm{A}} := (\mathrm{A}_0, \mathrm{A}_1, \dots, \mathrm{A}_s)$ and $\underline{\mathrm{B}} := (\mathrm{B}_0, \mathrm{B}_1, \dots, \mathrm{B}_s)$ be elements of $\Re_\ell(q, s)$.

Theorem 6. *The map* (4) *is a lattice isomorphism of*

$$\langle\, \Re_\ell(q, s); \sqcup, \sqcap; \underline{\varnothing}, \underline{\Sigma_\ell(q)}\,\rangle \quad \text{to} \quad \langle\, \mathrm{Cy}(R, \ell); +, \cap; \{\underline{\mathbf{0}}\}, R^\ell \rangle,$$

where $\underline{\varnothing} := (\varnothing, \dots, \varnothing, \Sigma_\ell(q))$ *and* $\underline{\Sigma_\ell(q)} := (\Sigma_\ell(q), \varnothing, \dots, \varnothing)$.

Proof. Let $\underline{\mathrm{A}} := (\mathrm{A}_0, \mathrm{A}_1, \dots, \mathrm{A}_s) \in \Re_\ell(q, s)$, and $\underline{\mathrm{B}} := (\mathrm{B}_0, \mathrm{B}_1, \dots, \mathrm{B}_s) \in \Re_\ell(q, s)$. We have

$$\begin{aligned}
&\mathbf{C}_{\ell,R}(\underline{\mathrm{A}}) + \mathbf{C}_{\ell,R}(\underline{\mathrm{B}}) \\
&\qquad = \sum_{t=0}^{s-1} \theta^t (\mathbf{C}_\eta(R; \mathrm{A}_t) + \mathbf{C}_\eta(R; \mathrm{B}_t)), \quad \text{by the associativity of } +, \\
&\qquad = \mathbf{C}_\eta(R; \mathrm{A}_0 \cup \mathrm{B}_0) \oplus \theta \mathbf{C}_\eta(R; (\mathrm{A}_1 \cup \mathrm{B}_1) \setminus (\mathrm{A}_0 \cup \mathrm{B}_0)) \\
&\qquad\quad \oplus \cdots \oplus \theta^t \mathbf{C}_\eta\Big(R; (\mathrm{A}_t \cup \mathrm{B}_t) \setminus (\bigcup_{u=0}^{t-1} (\mathrm{A}_u \cup \mathrm{B}_u))\Big) \\
&\qquad\quad \oplus \cdots \oplus \theta^{s-1} \mathbf{C}_\eta\Big(R; (\mathrm{A}_{s-1} \cup \mathrm{B}_{s-1}) \setminus (\bigcup_{u=0}^{s-2} (\mathrm{A}_u \cup \mathrm{B}_u))\Big) \\
&\qquad = \mathbf{C}_{\ell,R}(\underline{\mathrm{A}} \sqcup \underline{\mathrm{B}}).
\end{aligned}$$

From Propositions 6 and 17, we deduce that $\mathbf{C}_{\ell,R}(\underline{\mathrm{A}})\cap\mathbf{C}_{\ell,R}(\underline{\mathrm{B}}) = \mathbf{C}_{\ell,R}(\underline{\mathrm{A}}\sqcap\underline{\mathrm{B}})$. Finally, by Lemma 4, we have the expected result. □

References

[1] A. Batoul, K. Guenda, and T.A. Guelliver, *On the self-dual cyclic codes over finite chain rings*, Des. Codes Cryptogr. 70(**1**): (2014), pp. 347-358.

[2] J. Bierbrauer , *The Theory of Cyclic Codes and a Generalization to Additive Codes.* Des.Codes.Cryptogr. 25(**2**): (2002), pp. 189-206.

[3] A. R. Calderbank and N. J. A. Sloane , *Modular and p-adic cyclic codes*, Des. Codes Cryptogr. **6**(1): (1995), pp. 21-35.

[4] F. DeMeyer and E. Ingraham, *Separable Algebras Over Commutative Rings*, Springer, 1971.

[5] H. Dinh and S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory 50 (**8**) (2004), pp. 1728-1744.

[6] A. Fotue Tabue and C. Mouaha, *A New Approach of Free Cyclic Linear Codes over Commutative Finite Chain Rings.* GJPAM, **9**(5), 475-482 (2013).

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

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

[9] H. Horimoto and K. Shiromoto, *On generalized Hamming weights for codes over finite chain rings.* In: Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer-Verlag, Berlin, Heidelberg, 2001, 141-150.

[10] P. Kanwar and S. R. López-Permouth , *Cyclic codes over the interger modulo p^m*, Finite Fields Appl. Vol **3** (1997), pp. 334-352.

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

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

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

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

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

Contact information

Alexandre Fotue-Tabue
Department of Mathematics, Faculty of Science, University of Yaoundé 1, Cameroon
E-Mail(s): alexfotue@gmail.com

Christophe Mouaha
Department of Mathematics, Higher Teachers Training College, University of Yaoundé 1, Cameroon
E-Mail(s): cmouaha@yahoo.fr

Received by the editors: 16.03.2017.