Finite Fields and Their Applications 77 (2022) 101950

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Hulls of cyclic serial codes over a finite chain ring

Sarra Talbi [a], Aicha Batoul [a], Alexandre Fotue Tabue [b], Edgar Martínez-Moro [c,*,1]

[a] *Faculty of Mathematics USTHB, University of Science and Technology of Algiers, Algeria*
[b] *Department of Mathematics, HTTC Bertoua, The University of Ngaoundéré, Cameroon*
[c] *Institute of Mathematics, University of Valladolid, Castilla, Spain*

ARTICLE INFO

Article history:
Received 13 February 2021
Received in revised form 21 September 2021
Accepted 14 October 2021
Available online xxxx
Communicated by W. Cary Huffman

MSC:
13B02
94B05

Keywords:
Finite chain ring
Cyclotomic coset
Cyclic serial code
Galois dual code
Average p^r-dimension

ABSTRACT

In this paper, we explore some properties of hulls of cyclic serial codes over a finite chain ring and we provide an algorithm for computing all the possible parameters of the Euclidean hulls of that codes. We also establish the average p^r-dimension of the Euclidean hull, where $\mathbb{F}_{p^r}$ is the residue field of R, as well as we give some results of its relative growth.

* Corresponding author.
E-mail addresses: talbissarra@gmail.com (S. Talbi), a.batoul@hotmail.fr (A. Batoul), alexfotue@gmail.com (A. Fotue Tabue), edgar.martinez@uva.es (E. Martínez-Moro).

1 This author is partially funded by the Spanish Research Agency (AEI) under Grant PGC2018-096446-B-C21.

https://doi.org/10.1016/j.ffa.2021.101950

1. Introduction

The Euclidean hull is defined to be the intersection of a code and its Euclidean dual. It was originally introduced in [1] to classify finite projective planes. Knowing the hull of a linear code is also a key point to determine the complexity of some algorithms for investigating permutations of two linear codes and computing the automorphism group of the code [11,15,16]. In general, those algorithms have been proved to be very effective if the size of the Euclidean hull is small. In the case of codes over finite fields, Sendrier [17] established the number of linear codes of length n with a fix dimension Euclidean hull, also Skersys [19] discussed the average dimension of the Euclidean hull of cyclic codes. Later, Sangwisut et al. [18] determined the dimension of the Euclidean hull of cyclic and negacyclic codes of length n over a finite field. Furthermore, in [9] the authors gave the average Euclidean hull dimension of negacyclic codes over a finite field. Recently, the concept of the Euclidean hulls has been generalized to cyclic codes of odd length over $\mathbb{Z}_4$ in [10] where the authors provided an algorithm to determine the type of the Euclidean hull of cyclic codes over $\mathbb{Z}_4$.

An important class of linear codes over rings is the class of cyclic codes and they have been extensively studied, see for example [4,5,7,13,14]. In particular, Dinh and Permouth [4] gave the algebraic structure of simple root cyclic codes over finite chain rings R and in [13] this was generalized to multivariable cyclic codes. Free cyclic serial codes have been determined by using cyclotomic cosets and trace map over finite chain rings [5]. It is clear that the Euclidean hull of cyclic codes is also cyclic, two special families of cyclic codes are of great interest, namely linear complementary dual codes, which are codes whose Euclidean hull is trivial (see for example [3]) and self-orthogonal codes, which are linear codes whose Euclidean hulls are the whole code (see for example [20,2]). These works motivate us to study the hulls of cyclic codes over finite chain rings. In this paper, we focus on the study of the hulls of cyclic codes of length n over a finite chain ring R of parameters (p, r, a, e, r) such that n and p are coprime. This is the serial case stated in [13], i.e. the cyclic codes over R whose length n is coprime with p are serial modules over R. We will generalize the techniques used in [10] (for $\mathbb{Z}_4$) to obtain the parameters and the average p^r-dimensions Euclidean hull of cyclic serial codes over finite chain rings.

The paper is organized as follows. In Section 2, some preliminary concepts and some basic results are recalled. In Section 3, we characterize Galois hulls of cyclic serial code over finite chain rings. Section 4 shows the parameters and the q-dimensions of the Euclidean hull of cyclic serial codes. Finally, the average dimension of the Euclidean hull of cyclic serial codes is computed in Section 5.

2. Preliminaries

2.1. Chain rings

For an account on the results on finite rings in this section check [12]. Throughout this paper, p is a prime number, a, e, r, s are positive integers and $\mathbb{Z}_{p^a}$ is the residue ring of integers modulo p^a. R will denote a finite commutative chain ring of characteristic p^a, of nilpotency index s, and of residue field $\mathbb{F}_q$ (where $q = p^r$). We will denote its maximal ideal by $\mathtt{J}(R)$ and $R^\times$ will denote its multiplicative group. Note that since R is a chain ring it is a principal ideal ring, thus we will denote by θ a generator of $\mathtt{J}(R)$, the ideals of R form a chain under inclusion $\{0\} = \mathtt{J}(R)^s \subsetneq \mathtt{J}(R)^{s-1} \subsetneq \cdots \subsetneq \mathtt{J}(R) \subsetneq R$ and $\mathtt{J}(R) = \theta^t R$ for $0 \leq t < s$.

The ring epimorphism $\pi : R \to R/\mathtt{J}(R) \simeq \mathbb{F}_q$ naturally extends a ring epimorphism from $R[X]$ to $\mathbb{F}_{p^r}[X]$ and on the other hand it naturally induces an R-module epimorphism from R^n to $(\mathbb{F}_{p^r})^n$. As an abuse of notation we will denote both mappings by π.

A monic polynomial f is *basic-irreducible* over R if $\pi(f)$ is irreducible over $\mathbb{F}_{p^r}$. We will denote by $\mathtt{GR}(p^a, r)$ the *Galois ring* of characteristic p^a and cardinality p^{ra}. It is well known that, for a given finite chain ring R there is a 5-tuple (p, a, r, e, s) of positive integers, the so-called parameters of R, such that $R = \mathtt{GR}(p^a, r)[\theta]$, and $\langle\theta\rangle = \mathtt{J}(R)$, $\theta^e \in p(\mathbb{Z}_{p^a}[\theta])^\times$ and $\theta^{s-1} \neq \theta^s = 0_R$. From now on, we will denote as S_d the subring of R such that $S_d := \mathtt{GR}(p^a, d)[\theta]$ and d is a divisor of r. The *Teichmüller set* of R will be denoted as $\Gamma(R)$ and it is defined as $\Gamma(R) = \{0\} \cup \{a \in R \,:\, a^{p^r-2} \neq a^{p^r-1} = 1\}$. It is the only cyclic subgroup of $R^\times$ isomorphic to the multiplicative group of $\mathbb{F}_{p^r}$. For each element a in R, there is a unique $(a_0, a_1, \cdots, a_{s-1})$ in $\Gamma(R)^s$ such that $a = a_0 + a_1\theta + \cdots + a_{s-1}\theta^{s-1}$.

Let R and S be two finite commutative chain rings, we say that we say that R is an extension of S and we denote it by $S|R$ if $S \subset R$ and $1_R = 1_S$. We say that the extension is separable if $J(S)R = J(R)$. The Galois group of the extension $S|R$, denoted $\mathtt{Aut}_S(R)$, is the group of all the automorphisms γ of R whose restriction $\gamma_{|S}$ of γ to S, is the identity map of R. A separable extension is called Galois if $\{r \in R \,:\, (\forall\gamma \in \mathtt{Aut}_S(R))(\gamma(r) = r)\} = S$. This condition is equivalent to the condition R is ring-isomorphic to $S[X]/\langle f\rangle$, where f is a monic basic irreducible polynomial in $S[X]$, see [22, Section 4][12, Theorem XIV.8].

Let d be positive divisor of r, and let us consider $S = \mathbb{Z}_{p^a}[\theta]$, $R = \mathtt{GR}(p^a, r)[\theta]$, $S_d = \mathtt{GR}(p^a, d)[\theta]$, and

$$\mathtt{GSub}(S|R) := \{S_d \,:\, d \text{ is a divisor of } r \text{ and } \mathbb{Z}_{p^a}[\theta] \subseteq S_d\}.$$

It is well known that $\mathtt{Aut}_S(R)$ is a cyclic group generated by the *Frobenius automorphism* $\sigma : R \to R$ given by: $\sigma\left(\sum_{t=0}^{s-1} a_t\theta^t\right) = \sum_{t=0}^{s-1} a_t^p\theta^t$, and therefore, the set $\mathtt{Sub}(\mathtt{Aut}_S(R))$ of subgroups of $\mathtt{Aut}_S(R)$ is given by

$$\mathtt{Sub}(\mathtt{Aut}_S(R)) = \{\langle\sigma^d\rangle \,:\, d \text{ is a divisor of } r\}.$$

In [6], the authors established the Galois correspondence $(\mathtt{Stab}; \mathtt{Fix})$ between $\mathtt{GSub}(S|R)$ and $\mathtt{Sub}(\mathtt{Aut}_S(R))$ as follows $\mathtt{Stab} : \mathtt{GSub}(S|R) \to \mathtt{Sub}(\mathtt{Aut}_S(R))$ and $\mathtt{Fix} : \mathtt{Sub}(\mathtt{Aut}_S(R)) \to \mathtt{GSub}(S|R)$ where $\mathtt{Stab}(S_d) = \langle\sigma^d\rangle$ and $\mathtt{Fix}(\langle\sigma^d\rangle) = S_d$, where d is a divisor of r (recall that $q = p^r$).

Given a divisor d of r, from [12, Theorem XV.2], σ^d is the only automorphism in $\mathtt{Aut}_S(R)$ such that $\overline{\sigma}^d \circ \pi = \pi \circ \sigma^d$, where $\overline{\sigma}$ is a generator of $\mathtt{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^r})$. The trace map $\mathtt{T}_d : S \to S_d$ of the ring extension $R|S_d$ is defined by $\mathtt{T}_d := \sum_{i=0}^{\frac{r}{d}-1} \sigma^{id}$, and the trace map $\overline{\mathtt{T}}_d : \mathbb{F}_{p^r} \to \mathbb{F}_{p^d}$ of the field extension $\mathbb{F}_{p^r}|\mathbb{F}_{p^d}$ is defined by $\overline{\mathtt{T}}_d := \sum_{i=0}^{\frac{r}{d}-1} \overline{\sigma}^{id}$. It is well known that $\mathtt{T}_d : R \to S_q$ is an epimorphism of S_d-modules and $\overline{\mathtt{T}}_d : \mathbb{F}_{p^d} \to \mathbb{F}_{p^r}$ is an epimorphism of vector spaces over $\mathbb{F}_{p^d}$. Hence, for any divisor d of r, the following diagram commutes.

$$\begin{array}{ccccc} R & \xrightarrow{\sigma^d} & R & \xrightarrow{\mathtt{T}_d} & S_d \\ \pi\downarrow & & \pi\downarrow & & \downarrow\pi \\ \mathbb{F}_{p^r} & \xrightarrow{\overline{\sigma}^d} & \mathbb{F}_{p^r} & \xrightarrow{\overline{\mathtt{T}}_d} & \mathbb{F}_{p^d} \end{array}$$

2.2. Codes over a chain ring

A *linear code* C of length n over a ring R, is a submodule of the R-module R^n. We will denote by $\{\mathbf{0}\}$, the zero-submodule where $\mathbf{0} = (0, 0, \dots, 0) \in R^n$. A linear code C over R is free if, $C \cong R^k$ as R-modules for some positive integer k. The residue code of a linear code C over R is the linear code $\pi(C)$ over $\mathbb{F}_q$, where

$$\pi(C) = \{(\pi(c_0), \pi(c_1), \cdots, \pi(c_{n-1}) : (c_0, c_1, \cdots, c_{n-1}) \in C\}.$$

In [6], the authors introduced the Galois closure of a linear code C over R of length n as follows, $\mathtt{Cl}_d(C) = \mathtt{Ext}(\mathtt{T}_d(C))$, where $\mathtt{Ext}(\mathtt{T}_d(C))$ is the linear code over R of all R-combinations of codewords in the linear code $\mathtt{T}_d(C)$ over S_d. A linear code C over R is $\langle\sigma^d\rangle$-invariant, if $\sigma^d(C) = C$, where d is a divisor of r. Recall that for any linear code C over R of length n, its subring subcode is given by $\mathtt{Res}_d(C) = C \cap (S_d)^n$. In [6], it is shown that any linear code C over R is $\langle\sigma^d\rangle$-invariant, if and only if, $\mathtt{T}_d(C) = \mathtt{Res}_d(C)$ if and only if, $C = \mathtt{Ext}(\mathtt{Res}_d(C))$. For $\ell \in \{0, 1, \dots, r-1\}$ we equip R^n with the ℓ-Galois inner-product defined as follows:

$$\langle\, \mathbf{u},\, \mathbf{v}\rangle_\ell = \sum_{j=0}^{n-1} u_j \sigma^\ell(v_j), \qquad \text{for all } \mathbf{u}, \mathbf{v} \in R^n.$$

When $\ell = 0$ it is just the usual Euclidean inner-product and if r is even and $r = 2\ell$ it is the Hermitian inner-product. The ℓ-Galois dual of a linear code C over R of length n, denoted $C^{\perp_\ell}$, is defined to be the linear code

$$C^{\perp_\ell} = \{\mathbf{u} \in R^n \;:\; \langle\, \mathbf{u},\, \mathbf{c}\rangle_\ell = 0_R \text{ for all } \mathbf{c} \in C\}.$$

If $C \subseteq C^{\perp_\ell}$, then C is ℓ-Galois *self-orthogonal*. Moreover, C is ℓ-Galois self-dual if, $C = C^{\perp_\ell}$. The two statements in Proposition 2 below follow immediately from the identity

$$\langle \mathbf{u}, \mathbf{v}\rangle_\ell = \langle \mathbf{u}, \sigma^h(\mathbf{v})\rangle_{\ell-h} = \sigma^h\left(\langle \sigma^{\ell-h}(\mathbf{v}), \mathbf{u}\rangle_{r-h}\right), \text{ for all } 0 \le h \le \ell, \mathbf{u}, \mathbf{v} \in R^n$$

where the action is taken componentwise $\sigma^\ell(\mathbf{v}) = (\sigma^\ell(v_0), \cdots, \sigma^\ell(v_{n-1}))$. The following proposition is a generalized Delsarte's Theorem.

Proposition 1. *([6, Theorem 3.3]) Let C be a linear code over R of length n. Then for any $\ell \in \{0, 1, \ldots, r-1\}$, $\mathtt{T}_d(C^{\perp_\ell}) = (\mathtt{Res}_d(C))^{\perp_\ell}$.*

Also [8, Proposition 2.2] has a natural generalization to finite chain rings.

Proposition 2. *Let C be a linear code over R of length n. Then*

1. $\left(\sigma^h(C)\right)^{\perp_\ell} = \sigma^h(C^{\perp_\ell})$, *and* $C^{\perp_\ell} = \sigma^h(C^{\perp_{\ell-h}})$, *for any* $0 \le h \le \ell$*;*
2. $(C^{\perp_\ell})^{\perp_h} = \sigma^{2r-\ell-h}(C)$, *for all* $0 \le \ell, h \le r-1$.

From Proposition 2 and [7, Theorem 3.1], we obtain the following result.

Corollary 1. *Let C and C' be linear codes over R of length n. Then*

1. $(C + C')^{\perp_\ell} = C^{\perp_\ell} \cap C'^{\perp_\ell}$*;*
2. $(C \cap C')^{\perp_\ell} = C^{\perp_\ell} + C'^{\perp_\ell}$.

Definition 1. Let C be a linear code over R. The ℓ-*Galois hull* of C will be denoted as $\mathcal{H}_\ell(C)$, is the intersection of C and its ℓ-Galois dual, that is,

$$\mathcal{H}_\ell(C) = C \cap C^{\perp_\ell}.$$

A linear code C over R is ℓ-*Galois Linear Complementary Dual* (Shortly, Galois LCD) if $\mathcal{H}_\ell(C) = \{\mathbf{0}\}$, and C is ℓ-*Galois self-orthogonal* if $\mathcal{H}_\ell(C) = C$. If we denote that for all $0 \le \ell; h \le r-1$, we have $\sigma^h(\mathcal{H}_\ell(C)) = \mathcal{H}_\ell(\sigma^h(C))$, and $\mathcal{H}_\ell(C) = \mathcal{H}_{r-\ell}(C^{\perp_\ell})$. From the generalized Delsarte's Theorem in Proposition 1, it follows that $\mathtt{T}_d(\mathcal{H}_\ell(C)) = (\mathtt{Res}_d(\mathcal{H}_{r-\ell}(C)))^{\perp_\ell}$. Note that if C is $\langle \sigma^\ell \rangle$-invariant, then $\mathcal{H}_\ell(C) = \mathcal{H}_0(C)$.

From [14, Proposition 3.2 and Theorem 3.5], for any linear code C over R of length n, there is a unique s-tuple $(k_0, k_1, \cdots, k_{s-1})$ of positive integers, such that C has a generator matrix in standard form

$$\begin{pmatrix} \mathrm{I}_{k_0} & \mathrm{G}_{0,1} & \mathrm{G}_{0,2} & \cdots & \mathrm{G}_{0,s-2} & \mathrm{G}_{0,s-1} & \mathrm{G}_{0,s} \\ \mathrm{O} & \theta\mathrm{I}_{k_1} & \theta\mathrm{G}_{1,2} & \cdots & \theta\mathrm{G}_{1,s-2} & \theta\mathrm{G}_{1,s-1} & \theta\mathrm{G}_{1,s} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \cdots & \mathrm{O} & \theta^{s-1}\mathrm{I}_{k_{s-1}} & \theta^{s-1}\mathrm{G}_{s-1,s} \end{pmatrix} \mathrm{U},$$

where U is a suitable permutation matrix and O the all zeros matrix of suitable size. The elements in the s-tuple $(k_0, k_1, \cdots, k_{s-1})$ are called parameters of C and the rank of C is $k_0 + k_1 + \cdots + k_{s-1}$. From [14, Theorem 3.10], the parameters of $C^{\perp_\ell}$ are $(n - k, k_{s-1}, \cdots, k_2, k_1)$, where $k = \mathtt{rank}_R(C)$. Note that C is free if and only if $\mathtt{rank}_R(C) = k_0$ and $k_1 = \cdots = k_{s-1} = 0$. The q-dimension of a linear code C over R, denoted $\mathtt{dim}_q(C)$, is defined to be $\mathtt{log}_q(|C|)$. Thus the q-dimension of a linear code C over R of parameters $(k_0, k_1, \cdots, k_{s-1})$ is $\sum_{t=0}^{s-1}(s-t)k_t$. Since R is also a Frobenius ring, it follows that $\mathtt{dim}_q(C) + \mathtt{dim}_q(C^{\perp_\ell}) = sn$.

Proposition 3. *Let C and C' be two codes over R of the same length. Then*

$$\mathtt{dim}_q(C + C') = \mathtt{dim}_q(C) + \mathtt{dim}_q(C') - \mathtt{dim}_q(C \cap C').$$

Moreover $\mathtt{dim}_q(\mathcal{H}_\ell(C)) = \mathtt{dim}_q(\mathcal{H}_{r-\ell}(C))$.

Proof. The map $\eta : C \times C' \to C + C'$ defined as follows: $\eta(x; x') = x + x'$, is an R-module epimorphism. From the First Isomorphism Theorem, it follows that $C \times C'/\mathtt{Ker}(\eta)$ and $C + C'$ are isomorphic as R-modules. Since $\mathtt{Ker}(\eta) = \{(x; -x) \ : x \in C \cap C'\}$, it is easy to see that $\mathtt{Ker}(\eta)$ and $C \cap C'$ are isomorphic R-modules. Thus $|C + C'| = \frac{|C|}{|C \cap C'|} \times |C'|$. Therefore $\log_q(|C+C'|) = \log_q(|C|) - \log_q(|C \cap C'|) + \log_q(|C'|)$. From the definition of q-dimension of a linear code we have that $\mathtt{dim}_q(C+C') = \mathtt{dim}_q(C) + \mathtt{dim}_q(C') - \mathtt{dim}_q(C \cap C')$. Moreover,

$$\begin{aligned}
\mathtt{dim}_q(\mathcal{H}_\ell(C)) &= \mathtt{dim}_q((C + C^{\perp_{r-\ell}})^{\perp_\ell}),\ \text{from Corollary 1 ;} \\
&= sn - \mathtt{dim}_q(C + C^{\perp_{r-\ell}}),\ \text{since } \mathtt{dim}_q(C + C^{\perp_{r-\ell}}) \\
&\quad + \mathtt{dim}_q((C + C^{\perp_{r-\ell}})^{\perp_\ell}) = sn; \\
&= sn - \left(\mathtt{dim}_q(C) + \mathtt{dim}_q(C^{\perp_{r-\ell}}) - \mathtt{dim}_q(\mathcal{H}_{r-\ell}(C))\right); \\
&= \mathtt{dim}_q(\mathcal{H}_{r-\ell}(C)),\ \text{since } \mathtt{dim}_q(C) + \mathtt{dim}_q(C^{\perp_{r-\ell}}) = sn. \quad \square
\end{aligned}$$

Proposition 4. *Let C be a free code over R of length n and ℓ be a positive integer. Then*

1. $\mathtt{dim}_q(\sigma^\ell(C)) = s \times \mathtt{rank}(\sigma^\ell(C)) = s \times \mathtt{dim}_q(\pi(\sigma^\ell(C)))$;
2. $\pi(C)^{\perp_\ell} = \pi(C^{\perp_\ell})$;
3. $\pi(\mathcal{H}_\ell(C)) = \mathcal{H}_\ell(\pi(C))$.

Proof. Since C is free, a generator matrix for $\sigma^\ell(C)$ is $\left(\mathrm{I}_k \middle| \sigma^\ell(\mathrm{A})\right)\mathrm{U}$, where A is a $k \times (n-k)$-matrix over R and U is a permutation matrix. Thus $\left(\mathrm{I}_k \middle| \pi(\sigma^\ell(\mathrm{A}))\right)\mathrm{U}$ is a generator matrix for $\pi(C)$. It follows that $|\sigma^\ell(C)| = q^{sk}$ and $\mathtt{rank}(\sigma^\ell(C)) = \mathtt{dim}_q(\pi(\sigma^\ell(C))) = k$. This proves Item 1. Now to prove Item 2. The codes $\pi(C)^{\perp_\ell}$ and $\pi(C^{\perp_\ell})$ have the same parity matrix, which is $\left(\mathrm{I}_k \middle| \pi(\sigma^\ell(\mathrm{A}))\right)\mathrm{U}$. Hence $\pi(C)^{\perp_\ell} = \pi(C^{\perp_\ell})$. Item 3. is a consequence of the fact that the above diagram commutes, $\pi(\mathcal{H}_\ell(C)) \subseteq \mathcal{H}_\ell(\pi(C))$ and $\mathtt{dim}_q(\pi(\mathcal{H}_\ell(C))) = \mathtt{dim}_q(\mathcal{H}_\ell(\pi(C)))$. $\square$

3. Galois hulls of cyclic serial codes

Let $\mathbb{N}$ be the set of nonnegative integers and n be a positive integer such that $\mathtt{gcd}(n,q)=1$. Set $[|a;b|]=\{a,a+1,\cdots,b\}$ where $(a,b)\in\mathbb{N}^2$ such that $a<b$. Let A and B be two subsets in $[|0;n-1|]$, as usual, the opposite of A, denoted $-\mathrm{A}$, is defined as $-\mathrm{A}=\{n-z \ : \ z\in \mathrm{A}\}$ and its complementary, denoted $\overline{\mathrm{A}}$, is defined as: $\overline{\mathrm{A}}=\{z\in[|0;n-1|] \ : \ z\notin \mathrm{A}\}$. The set A is symmetric, if $\mathrm{A}=-\mathrm{A}$, and the pair $\{\mathrm{A},\mathrm{B}\}$ is asymmetric, if $\mathrm{B}=-\mathrm{A}$. Recall that the pair is a set with two elements. If $u\in\mathbb{N}\backslash\{0\}$, then $u\mathrm{A}=\{i\in[|0;n-1|] \, : \, (\exists z\in \mathrm{A})(uz\equiv i(\mathtt{mod}\, n)\}$. It defines the binary relation on $[|0;n-1|]$ by $x\sim_q y$ if there is i in $\mathbb{N}$ such that $y\equiv q^ix(\mathtt{mod}\, n)$. Obviously, the binary relation $\sim_q$ is an equivalence relation on $[|0;n-1|]$. The cosets of $\sim_q$, are called q-cyclotomic cosets modulo n. Denote by $[|0;n-1|]_q$, a complete system of representatives of $\sim_q$. A subset Z of $[|0;n-1|]$ is a q-closed set modulo n, if $\mathrm{Z}=q\mathrm{Z}$. The smallest q-closed set modulo n, containing a subset Z of $[|0;n-1|]$ is $\bigcup_{i\in\mathbb{N}} q^i\mathrm{Z}$ and we will denote it by $\mathtt{C}_q(\mathrm{Z})$. In particular, the set of q-cyclotomic cosets modulo n which is $\left\{\mathtt{C}_q(\{z\}) \ : \ z\in[|0;n-1|]_q\right\}$, forms a partition of $[|0;n-1|]$. Since $\mathtt{C}_q(\{z\})=\{x\in[|0;n-1|] \ : \ x\sim_q z\}$ for any z in $[|0;n-1|]$. We will take $\mathtt{C}_q(\emptyset)=\emptyset$ by convention. Let j be a divisor of n, we will use the following notation

- $\phi(\,.\,)$ is the Euler totient function;
- $\mathtt{ord}_j(q)$ the multiplicative order of q modulo j;
- $\omega(n;q)$ the number of q-cyclotomic cosets modulo n;
- $\mathcal{N}_q=\left\{d\in\mathbb{N}\backslash\{0\} \, : \, (\exists i\in\mathbb{N}\backslash\{0\})(d \text{ divides } q^i+1)\right\}$;
- Λ_j the set of symmetric q-cyclotomic cosets modulo n of size $\mathtt{ord}_j(q)$;
- $\gamma(j;q):=|\Lambda_j|$;
- $\overline{\Lambda}_j$ the set of asymmetric pairs of q-cyclotomic cosets modulo n of size $\mathtt{ord}_j(q)$;
- $\beta(j;q):=|\overline{\Lambda}_j|$.

Let δ be a generator of the cyclic multiplicative subgroup $\Gamma(\mathtt{GR}(p^a,m))\backslash\{0\}$ of $(\mathtt{GR}(p^a,m))^\times$, where $m=\mathtt{ord}_n(q)$. The following result is straightforward from Hensel's Lemma [12], which guarantees the uniqueness of this monic basic-irreducible factorization of X^n-1, and $X^n-1=\prod_{z\in[|0;n-1|]_q} m_z$ where $m_z:=\prod_{a\in\mathtt{C}_q(\{z\})}(X-\delta^a)$. Obviously, for any z in $[|0;n-1|]_q$, the polynomial m_z is monic basic-irreducible over R.

Lemma 1. *The map*

$$\begin{array}{rcl}\Omega: \left\{\mathtt{C}_q(\mathrm{Z}) \, : \, \mathrm{Z}\subseteq[|0;n-1|]_q\right\} & \rightarrow & \{f\in \mathtt{GR}(p^a,r)[X] \, : \, f \textit{ is monic and } f|X^n-1\} \\ \mathrm{A} & \mapsto & \prod_{a\in\mathrm{A}}(X-\delta^a)\end{array} \tag{1}$$

where $\Omega(\emptyset)=1$, is bijective. Moreover, for any $z\in[|0;n-1|]$ and for all q-closure sets A *and* B *modulo n, we have*

1. $\Omega\left(\mathtt{C}_q(\{z\})\right)$ *is a monic basic-irreducible polynomial over* $\mathtt{GR}(p^a, r)$ *of degree* $\left|\mathtt{C}_q(\{z\})\right|$*;*
2. $\mathtt{lcm}(\Omega(\mathrm{A}), \Omega(\mathrm{B})) = \Omega(\mathrm{A} \cup \mathrm{B})$ *and* $\mathtt{gcd}(\Omega(\mathrm{A}), \Omega(\mathrm{B})) = \Omega(\mathrm{A} \cap \mathrm{B})$*;*
3. *if* $\mathrm{A} \cap \mathrm{B} = \emptyset$*, then* $\Omega(\mathrm{A} \cup \mathrm{B}) = \Omega(\mathrm{A})\,\Omega(\mathrm{B})$*.*

Proof. Since $\delta \in \Gamma(\mathtt{GR}(p^a, m))\backslash\{0\} \subset \mathtt{GR}(p^a, m)$ and $\mathtt{GR}(p^a, m)$ is a Galois extension of $\mathtt{GR}(p^a, r)$, it follows that for any q-cyclotomic cosets A modulo n, the monic polynomial $\prod\limits_{a \in \mathrm{A}} (X - \delta^a)$ is basic-irreducible over $\mathtt{GR}(p^a, r)$. Therefore, the correspondence Ω is well-defined, and by Hensel lemma, $X^n - 1$ admits a unique monic basic-irreducible factorization in $\mathtt{GR}(p^a, r)[X]$. Thus the existence and the uniqueness of this basic-irreducible factorization over $\mathtt{GR}(p^a, r)$, the map Ω is bijective. Items 2. and 3. are straightforward to prove. $\square$

Proposition 5. *[18, Subsection 2.2] Let j be a divisor of n. Then*

$$\gamma(j;q) = \begin{cases} \frac{\phi(j)}{ord_j(q)}, & \text{if } j \in \mathcal{N}_q; \\ 0, & \text{otherwise,} \end{cases} \quad \text{and } \beta(j;q) = \begin{cases} \frac{\phi(j)}{2ord_j(q)}, & \text{if } j \notin \mathcal{N}_q, \\ 0, & \text{otherwise.} \end{cases}$$

Moreover, $\omega(n;q) = \sum\limits_{\substack{i \,|\, n \\ i \in \mathcal{N}_q}} \gamma(i;q) + 2 \sum\limits_{\substack{j \,|\, n \\ j \notin \mathcal{N}_q}} \beta(j;q)$.

We will introduce the following notation

$$\mathcal{E}_n(q,s) = \mathcal{I}_n(q,s) \times \left(\mathcal{J}_n(q,s)\right)^2, \tag{2}$$

where $\mathcal{I}_n(q,s) = \prod\limits_{\substack{i \,|\, n \\ i \in \mathcal{N}_q}} \mathcal{E}_s^{\gamma(i;q)}$ and $\mathcal{J}_n(q,s) = \prod\limits_{\substack{j \,|\, n \\ j \notin \mathcal{N}_q}} \mathcal{E}_s^{\beta(j;q)}$, with

$$\mathcal{E}_s = \left\{ (x^{(0)}, x^{(1)}, \cdots, x^{(s-1)}) \in \{0;1\}^s \;:\; \sum_{a=0}^{s-1} x^{(a)} \in \{0;1\} \right\}. \tag{3}$$

Note that $\mathcal{E}_s = \{(0, \cdots, 0)\} \cup \left\{ \left(0, \cdots, 0, \underbrace{1}_{j\text{-i th position}}, 0, \cdots, 0 \right) \;:\; j \in \{1; \cdots; s\} \right\} \subseteq \{0;1\}^s$ and $|\mathcal{E}_s| = s + 1$.

The elements in $\mathcal{I}_n(q,s)$ are arrays of the form $(((u_{il}^{(a)})_{0 \le a < s})^\circ)$ where $(u_{il}^{(a)})_{0 \le a < s}$ are in $\mathcal{E}_s$ and the indices i and l satisfy $i \,|\, n, i \in \mathcal{N}_q$ and $1 \le l \le \gamma(i;q)$, i.e.,

$$(((u_{il}^{(a)})_{0 \le a < s})^\circ) = \left(\left((u_{il}^{(a)})_{0 \le a < s} \right)_{1 \le l \le \gamma(i;q)} \right)_{i \,|\, n, i \in \mathcal{N}_q} \in \mathcal{I}_n(q,s).$$

Similarly, $(((v_{jh}^{(a)})_{0\leq a<s})^{\bullet}) = \left(\left((v_{jh}^{(a)})_{0\leq a<s}\right)_{1\leq h\leq \beta(j;q)}\right)_{j\,|\,n, j\notin \mathcal{N}_q} \in \mathcal{J}_n(q,s)$. Note that if $s=1$, then $\mathcal{E}_1 = \{0;1\}$, and in this case, we write $((u_{il})^{\circ}) = (((u_{il}^{(a)})_{0\leq a<1})^{\circ})$ and $((v_{jh})^{\bullet}) = (((v_{jh}^{(a)})_{0\leq a<1})^{\bullet})$.

Let i and j be positive integers such that $i\,|\,n, i\in\mathcal{N}_q$, and $j\,|\,n, j\notin\mathcal{N}_q$. From now on,

$$\Lambda_i = \{G_{il} \,:\, 1\leq l\leq \gamma(i;q)\} \qquad \text{and} \qquad \overline{\Lambda_j} = \{\{F_{jh}, -F_{jh}\} \,:\, 1\leq h\leq \beta(j;q)\}.$$

Of course, all the polynomials in $\{\Omega(G_{il}) \,:\, 1\leq l\leq \gamma(i;q)\}$ are basic-irreducible in $R[X]$ of degree $\mathtt{ord}_i(q)$, and all the elements in $\{\{\Omega(F_{jh}), \Omega(-F_{jh})\} \,:\, 1\leq h\leq \beta(j;q)\}$ are pairs of monic basic-irreducible reciprocal polynomials (up to a unit) in $R[X]$ of the same degree $\mathtt{ord}_j(q)$. The basic-irreducible factorization of X^n-1 in $R[X]$ is given as

$$X^n - 1 = \prod_{\substack{i\,|\,n\\ i\in\mathcal{N}_q}} \left(\prod_{l=1}^{\gamma(i;q)} \Omega\left(G_{il}\right)\right) \prod_{\substack{j\,|\,n\\ j\notin\mathcal{N}_q}} \left(\prod_{h=1}^{\beta(j;q)} \Omega\left(F_{jh}\right)\Omega\left(-F_{jh}\right)\right). \tag{4}$$

Thus, for any monic factor of $X^n-1 \in R[X]$, there is a unique $(((u_{il})^{\circ}), ((v_{jh})^{\bullet}), ((w_{jh})^{\bullet})))$ in $\mathcal{E}_n(q,1)$ such that

$$f = \prod_{\substack{i\,|\,n\\ i\in\mathcal{N}_q}} \left(\prod_{l=1}^{\gamma(i;q)} \Omega\left(G_{il}\right)^{u_{il}}\right) \prod_{\substack{j\,|\,n\\ j\notin\mathcal{N}_q}} \left(\prod_{h=1}^{\beta(j;q)} \Omega\left(F_{jh}\right)^{v_{jh}}\Omega\left(-F_{jh}\right)^{w_{jh}}\right), \tag{5}$$

and conversely. Denote the right-hand side of Equation (5) by $\partial(((u_{il})^{\circ}), ((v_{jh})^{\bullet}), ((w_{jh})^{\bullet}))$. Note that $\partial(((1)^{\circ}), ((1)^{\bullet}), ((1)^{\bullet})) = X^n-1$ and $\partial(((0)^{\circ}), ((0)^{\bullet}), ((0)^{\bullet})) = 1$. If we are given $f_1 = \partial(((u_{il})^{\circ}), ((v_{jh})^{\bullet}), ((w_{jh})^{\bullet}))$ and $f_2 = \partial(((u'_{il})^{\circ}), ((v'_{jh})^{\bullet}), ((w'_{jh})^{\bullet}))$, we have that

$$\begin{aligned}
\mathtt{lcm}(f_1;f_2) &= \partial(((\max\{u_{il},u'_{il}\})^{\circ}), ((\max\{v_{jh},v'_{jh}\})^{\bullet}), ((\max\{w_{jh},w'_{jh}\})^{\bullet}));\\
\mathtt{gcd}(f_1;f_2) &= \partial(((\min\{u_{il},u'_{il}\})^{\circ}), ((\min\{v_{jh},v'_{jh}\})^{\bullet}), ((\min\{w_{jh},w'_{jh}\})^{\bullet})),
\end{aligned}$$

and if all $(u_{il}+u'_{il}, v_{jh}+v'_{jh}, w_{jh}+w'_{jh})$ are in $\{0;1\}^3$ then

$$f_1 f_2 = \partial(((u_{il}+u'_{il})^{\circ}), ((v_{jh}+v'_{jh})^{\bullet}), ((w_{jh}+w'_{jh})^{\bullet})). \tag{6}$$

A *cyclic code* C of length n over R is a linear code that is invariant under the transformation $\tau((c_0,c_1,\cdots,c_{n-1})) = (c_{n-1},c_0,\cdots,c_{n-2})$. If we denote by $\langle X^n-1\rangle$ the ideal of $R[X]$ generated by X^n-1, it is well-known that any cyclic code of length n over R can be represented as an ideal of the quotient ring $R[X]/\langle X^n-1\rangle$ via the R-module isomorphism $\overline{\Psi} : R^n \to R[X]/\langle X^n-1\rangle$, where $\overline{\Psi}(\mathbf{c}) = \Psi(\mathbf{c}) + \langle X^n-1\rangle$ and

$$\begin{array}{llll} \Psi : & R^n & \rightarrow & R[X] \\ & \mathbf{u} = (u_0, u_1, \cdots, u_{n-1}) & \mapsto & \mathbf{u}(X) = u_0 + u_1 X + \cdots + u_{n-1} X^{n-1}, \end{array} \tag{7}$$

which is an R-module homomorphism. We will slightly abuse notation, identifying vectors in R^n as polynomials in $R[X]$ of degree less than n, and vice versa when the context is clear. It is well-known that $R[X]/\langle X^n - 1\rangle$ is a principal ideal ring and C is a cyclic code of length n over R if and only if $\overline{\Psi}(C)$ is an ideal of $R[X]/\langle X^n - 1\rangle$, (see [4] and references therein). Thus, the generator polynomial of a cyclic code C of R^n, is the monic polynomial f in $R[X]$ such that $\overline{\Psi}(C) = \langle\, f(x)\,\rangle$, where $\langle\, f(x)\,\rangle$ is the ideal of $R[X]/\langle X^n - 1\rangle$ generated by f.

A cyclic code over R of length n, is uniserial if its cyclic subcodes over R are totally ordered by inclusion (see the definition of serial modules in [21]). A cyclic code over R of length n, is serial if it is a direct sum of uniserial cyclic codes over R of length n. Note that, over a finite chain ring R, any cyclic code of length n is serial, if and only if $\mathtt{gcd}(p, n) = 1$.

For a polynomial f of degree k its reciprocal polynomial $X^k f(X^{-1})$ will be denoted by f^* and if f is a factor of $X^n - 1$ we denote $\widehat{f} = \frac{X^n-1}{f}$. A polynomial f is *self-reciprocal* if $f = f^*$, otherwise f and f^* are called a *reciprocal polynomial pair*.

For any union A of q-cyclotomic cosets modulo n, $\Omega(\mathrm{A})^* = \Omega(-\mathrm{A})$ and $\widehat{\Omega(\mathrm{A})} = \Omega(-\mathrm{A})$. The $(s+1)$-tuple $(\mathrm{A}_0, \mathrm{A}_1, \cdots, \mathrm{A}_s)$ is called to be an ordered (q, s)-partition cyclotomic modulo n, if $\mathrm{A}_0, \mathrm{A}_1, \cdots, \mathrm{A}_s$ are unions of q-cyclotomic cosets modulo n whose $\{\mathrm{A}_t \,:\, \mathrm{A}_t \neq \emptyset, \;\; \text{for } 0 \leq t \leq s\}$ forms a partition of $[|0; n-1|]$. Denote by $\Re_n(q, s)$ the set of ordered (q, s)-partition cyclotomic modulo n. Note that

$$\Re_n(q,s) = \left\{ \left(\mathtt{C}_q(\lambda^{-1}(\{0\})), \mathtt{C}_q(\lambda^{-1}(\{1\})), \ldots, \mathtt{C}_q(\lambda^{-1}(\{s\}))\right) \,:\, \lambda \in [|0; s|]^{[|0;n-1|]_q} \right\}.$$

It follows that $|\Re_n(q, s)| = (s+1)^{\omega(n;q)}$. Let $\underline{\mathbf{A}} = (\mathrm{A}_0, \mathrm{A}_1, \cdots, \mathrm{A}_s)$ be in $\Re_n(q, s)$. For a positive integer u we denote by $u\underline{\mathbf{A}} = (u\mathrm{A}_0, u\mathrm{A}_1, \cdots, u\mathrm{A}_{s-1})$. Now, the $\mathrm{A}_0, \mathrm{A}_1, \cdots, \mathrm{A}_s$ are unions of q-cyclotomic cosets modulo n, therefore $p^\ell \mathrm{A}_t$ is also another union of q-cyclotomic cosets modulo n, for any t in $\{0; 1; \cdots; s-1\}$ and for any ℓ in $\{0; 1; \cdots; r-1\}$. Hence, $p^\ell \underline{\mathbf{A}} \in \Re_n(q, s)$ for any $0 \leq \ell < r$. From [4, Theorems 3.4, 3.5 and 3.8], we have the following result.

Lemma 2. *For any cyclic serial code C over R of length n, there is a unique $(s+1)$-tuple $(\mathrm{A}_0, \mathrm{A}_1, \cdots, \mathrm{A}_s)$ in $\Re_n(q, s)$ such that*

$$\overline{\Psi}(C) = \bigoplus_{t=0}^{s-1} \theta^t \left\langle\, \Omega(\overline{\mathrm{A}_t})\,\right\rangle = \left\langle \left\{ \theta^t \prod_{a=t+1}^{s} \Omega(\mathrm{A}_a) \,:\, 0 \leq t \leq s-1 \right\} \right\rangle. \tag{8}$$

Moreover, $\overline{\Psi}(C^{\perp_0}) = \bigoplus_{t=0}^{s-1} \theta^t \left\langle\, \Omega(-\overline{\mathrm{A}_{s-t}})\,\right\rangle$.

Let A be a union of q-cyclotomic cosets modulo n. From now on, we will consider the code

$$\mathcal{C}\,(\mathrm{A}) = \left\{ \mathbf{c} \in R^n \,:\, \Omega(\overline{\mathrm{A}}) \text{ divides } \Psi(\mathbf{c}) \right\}, \tag{9}$$

thus it is clear that $\overline{\Psi}(\mathcal{C}\,(\mathrm{A})) = \left\langle\, \Omega(\overline{\mathrm{A}})\, \right\rangle$.

Remark 1. Free cyclic serial codes over a finite chain ring have been studied in [5] using the cyclotomic cosets and the trace map. Note that $\mathcal{C}\,([|0; n-1|]) = \{\mathbf{0}\}$ and $\mathcal{C}\,(\emptyset) = R^n$. From Lemma 2, for any free cyclic serial code C of length n over R there exists a unique set A which is a union of q-cyclotomic cosets modulo n such that $C = \mathcal{C}\,(\mathrm{A})$. Moreover, $\mathcal{C}\,(\mathrm{A})^{\perp_0} = \mathcal{C}\left(-\overline{\mathrm{A}}\right)$, the generator polynomial of $\mathcal{C}\,(\mathrm{A})$ is $\Omega(\overline{\mathrm{A}})$, and $\mathtt{rank}_R(\mathcal{C}\,(\mathrm{A})) = |\mathrm{A}|$.

Proposition 6. *If* A *and* B *are unions of q-cyclotomic cosets modulo n, then*

1. $\mathrm{A} \subseteq \mathrm{B}$ *if and only if* $\mathcal{C}(\mathrm{A}) \subseteq \mathcal{C}(\mathrm{B})$*;*
2. $\mathcal{C}(\mathrm{A} \cap \mathrm{B}) = \mathcal{C}(\mathrm{A}) \cap \mathcal{C}(\mathrm{B})$*, and* $\mathcal{C}(\mathrm{A} \cup \mathrm{B}) = \mathcal{C}(\mathrm{A}) + \mathcal{C}(\mathrm{B})$*;*
3. $\sigma^\ell\left(\mathcal{C}\,(\mathrm{A})\right) = \mathcal{C}\left(p^\ell \mathrm{A}\right)$ *and* $\mathcal{C}\,(\mathrm{A})^{\perp_\ell} = \mathcal{C}\left(-p^\ell \overline{\mathrm{A}}\right)$*, for all* $0 \le \ell \le r-1$*.*

Proof. Item (1) follows from the definition of $\mathcal{C}(\mathrm{A})$ and $\mathcal{C}(\mathrm{B})$ and the fact that $\mathrm{A} \subseteq \mathrm{B}$ if and only if $\Omega(\overline{\mathrm{B}})$ divides $\Omega(\overline{\mathrm{A}})$. To prove (2), we note that since $\mathrm{A} \cap \mathrm{B} \subseteq \mathrm{A} \subseteq \mathrm{A} \cup \mathrm{B}$, and $\mathrm{A} \cap \mathrm{B} \subseteq \mathrm{B} \subseteq \mathrm{A} \cup \mathrm{B}$, from item (1), we have $\mathcal{C}(\mathrm{A} \cap \mathrm{B}) \subseteq \mathcal{C}(\mathrm{A}) \cap \mathcal{C}(\mathrm{B})$ and $\mathcal{C}(\mathrm{A}) + \mathcal{C}(\mathrm{B}) \subseteq \mathcal{C}(\mathrm{A} \cup \mathrm{B})$. Conversely, if $\mathbf{c} \in \mathcal{C}(\mathrm{A}) \cap \mathcal{C}(\mathrm{B})$ then $\Omega(\overline{\mathrm{A}})$ and $\Omega(\overline{\mathrm{B}})$ divide $\Psi(\mathbf{c})$. Thus $\mathtt{lcm}(\Omega(\overline{\mathrm{A}})\,, \Omega(\overline{\mathrm{B}}))$ divides $\Psi(\mathbf{c})$. Now, $\mathtt{lcm}(\Omega(\overline{\mathrm{A}})\,, \Omega(\overline{\mathrm{B}})) = \Omega(\overline{\mathrm{A}} \cup \overline{\mathrm{B}}) = \Omega(\overline{\mathrm{A} \cap \mathrm{B}})$, so we have $\mathcal{C}(\mathrm{A}) \cap \mathcal{C}(\mathrm{B}) \subseteq \mathcal{C}(\mathrm{A} \cap \mathrm{B})$. Since $\mathtt{gcd}(\Omega(\overline{\mathrm{A}})\,, \Omega(\overline{\mathrm{B}})) = \Omega(\overline{\mathrm{A}} \cap \overline{\mathrm{B}}) = \Omega(\overline{\mathrm{A} \cup \mathrm{B}})$, hence $\mathcal{C}(\mathrm{A}) + \mathcal{C}(\mathrm{B}) \supseteq \mathcal{C}(\mathrm{A} \cup \mathrm{B})$. To finish with the proof of the item (3), we have $\sigma^\ell\left(\mathcal{C}\,(\mathrm{A})\right) = \left\{\mathbf{c} \in R^n \,:\, \sigma^\ell\left(\Omega(\overline{\mathrm{A}})\right) \text{ divides } \Psi(\mathbf{c})\right\}$, thus $\sigma^\ell\left(\mathcal{C}\,(\mathrm{A})\right) = \mathcal{C}\left(p^\ell \mathrm{A}\right)$, since $\sigma^\ell\left(\Omega(\overline{\mathrm{A}})\right) = \Omega(p^\ell \overline{\mathrm{A}})$. Finally, for any $0 \le \ell \le r-1$ we have

$$\begin{aligned}
\mathcal{C}\,(\mathrm{A})^{\perp_\ell} &= \left(\sigma^\ell\left(\mathcal{C}\,(\mathrm{A})\right)\right)^{\perp_0}, \quad \text{from Proposition 2;} \\
&= \left(\mathcal{C}\left(p^\ell \mathrm{A}\right)\right)^{\perp_0}; \\
&= \mathcal{C}\left(-p^\ell \overline{\mathrm{A}}\right), \quad \text{from Remark 1.} \quad \square
\end{aligned}$$

Let $\underline{\mathbf{A}} = (\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s)$ and $\underline{\mathbf{B}} = (\mathrm{B}_0, \mathrm{B}_1, \ldots, \mathrm{B}_s)$ be elements in $\Re_n(q,s)$. We will define the following set in R^n

$$\mathbb{C}\,(\underline{\mathbf{A}}) = \bigoplus_{t=0}^{s-1} \theta^t \mathcal{C}(\mathrm{A}_t).$$

Taking into account the map Ψ in Equation (7) and from [4, Theorem 3.4], it follows that $\mathbb{C}\,(\underline{\mathbf{A}})$ is a direct sum of cyclic serial codes of length n over R. Therefore, $\mathbb{C}\,(\underline{\mathbf{A}})$ is a cyclic serial code of length n over R. The parameters of $\mathbb{C}(\underline{\mathbf{A}})$ are given by the entries in $(|\mathrm{A}_0|, |\mathrm{A}_1|, \cdots, |\mathrm{A}_s|)$ and from Lemma 2 it follows that for any cyclic serial code C over R of length n, there is a unique $\underline{\mathbf{A}}$ in $\Re_n(q,s)$ such that $C = \mathbb{C}(\underline{\mathbf{A}})$. Thus $\underline{\mathbf{A}}$ is called the defining multiset of $\mathbb{C}(\underline{\mathbf{A}})$.

Let us denote by

$$\underline{\mathbf{A}}^{\diamond} = (\mathrm{A}_s, \mathrm{A}_{s-1}, \ldots, \mathrm{A}_0), \quad \underline{\mathbf{A}} \sqcup \underline{\mathbf{B}} = (\mathrm{E}_0, \mathrm{E}_1, \ldots, \mathrm{E}_s)$$

where $\mathrm{E}_0 = \mathrm{A}_0 \cup \mathrm{B}_0$, and $\mathrm{E}_t = (\mathrm{A}_t \cup \mathrm{B}_t) \backslash \left(\bigcup_{i=0}^{t-1} (\mathrm{A}_i \cup \mathrm{B}_i) \right)$ for all $0 < t \leq s$. It is easy to see that $\underline{\mathbf{A}}^{\diamond}$ and $\underline{\mathbf{A}} \sqcup \underline{\mathbf{B}}$ are in $\Re_n(q,s)$. Moreover, $C^{\perp_\ell} = \mathbb{C}(-p^\ell \underline{\mathbf{A}}^{\diamond})$, and $\mathtt{dim}_q(C) = \sum_{t=0}^{s-1} (s-t)|\mathrm{A}_t|$. Note that if $\underline{\mathbf{A}} \sqcap \underline{\mathbf{B}} = (\underline{\mathbf{A}}^{\diamond} \sqcup \underline{\mathbf{B}}^{\diamond})^{\diamond} = (\mathrm{E}_0, \mathrm{E}_1, \cdots, \mathrm{E}_s)$, then $\mathrm{E}_s = \mathrm{A}_s \cup \mathrm{B}_s$ and $\mathrm{E}_{s-t} = (\mathrm{A}_{s-t} \cup \mathrm{B}_{s-t}) \setminus \left(\bigcup_{i=0}^{t-1} (\mathrm{A}_{s-i} \cup \mathrm{B}_{s-i}) \right)$, for all $0 < t \leq s$.

Proposition 7. *[5, Theorem 6] Let $\underline{\boldsymbol{A}} = (\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s)$ and $\underline{\boldsymbol{B}} = (\mathrm{B}_0, \mathrm{B}_1, \ldots, \mathrm{B}_s)$ in $\Re_n(q,s)$. Then $\mathbb{C}(\underline{\boldsymbol{A}}) + \mathbb{C}(\underline{\boldsymbol{B}}) = \mathbb{C}(\underline{\boldsymbol{A}} \sqcup \underline{\boldsymbol{B}})$ and $\mathbb{C}(\underline{\boldsymbol{A}}) \cap \mathbb{C}(\underline{\boldsymbol{B}}) = \mathbb{C}(\underline{\boldsymbol{A}} \sqcap \underline{\boldsymbol{B}})$.*

Corollary 2. *Let $\underline{\boldsymbol{A}} = (\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s)$ and $\underline{\boldsymbol{B}} = (\mathrm{B}_0, \mathrm{B}_1, \ldots, \mathrm{B}_s)$ in $\Re_n(q,s)$, and define $g_t = \prod_{a=t+1}^{s} \Omega(\mathrm{A}_a)$ and $h_t = \prod_{a=t+1}^{s} \Omega(\mathrm{B}_a)$, for all $0 \leq t < s$. Then*

1. $\overline{\Psi}(\mathbb{C}(\underline{\boldsymbol{A}})) = \langle \{\theta^t g_t(x) \, : \, 0 \leq t < s\} \rangle$, *and* $\overline{\Psi}(\mathbb{C}(\underline{\boldsymbol{B}})) = \langle \{\theta^t h_t(x) \, : \, 0 \leq t < s\} \rangle$;
2. $\overline{\Psi}(\mathbb{C}(\underline{\boldsymbol{A}} \sqcap \underline{\boldsymbol{B}})) = \langle \{\theta^t \, \mathtt{lcm}(g_t, h_t) \, : \, 0 \leq t < s\} \rangle$.

Proof. We have $\underline{\mathrm{A}} \sqcap \underline{\mathrm{B}} = (\mathrm{E}_0, \mathrm{E}_1, \ldots, \mathrm{E}_s)$, where $\mathrm{E}_s = \mathrm{A}_s \cup \mathrm{B}_s$ and $\mathrm{E}_{s-t} = (\mathrm{A}_{s-t} \cup \mathrm{B}_{s-t}) \setminus \left(\bigcup_{i=0}^{t-1} (\mathrm{A}_{s-i} \cup \mathrm{B}_{s-i}) \right)$, for all $0 < t \leq s$. From Lemma 2 it follows that $\overline{\Psi}(\mathbb{C}(\underline{\mathbf{A}})) = \langle \{\theta^t g_t(x) \, : \, 0 \leq t < s\} \rangle$, and $\overline{\Psi}(\mathbb{C}(\underline{\mathbf{B}})) = \langle \{\theta^t h_t(x) \, : \, 0 \leq t < s\} \rangle$. Since $\overline{\Psi}(\mathbb{C}(\underline{\mathbf{A}} \sqcap \underline{\mathbf{B}})) = \overline{\Psi}(\mathbb{C}(\underline{\mathbf{A}})) \cap \overline{\Psi}(\mathbb{C}(\underline{\mathbf{B}}))$, using again Lemma 2 and Proposition 7 it follows that

$$\overline{\Psi}(\mathbb{C}(\underline{\mathbf{A}} \sqcap \underline{\mathbf{B}})) = \left\langle f_0(x), \theta f_1(x), \ldots, \theta^{s-1} f_{s-1}(x) \right\rangle,$$

where $f_t = \prod_{a=t+1}^{s} \Omega(\mathrm{E}_a)$. Thus for all $0 \leq t < s$, $f_t = \Omega\left(\bigcup_{a=t+1}^{s} \mathrm{E}_a \right)$ and $\bigcup_{a=t+1}^{s} \mathrm{E}_a = \bigcup_{a=t+1}^{s} (\mathrm{A}_{s-t-1} \cup \mathrm{B}_{s-t-1})$. Then $f_t = \Omega\left(\bigcup_{a=t+1}^{s} (\mathrm{A}_{s-t-1} \cup \mathrm{B}_{s-t-1}) \right) = \mathtt{lcm}(g_t, h_t)$. $\square$

Theorem 1. *Let $\underline{\boldsymbol{A}}$ in $\Re_n(q,s)$. Then*

$$\mathcal{H}_\ell(\mathbb{C}(\underline{\boldsymbol{A}})) = \mathbb{C}\left(\underline{\boldsymbol{A}} \sqcap -p^\ell \underline{\boldsymbol{A}}^{\diamond} \right). \tag{10}$$

Proof. Let $\underline{\mathbf{A}}$ in $\Re_n(q,s)$ and $0 \le \ell < r$. We have

$$\begin{aligned}\mathcal{H}_\ell(\mathbb{C}(\underline{\mathbf{A}})) &= \mathbb{C}(\underline{\mathbf{A}}) \cap \mathbb{C}(\underline{\mathbf{A}})^{\perp_\ell}, \text{ from Definition 1 ;}\\ &= \mathbb{C}(\underline{\mathbf{A}}) \cap \mathbb{C}(-p^\ell \underline{\mathbf{A}}^\diamond), \text{ since } \mathbb{C}(\underline{\mathbf{A}})^{\perp_\ell} = \mathbb{C}(-p^\ell \underline{\mathbf{A}}^\diamond);\\ &= \mathbb{C}\left(\underline{\mathbf{A}} \sqcap -p^\ell \underline{\mathbf{A}}^\diamond\right), \text{ from Proposition 7. } \square\end{aligned}$$

Example 3.1. Let $R = \mathbb{Z}_{2^a}[\theta]$ with $1 \le a \le 2$ be the finite chain ring of parameters $(2,a,1,e,2)$. Consider the 2-cyclotomic cosets modulo 7 given by $\mathtt{C}_2(\{0\}) = \{0\}, \mathtt{C}_2(\{1\}) = \{1;2;4\}$, and $\mathtt{C}_2(\{3\}) = \{3;5;6\}$. Note that $\left\{\mathtt{C}_2(\{1\}), \mathtt{C}_2(\{3\})\right\}$ is an asymmetric set, and $\mathtt{C}_2(\{0\})$ is a symmetric set. Consider the cyclic serial code over R of length 7 with defining multiset $\underline{\mathbf{A}} = \left(\mathtt{C}_2(\{0\}), \mathtt{C}_2(\{3\}), \mathtt{C}_2(\{1\})\right)$.
Then $-\underline{\mathbf{A}}^\diamond = \left(\mathtt{C}_2(\{3\}), \mathtt{C}_2(\{1\}), \mathtt{C}_2(\{0\})\right)$, and $\mathbb{C}\left(\underline{\mathbf{A}}\right) = \mathcal{C}\left(\mathtt{C}_2(\{0\})\right) \oplus \theta\mathcal{C}\left(\mathtt{C}_2(\{3\})\right)$. Thus $\mathbb{C}\left(\underline{\mathbf{A}}\right)^{\perp_0} = \mathbb{C}\left(-\underline{\mathbf{A}}^\diamond\right) = \mathcal{C}\left(\mathtt{C}_2(\{3\})\right) \oplus \theta\mathcal{C}\left(\mathtt{C}_2(\{1\})\right)$. Finally, $\underline{\mathbf{A}} \sqcap -\underline{\mathbf{A}}^\diamond = (\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2)$ where $\mathrm{F}_0 = \emptyset, \mathrm{F}_1 = \mathtt{C}_2(\{3\})$, and $\mathrm{F}_2 = \mathtt{C}_2(\{0;1\})$. Therefore $\mathcal{H}_0(\mathbb{C}\left(\underline{\mathbf{A}}\right)) = \mathbb{C}\left(\underline{\mathbf{A}} \sqcap -\underline{\mathbf{A}}^\diamond\right) = \mathbb{C}(\emptyset, \mathtt{C}_2(\{3\}), \mathtt{C}_2(\{0;1\})) = \theta\mathcal{C}\left(\mathtt{C}_2(\{3\})\right)$.

3.1. Euclidean hulls

From now on, $\ell = 0$. The following result provides us a way of checking whether a given cyclic serial code D is the Euclidean hull of a cyclic code C or not. Of course, if $\mathcal{H}_0(C) = D$, then D is a serial cyclic code if, and only if C is also a serial code. In the sequel, for each $\underline{\mathbf{X}} = (\mathrm{X}_0, \mathrm{X}_1, \cdots, \mathrm{X}_s) \in \Re_n(q,s)$, we will denote $\Omega(\mathrm{X}_a) = \partial\left(((x_{il}^{(a)})^\circ), ((y_{jh}^{(a)})^\bullet), ((z_{jh}^{(a)})^\bullet)\right)$, for a in $\{0;1;\cdots;s\}$. Thus $\Omega(-\mathrm{X}_a) = \partial\left(((x_{il}^{(a)})^\circ), ((z_{jh}^{(a)})^\bullet), ((y_{jh}^{(a)})^\bullet)\right)$, and from Equation (6), we have for $0 \le t \le s-1$,

$$\prod_{a=t+1}^{s} \Omega(\mathrm{X}_a) = \partial\left(\left(\left(\sum_{a=t+1}^{s} x_{il}^{(a)}\right)^\circ\right), \left(\left(\sum_{a=t+1}^{s} y_{jh}^{(a)}\right)^\bullet\right), \left(\left(\sum_{a=t+1}^{s} z_{jh}^{(a)}\right)^\bullet\right)\right).$$

Since $\partial(((1)^\circ), ((1)^\bullet), ((1))^\bullet) = X^n - 1 = g_0 \cdot \partial(((x_{il}^{(0)})^\circ), ((y_{jh}^{(0)})^\bullet), ((z_{jh}^{(0)})^\bullet))$, it follows that

$$\sum_{a=0}^{s} x_{il}^{(a)} = \sum_{a=0}^{s} y_{jh}^{(a)} = \sum_{a=0}^{s} z_{jh}^{(a)} = 1.$$

From Eqs. (5) and (8), there exists a unique

$$\left(((x_{il}^{(a)})_{0\le a<s})^\circ), (((y_{jh}^{(a)})_{0\le a<s})^\bullet), (((z_{jh}^{(a)})_{0\le a<s})^\bullet)\right)$$

in $\mathcal{E}_n(q,s)$ such that

$$\overline{\Psi}(\mathbb{C}(\underline{\mathbf{X}})) = \left\langle \left\{ \theta^t \cdot \partial \left(\left(\left(\sum_{a=t+1}^{s} x_{il}^{(a)} \right)^{\circ} \right), \left(\left(\sum_{a=t+1}^{s} y_{jh}^{(a)} \right)^{\bullet} \right), \left(\left(\sum_{a=t+1}^{s} z_{jh}^{(a)} \right)^{\bullet} \right) \right) : 0 \leq t \leq s-1 \right\} \right\rangle .$$

From Eqs. (4), (5), and (8), the following lemma follows.

Lemma 3. *There is a bijection between the set $\mathcal{C}(n; R)$ of cyclic serial codes of length n over R and the set $\mathcal{E}_n(q, s)$.*

When $\ell = 0$, and with the triple-sequence of a cyclic serial code, by comparing the two sides of Equation(10) in Theorem 1, the following result is obtained.

Corollary 3. *Let*

$$\left((((x_{il}^{(a)})_{0\leq a<2})^{\circ}), (((y_{jh}^{(a)})_{0\leq a<2})^{\bullet}), (((z_{jh}^{(a)})_{0\leq a<2})^{\bullet}) \right) \text{ and}$$
$$\left((((u_{il}^{(a)})_{0\leq a<2})^{\circ}), (((v_{jh}^{(a)})_{0\leq a<2})^{\bullet}), (((w_{jh}^{(a)})_{0\leq a<2})^{\bullet}) \right)$$

in $\mathcal{E}_n(q, s)$ such that

$$\overline{\Psi}(C) = \left\langle \left\{ \theta^t \cdot \partial \left(\left(\left(\sum_{a=t+1}^{s} x_{il}^{(a)} \right)^{\circ} \right), \left(\left(\sum_{a=t+1}^{s} y_{jh}^{(a)} \right)^{\bullet} \right), \left(\left(\sum_{a=t+1}^{s} z_{jh}^{(a)} \right)^{\bullet} \right) \right) : 0 \leq t \leq s-1 \right\} \right\rangle ,$$

and

$$\overline{\Psi}(D) = \left\langle \left\{ \theta^t \cdot \partial \left(\left(\left(\sum_{a=t+1}^{s} u_{il}^{(a)} \right)^{\circ} \right), \left(\left(\sum_{a=t+1}^{s} v_{jh}^{(a)} \right)^{\circ} \right), \left(\left(\sum_{a=t+1}^{s} w_{jh}^{(a)} \right)^{\circ} \right) \right) : 0 \leq t \leq s-1 \right\} \right\rangle .$$

Then $\mathcal{H}_0(C) = D$ if, and only if for all $0 \leq t \leq s-1$,

$$\begin{cases} \sum_{a=t+1}^{s} u_{il}^{(a)} = \max \left\{ \sum_{a=t+1}^{s} x_{il}^{(a)}; \sum_{a=t+1}^{s} x_{il}^{(s-a)} \right\}; \\ \sum_{a=t+1}^{s} v_{jh}^{(a)} = \max \left\{ \sum_{a=t+1}^{s} y_{jh}^{(a)}; \sum_{a=t+1}^{s} z_{jh}^{(s-a)} \right\}; \\ \sum_{a=t+1}^{s} w_{jh}^{(a)} = \max \left\{ \sum_{a=t+1}^{s} z_{jh}^{(a)}; \sum_{a=t+1}^{s} y_{jh}^{(s-a)} \right\}. \end{cases} \tag{11}$$

In such a case, for all $0 \leq t \leq s-1$, *if* $2t \leq s-1$, *then* $\sum\limits_{a=t+1}^{s} u_{il}^{(a)} = \max\left\{\sum\limits_{a=t+1}^{s} x_{il}^{(a)}; \sum\limits_{a=t+1}^{s} x_{il}^{(s-a)}\right\} = 1$, *and* $\left(\sum\limits_{a=t+1}^{s} v_{jh}^{(a)}; \sum\limits_{a=t+1}^{s} w_{jh}^{(a)}\right) \in \{(1;0),(0;1),(1;1)\}$, *since* $\sum\limits_{a=0}^{s} x_{il}^{(a)} = 1$.

From Corollary 3, we recover the characterization of LCD cyclic codes and of self-orthogonal cyclic codes in [10, Theorem 3.4, and Corollaries 3.5 and 3.6] and we naturally extend it to finite chain rings of nilpotency index 2. The following remark provides this generalization.

Remark 2. Let

$$\left((((x_{il}^{(a)})_{0\leq a<2})^{\circ}),(((y_{jh}^{(a)})_{0\leq a<2})^{\bullet}),(((z_{jh}^{(a)})_{0\leq a<2})^{\bullet})\right) \text{ and}$$
$$\left((((u_{il}^{(a)})_{0\leq a<2})^{\circ}),(((v_{jh}^{(a)})_{0\leq a<2})^{\bullet}),(((w_{jh}^{(a)})_{0\leq a<2})^{\bullet})\right)$$

in $\mathcal{E}_n(q,2)$ such that

$$\begin{aligned}\overline{\Psi}(C) = \Big\langle \Big\{ &\partial\left(((x_{il}^{(1)}+x_{il}^{(2)})^{\circ}),((y_{jh}^{(1)}+y_{jh}^{(2)})^{\bullet}),((z_{jh}^{(1)}+z_{jh}^{(2)})^{\bullet})\right),\\ &\theta\cdot\partial\left(((x_{il}^{(2)})^{\circ}),((y_{jh}^{(2)})^{\bullet}),((z_{jh}^{(2)})^{\bullet})\right)\Big\}\Big\rangle,\end{aligned}$$

and

$$\begin{aligned}\overline{\Psi}(D) = \Big\langle \Big\{ &\partial\left(((u_{il}^{(1)}+u_{il}^{(2)})^{\circ}),((v_{jh}^{(1)}+v_{jh}^{(2)})^{\bullet}),((w_{jh}^{(1)})^{\bullet}+w_{jh}^{(2)})^{\bullet})\right),\\ &\theta\cdot\partial\left(((u_{il}^{(2)})^{\circ}),((v_{jh}^{(2)})^{\bullet}),((w_{jh}^{(2)})^{\bullet})\right)\Big\}\Big\rangle.\end{aligned}$$

Then $\mathcal{H}_0(C) = D$ if, and only if $(x_{il}^{(1)};x_{il}^{(2)}) \in \begin{cases}\{(0;1)\}, & \text{if } u_{il}^{(2)}=0;\\ \{(0;0),(1;0)\}, & \text{if } u_{il}^{(2)}=1,\end{cases}$ and

$(y_{jh}^{(1)};y_{jh}^{(2)};z_{jh}^{(1)};z_{jh}^{(2)}) \in$

$$\begin{cases}\{(0;0;0;0),(1;0;1;0)\}, & \text{if } (u_{il}^{(1)}+u_{il}^{(2)};v_{jh}^{(1)}+v_{jh}^{(2)};w_{jh}^{(1)}+w_{jh}^{(2)};v_{jh}^{(2)};w_{jh}^{(2)})=(1;1;1;1;1);\\ \{(0;1;1;0),(1;0;1;1)\}, & \text{if } (u_{il}^{(1)}+u_{il}^{(2)};v_{jh}^{(1)}+v_{jh}^{(2)};w_{jh}^{(1)}+w_{jh}^{(2)};v_{jh}^{(2)};w_{jh}^{(2)})=(1;1;1;0;1);\\ \{(0;1;0;0),(1;0;0;1)\}, & \text{if } (u_{il}^{(1)}+u_{il}^{(2)};v_{jh}^{(1)}+v_{jh}^{(2)};w_{jh}^{(1)}+w_{jh}^{(2)};v_{jh}^{(2)};w_{jh}^{(2)})=(1;1;1;1;0);\\ \{(1;0;0;0)\}, & \text{if } (u_{il}^{(1)}+u_{il}^{(2)};v_{jh}^{(1)}+v_{jh}^{(2)};w_{jh}^{(1)}+w_{jh}^{(2)};v_{jh}^{(2)};w_{jh}^{(2)})=(1;1;0;1;0);\\ \{(0;0;1;0)\}, & \text{if } (u_{il}^{(1)}+u_{il}^{(2)};v_{jh}^{(1)}+v_{jh}^{(2)};w_{jh}^{(1)}+w_{jh}^{(2)};v_{jh}^{(2)};w_{jh}^{(2)})=(1;0;1;0;1);\\ \{(0;1;0;1)\}, & \text{if } (u_{il}^{(1)}+u_{il}^{(2)};v_{jh}^{(1)}+v_{jh}^{(2)};w_{jh}^{(1)}+w_{jh}^{(2)};v_{jh}^{(2)};w_{jh}^{(2)})=(1;1;1;0;0),\end{cases}$$

for all i,l,j,h. Moreover,

1. C is LCD if, and only if $x_{il}^{(2)} = x_{il}^{(1)}, y_{jh}^{(2)} = y_{jh}^{(1)}, z_{jh}^{(2)} = z_{jh}^{(1)}$ and $(x_{il}^{(2)}; y_{jh}^{(2)}; z_{jh}^{(2)}) \in \{(0;0;0), (0;1;1), (1;0;0), (1;1;1)\}$, for all i, l, j, h.
2. C is self-orthogonal if, and only if $(x_{il}^{(2)}; x_{il}^{(1)}) \in \{(0;1), (1;0)\}$ and

$$(y_{jh}^{(2)}; y_{jh}^{(1)}; z_{jh}^{(2)}; z_{jh}^{(1)}) \in \{(1;0;1;0), (0;1;1;0), (1;0;0;1), (1;0;0;0), (0;0;1;0), (0;1;0;1)\},$$

for all i, l, j, h.

Note that Corollary 3 is insufficient to characterize the nontrivial self-dual cyclic codes over R when s is even (see [4, Theorem 4.4]).

4. The q-dimensions of Euclidean hulls of cyclic serial codes

In this section, C is a cyclic serial code of length n over R with triple-sequence

$$\left((((x_{il}^{(a)})_{0\leq a<s})^{\circ}), (((y_{jh}^{(a)})_{0\leq a<s})^{\bullet}), (((z_{jh}^{(a)})_{0\leq a<s})^{\bullet})\right)$$

in $\mathcal{E}_n(q,s)$. Then

$$\overline{\Psi}(C) = \left\langle \left\{ \theta^t \cdot \partial \left(\left(\left(\sum_{a=t+1}^{s} x_{il}^{(a)} \right)^{\circ} \right), \left(\left(\sum_{a=t+1}^{s} y_{jh}^{(a)} \right)^{\bullet} \right), \left(\left(\sum_{a=t+1}^{s} z_{jh}^{(a)} \right)^{\bullet} \right) \right) : 0 \leq t \leq s-1 \right\} \right\rangle.$$

From Corollary 3,

$$\overline{\Psi}\left(\mathcal{H}_0(C)\right) = \left\langle \left\{ \theta^t \cdot \partial \left(\left(\left(\sum_{a=t+1}^{s} u_{il}^{(a)} \right)^{\circ} \right), \left(\left(\sum_{a=t+1}^{s} v_{jh}^{(a)} \right)^{\circ} \right), \left(\left(\sum_{a=t+1}^{s} w_{jh}^{(a)} \right)^{\circ} \right) \right) : 0 \leq t \leq s-1 \right\} \right\rangle,$$

where

$$\begin{cases} \sum_{a=t+1}^{s} u_{il}^{(a)} = 1 - \min\left\{ \sum_{a=0}^{t} x_{il}^{(a)}; 1 - \sum_{a=0}^{s-t-1} x_{il}^{(a)} \right\}; \\ \sum_{a=t+1}^{s} v_{jh}^{(a)} = 1 - \min\left\{ \sum_{a=0}^{t} y_{jh}^{(a)}; 1 - \sum_{a=0}^{s-t-1} z_{jh}^{(a)} \right\}; \\ \sum_{a=t+1}^{s} w_{jh}^{(a)} = 1 - \min\left\{ \sum_{a=0}^{t} z_{jh}^{(a)}; 1 - \sum_{a=0}^{s-t-1} y_{jh}^{(a)} \right\}, \end{cases}$$

for all $0 \leq t \leq s-1$. The following notations are important for the sequel of this paper. For all $0 \leq t \leq s-1$, $1 \leq l \leq \gamma(i;q)$ and $1 \leq h \leq \beta(j;q)$, denote by:

$$\varepsilon_{jh}^{(t)} = \sum_{a=t+1}^{s} (v_{jh}^{(a)} + w_{jh}^{(a)}). \tag{12}$$

Note that $\varepsilon_{jh}^{(-1)} = 2$. Let us consider now

$$\triangle_{il} = \sum_{t=0}^{s-1} (s-t) u_{il}^{(t)}, \text{ and } \blacktriangle_{jh} = \sum_{t=0}^{s-1} (s-t)(\varepsilon_{il}^{(t-1)} - \varepsilon_{il}^{(t)}). \tag{13}$$

Obviously, $\triangle_{il} = \sum\limits_{t=0}^{s-1} \triangle_{il}^{(t)}$, where $\triangle_{il}^{(t)} = \min\left\{\sum\limits_{a=0}^{t} x_{il}^{(a)}; 1 - \sum\limits_{a=0}^{s-t-1} x_{il}^{(a)}\right\}$, and $\blacktriangle_{jh} = \sum\limits_{t=0}^{s-1} \blacktriangle_{jh}^{(t)}$, where

$$\blacktriangle_{jh}^{(t)} = \min\left\{\sum_{a=0}^{t} y_{jh}^{(a)}; 1 - \sum_{a=0}^{s-t-1} z_{jh}^{(a)}\right\} + \min\left\{\sum_{a=0}^{t} z_{jh}^{(a)}; 1 - \sum_{a=0}^{s-t-1} y_{jh}^{(a)}\right\}.$$

Thus, we set $\triangle_i := \sum\limits_{l=1}^{\gamma(i;q)} \triangle_{il}$, $\varepsilon_j^{(t)} := \sum\limits_{h=1}^{\beta(j;q)} \varepsilon_{jh}^{(t)}$ and $\blacktriangle_j := \sum\limits_{h=1}^{\beta(j;q)} \blacktriangle_{jh}$.

Remark 3. Let $0 \leq t \leq s-1$.

1. $\triangle_{il}^{(t)} \in \{0;1\}$ and $\blacktriangle_{jh}^{(t)} \in \{0;1;2\}$.
2. If $0 < t < s$, then $\triangle_{il}^{(t-1)} \leq \triangle_{il}^{(t)}$ and $\blacktriangle_{jh}^{(t-1)} \leq \blacktriangle_{jh}^{(t)}$.
3. If $2t < s$, then $\triangle_{il}^{(t)} = 0$ and $\blacktriangle_{jh}^{(t)} \leq 1$.

Lemma 4. *Let j be a divisor of n such that $j \notin \mathcal{N}_q$. Then*

$$\begin{cases} 0 \leq \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)} \leq \beta(j;q) - (\varepsilon_j^{(t-2)} - \varepsilon_j^{(t-1)}), & \text{if } t < \left\lceil \frac{s}{2} \right\rceil; \\ 0 \leq \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)} \leq 2\left(\beta(j;q) - (\varepsilon_j^{(t-2)} - \varepsilon_j^{(t-1)})\right), & \text{if } t \geq \left\lceil \frac{s}{2} \right\rceil. \end{cases}$$

Proof. Let $0 \leq t \leq s-1$ and $\blacktriangle_j^{(t)} = \sum\limits_{h=1}^{\beta(j;q)} \blacktriangle_{jh}^{(t)}$. We have $\varepsilon_{jh}^{(t)} = 2 - \blacktriangle_{jh}^{(t)}$. From Remark 3, two cases are considered. Let $\varpi_j^{(t-1)} := |\{h \in \mathbb{N} : 1 \leq h \leq \beta(j;q) \text{ and } \varepsilon_{jh}^{(t-1)} = \varepsilon_{jh}^{(t)} = 1\}|$. Then there is a permutation τ in $\mathbb{S}_{\beta(j;q)}$ such that $\varepsilon_{jh}^{(t-1)} = \varepsilon_{jh}^{(t)} = 1$, for all $h \in \{\tau(1), \cdots, \tau(\varpi_j^{(t-1)})\}$. Obviously, $\varepsilon_j^{(t-2)} \leq 2\beta(j;q)$. For that $\varepsilon_j^{(t-2)} - \varepsilon_j^{(t-1)} \leq \varpi_j^{(t-1)}$.

Case 1: $t < \lceil \frac{s}{2} \rceil$**.** We have $\varepsilon_{jh}^{(t)} \in \{1;2\}$, and $\begin{cases} \varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)} \in \{0;1\}, & \text{if } \varepsilon_{jh}^{(t-1)} = 2; \\ \varepsilon_{jh}^{(t)} = \varepsilon^{(t-1)}, & \text{if } \varepsilon_{jh}^{(t-1)} = 1. \end{cases}$

Thus

$$\begin{aligned} \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)} &= \left(\sum_{h \in \{\tau(1), \cdots, \tau(\varpi_j^{(t-1)})\}} (\varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)}) \right) \\ &\quad + \left(\sum_{h \in \{\tau(\varpi_j^{(t-1)}+1), \cdots, \tau(\beta(j;q))\}} (\varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)}) \right); \\ &= 0 + \left(\sum_{h \in \{\tau(\varpi_j^{(t-1)}+1), \cdots, \tau(\beta(j;q))\}} (\varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)}) \right), \\ &\qquad \text{since } 0 \leq \varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)} \leq 1. \end{aligned}$$

Hence $0 \leq \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)} \leq \beta(j;q) - \varpi_j^{(t-1)} \leq \beta(j;q) - (\varepsilon_j^{(t-2)} - \varepsilon_j^{(t-1)})$.

Case 2: $t \geq \lceil \frac{s}{2} \rceil$**.** We have $\begin{cases} \varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)} \in \{0;1;2\}, & \text{if } \varepsilon_{jh}^{(t-1)} \in \{1;2\}; \\ \varepsilon_{jh}^{(t)} = \varepsilon_{jh}^{(t-1)}, & \text{if } \varepsilon_{jh}^{(t-1)} = 0. \end{cases}$ Thus

$$\begin{aligned} \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)} &= \left(\sum_{h \in \{\tau(1), \cdots, \tau(\varpi_j^{(t-1)})\}} (\varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)}) \right) \\ &\quad + \left(\sum_{h \in \{\tau(\varpi_j^{(t-1)}+1), \cdots, \tau(\beta(j;q))\}} (\varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)}) \right); \\ &= 0 + \left(\sum_{h \in \{\tau(\varpi_j^{(t-1)}+1), \cdots, \tau(\beta(j;q))\}} (\varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)}) \right), \\ &\qquad \text{since } 0 \leq \varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)} \leq 2. \end{aligned}$$

Therefore $0 \leq \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)} \leq 2(\beta(j;q) - \varpi_j^{(t-1)}) \leq 2\left(\beta(j;q) - (\varepsilon_j^{(t-2)} - \varepsilon_j^{(t-1)})\right)$. $\square$

Theorem 2. *The parameters of the Euclidean hull of a cyclic serial code over R of length n are given by $(k_0, k_1, \cdots, k_{s-1})$ where $2k_0 + k_1 + \cdots + k_{s-1} \leq n$,*

$$k_t = \sum_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \boldsymbol{ord}_i(q) \cdot u_i^{(t)} + \sum_{\substack{j \mid n \\ i \notin \mathcal{N}_q}} \boldsymbol{ord}_j(q) \cdot \nu_j^{(t)},$$

with

$$\begin{cases} u_i^{(t)} = 0, & \textit{if } t < \left\lceil \frac{s}{2} \right\rceil; \\ 0 \le u_i^{(t)} \le \gamma(i;q), & \textit{if } t \ge \left\lceil \frac{s}{2} \right\rceil \end{cases}, \ \textit{and}$$

$$\begin{cases} \varepsilon_j^{(t)} = 0, & \textit{if } n \in \mathcal{N}_q; \\ 0 \le \nu_j^{(t)} \le \beta(j;q) - \nu_j^{(t-1)}, & \textit{if } n \notin \mathcal{N}_q, \textit{ and } t < \left\lceil \frac{s}{2} \right\rceil; \\ 0 \le \nu_j^{(t)} \le 2(\beta(j;q) - \nu_j^{(t-1)}), & \textit{if } n \notin \mathcal{N}_q, \textit{ and } t \ge \left\lceil \frac{s}{2} \right\rceil. \end{cases}$$

Moreover $\nu_j^{(-1)} = 0$.

Proof. Let $(k_0, k_1, \cdots, k_{s-1})$ be the parameters of $\mathcal{H}_0(C)$. When $\mathcal{H}_0(C) = C$, we have $2k_0 + k_1 + \cdots + k_{s-1} \le n$. Then for all $0 \le t \le s-1$,

$$\begin{aligned} k_t = {} & \texttt{deg}\left(\partial\left(\left(\left(\sum_{a=t}^{s} u_{il}^{(a)}\right)^{\circ}\right), \left(\left(\sum_{a=t}^{s} v_{ij}^{(a)}\right)^{\circ}\right), \left(\left(\sum_{a=t}^{s} w_{jh}^{(a)}\right)^{\circ}\right)\right)\right) \\ & -\texttt{deg}\left(\partial\left(\left(\left(\sum_{a=t+1}^{s} u_{il}^{(a)}\right)^{\circ}\right), \left(\left(\sum_{a=t+1}^{s} v_{jh}^{(a)}\right)^{\circ}\right), \left(\left(\sum_{a=t+1}^{s} w_{jh}^{(a)}\right)^{\circ}\right)\right)\right); \\ = {} & \sum_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \texttt{ord}_i(q) \cdot u_i^{(t)} + \sum_{\substack{j \mid n \\ j \notin \mathcal{N}_q}} \texttt{ord}_j(q) \cdot (\varepsilon_j^{(t-1)} - \varepsilon_j^{(t)}), \qquad \text{where } u_i^{(t)} = \sum_{l=1}^{\gamma(i;q)} u_{il}^{(t)}. \end{aligned}$$

Since $\begin{cases} u_i^{(t)} = 0, & \text{if } t < \left\lceil \frac{s}{2} \right\rceil; \\ 0 \le u_i^{(t)} \le \gamma(i;q), & \text{if } t \ge \left\lceil \frac{s}{2} \right\rceil \end{cases}$, it follows that $\begin{cases} u_i^{(t)} = 0, & \text{if } 2t < s; \\ 0 \le u_i^{(t)} \le \gamma(i;q), & \text{if } s \le 2t. \end{cases}$ On the other hand, one notes that if $n \in \mathcal{N}_q$, then any positive divisor of n is in then $\mathcal{N}_q$. By Lemma 4, we obtain

$$\begin{cases} \varepsilon_j^{(t)} = 0, & \text{if } n \in \mathcal{N}_q; \\ 0 \le \nu_j^{(t)} \le \beta(j;q) - \nu_j^{(t-1)}, & \text{if } n \notin \mathcal{N}_q, \text{ and } t < \left\lceil \frac{s}{2} \right\rceil; \\ 0 \le \nu_j^{(t)} \le 2(\beta(j;q) - \nu_j^{(t-1)}), & \text{if } n \notin \mathcal{N}_q, \text{ and } t \ge \left\lceil \frac{s}{2} \right\rceil, \end{cases}$$

where $\nu_j^{(t)} = \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)}$. Obviously $\nu_j^{(-1)} = \varepsilon_j^{(-2)} - \varepsilon_j^{(-1)} = 0$. $\square$

The previous discussion leads to the Algorithm 1 and justifies its correctness. Examples 4.1, 4.2, 4.3 show different outputs of the algorithm.

Example 4.1. All possible parameters of Euclidean hulls of cyclic codes of length 11 over $\mathbb{Z}_{27}$ are determined as follows.

1. The divisors of 11 are 1 and 11.
   a) We have $1 \in \mathcal{N}_3$, so $\texttt{ord}_1(3) = 1$ and $\gamma(1;3) = 1$.

Algorithm 1: Parameters of the Euclidean hull of a cyclic serial code over R.

Input: Length n, and a finite chain ring R of parameters (p, a, r, e, s) such that $\texttt{gcd}(p, n) = 1$.
Output: All possible s-tuples $(k_0, k_1, \cdots, k_{s-1})$ describing the parameters of the Euclidean hull of a cyclic serial code

. **if** $n \in \mathcal{N}_q$ **then**
  for $0 \leq t < s$ **do**
    if $t < \lceil \frac{s}{2} \rceil$ **then**
      $k_t = 0$.
    else
      For each $i \mid n$, compute $\texttt{ord}_i(q)$, and $\gamma(i; q)$,
      therefore all the possible values of k_t, such that

$$k_t = \sum_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \texttt{ord}_i(q) \cdot u_i^{(t)},$$

      with $0 \leq u_i^{(t)} \leq \gamma(i; q)$.
  return *The possible parameters* $(0, \cdots, 0, k_{\lceil \frac{s}{2} \rceil}, \cdots, k_{s-1})$ *such that* $k_{\lceil \frac{s}{2} \rceil} + \cdots + k_{s-1} \leq n$.
else
  For each $i \mid n$, if $i \in \mathcal{N}_q$, then compute $\texttt{ord}_i(q)$, and $\gamma(i; q)$.
  For each $j \mid n$, if $j \notin \mathcal{N}_q$, then compute $\texttt{ord}_j(q)$, and $\beta(j; q)$.
  for $0 \leq t < s,$ **do**
    if $t = 0$ **then**
      compute $k_0 = \sum_{\substack{j \mid n \\ i \notin \mathcal{N}_q}} \texttt{ord}_j(q) \cdot \nu_j^{(0)}$, where $0 \leq \nu_j^{(0)} \leq \beta(j; q)$
    else
      while $0 < t < \lceil \frac{s}{2} \rceil$ **do**
        For a fixed $\nu_j^{(t-1)}$ in k_{t-1}, compute $k_t = \sum_{\substack{j \mid n \\ i \notin \mathcal{N}_q}} \texttt{ord}_j(q) \cdot \nu_j^{(t)}$, where
        $0 \leq \nu_j^{(t)} \leq \beta(j; q) - \nu_j^{(t-1)}$,
        if $2k_0 + k_1 + \cdots + k_t \leq n$ **then**
          consider k_t,
        else
          reject k_t
      while $t \geq \lceil \frac{s}{2} \rceil$ **do**
        For a fixed $\nu_j^{(t-1)}$ in k_{t-1}, compute $k_t = \sum_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \texttt{ord}_i(q) \cdot u_i^{(t)} + \sum_{\substack{j \mid n \\ i \notin \mathcal{N}_q}} \texttt{ord}_j(q) \cdot \nu_j^{(t)}$,
        where $0 \leq u_i^{(t)} \leq \gamma(i; q)$ and $0 \leq \nu_j^{(t)} \leq 2 \cdot (\beta(j; q) - \nu_j^{(t-1)})$.
        if $2k_0 + k_1 + \cdots + k_t \leq n$ **then**
          consider k_t,
        else
          reject k_t
  return *The possible parameters* $(k_0, k_1, \cdots, k_{s-1})$ *describing the Euclidean hull of a cyclic serial code.*

b) We have $11 \notin \mathcal{N}_3$, so $\texttt{ord}_{11}(3) = 5$ and $\beta(11; 3) = 1$.

2. It follows that

$$\begin{aligned}
k_0 &= 5\nu_{11}^{(0)}, \text{ where } 0 \leq \nu_{11}^{(0)} \leq 1 \\
k_1 &= 5\nu_{11}^{(1)}, \text{ where } 0 \leq \nu_{11}^{(1)} \leq 1 - \nu_{11}^{(0)} \\
k_2 &= u_1^{(2)} + 5\nu_{11}^{(2)} \text{ where } 0 \leq u_1^{(2)} \leq 1 \text{ and } 0 \leq \nu_{11}^{(2)} \leq 2(1 - \nu_{11}^{(1)}).
\end{aligned}$$

Hence, the all possible parameters (k_0, k_1, k_2) of the Euclidean hulls of cyclic codes of length 7 over $\mathbb{Z}_8$ are given in the following table

k_0	k_1	k_2
0	0	0, 1, 5, 6, 10, 11
	5	0, 1
5	0	0, 1

Example 4.2. All the possible parameters (k_0, k_1, k_2) of the Euclidean hull of a cyclic code of length 7 over $\mathbb{Z}_8$ are determined as follows.

1. The divisors of 7 are 1 and 7.
   a) We have $1 \in \mathcal{N}_2$, so $\mathtt{ord}_1(2) = 1$ and $\gamma(1; 2) = 1$.
   b) We have $7 \notin \mathcal{N}_2$, so $\mathtt{ord}_7(2) = 3$ and $\beta(7; 2) = 1$.
2. It follows that

$$k_0 = 3\nu_7^{(0)}, \text{ where } 0 \le \nu_7^{(0)} \le 1$$
$$k_1 = 3\nu_7^{(1)}, \text{ where } 0 \le \nu_7^{(1)} \le 1 - \nu_7^{(0)}$$
$$k_2 = u_1^{(2)} + 3\nu_7^{(2)} \text{ where } 0 \le u_1^{(2)} \le 1 \text{ and } 0 \le \nu_7^{(2)} \le 2(1 - \nu_7^{(1)}).$$

Hence, the all possible parameters (k_0, k_1, k_2) of the Euclidean hulls of cyclic codes of length 7 over $\mathbb{Z}_8$ are given in the following table

k_0	k_1	k_2
0	0	0, 1, 3, 4, 6, 7
	3	0, 1
3	0	0, 1

Example 4.3. The parameters of the Euclidean hulls of cyclic codes of length 21 over $\mathbb{Z}_8$ are given by

1. The divisors of 21 are $\{1, 3, 7, 21\}$.
   (a) $1; 3 \in \mathcal{N}_2$, we have $\mathtt{ord}_1(2) = 1, \mathtt{ord}_3(2) = 2$ and $\gamma(1; 2) = \gamma(3; 2) = 1$.
   (b) $7; 21 \notin \mathcal{N}_2$, we have $\mathtt{ord}_7(2) = 3, \mathtt{ord}_{21}(2) = 6$ and $\beta(7; 2) = \beta(21; 2) = 1$.
2. It follows that

$$k_0 = 3\nu_7^{(0)} + 6\nu_{21}^{(0)}, \text{ with } 0 \le \nu_j^{(0)} \le 1, \text{ where } j \in \{7; 21\}.$$
$$k_1 = 3\nu_7^{(1)} + 6\nu_{21}^{(1)}, \text{ with } 0 \le \nu_j^{(1)} \le 1 - \nu_j^{(0)}, \text{ where } j \in \{7; 21\}.$$
$$k_2 = u_1^{(2)} + 2u_3^{(2)} + 3\nu_7^{(2)} + 6\nu_{21}^{(2)}, \text{ with } 0 \le u_i^{(2)} \le 1 \text{ and } 0 \le \nu_j^{(2)} \le 2(1 - \nu_j^{(1)}),$$
$$\text{where } i \in \{1; 3\}, \text{ and } j \in \{7; 21\}.$$

Hence, the all possible parameters (k_0, k_1, k_2) of the Euclidean hulls of cyclic codes of length 21 over $\mathbb{Z}_8$ are given in the following table

k_0	k_1	k_2
0	0	0, 1, 2, 3, $\cdots$, 21
	3	0, 1, 2, 3, 6, 7, 8, 9, 12, 13, 14, 15
	6	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
	9	0, 1, 2, 3
3	0	0, 1, 3, $\cdots$, 15
	6	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
6	0	0, 1, 3, $\cdots$, 9
	3	0, 1, 2, 3, 6, 7, 8, 9, 12, 13, 14, 15
9	0	0, 1, 2, 3

Corollary 4. *The set $\aleph(n,s,q)$ of q-dimensions of the Euclidean hull of a cyclic serial code of length n over R, is given by*

$$\aleph(n,s,q)=\left\{\sum_{\substack{i\,|\,n\\ i\in\mathcal{N}_q}}\mathtt{ord}_i(q)\left(\sum_{l=1}^{\gamma(i;q)}\triangle_{il}\right)+\sum_{\substack{j\,|\,n\\ i\notin\mathcal{N}_q}}\mathtt{ord}_j(q)\left(\sum_{h=1}^{\beta(j;q)}\blacktriangle_{jh}\right)\ \Big|\ \begin{array}{l}0\le\triangle_{il}\le s-\lceil\frac{s}{2}\rceil\\ 0\le\blacktriangle_{jh}\le s\end{array}\right\}.$$

Proof. Let C be a cyclic serial code of length n over R with triple-sequence

$$\Big((((x_{il}^{(a)})_{0\le a<s})^{\circ}),(((y_{jh}^{(a)})_{0\le a<s})^{\bullet}),(((z_{jh}^{(a)})_{0\le a<s})^{\bullet})\Big)$$

in $\mathcal{E}_n(q,s)$. From Theorem 2, the parameters $(k_0,k_1,\cdots,k_{s-1})$ of $\mathcal{H}_0(C)$ where for all $0\le t\le s-1$,

$$k_t=\sum_{\substack{i\,|\,n\\ i\in\mathcal{N}_q}}\mathtt{ord}_i(q)\cdot\left(\sum_{i=1}^{\gamma(i;q)}u_{il}^{(t)}\right)+\sum_{\substack{j\,|\,n\\ i\notin\mathcal{N}_q}}\mathtt{ord}_j(q)\cdot\left(\sum_{h=1}^{\beta(j;q)}(\varepsilon_{jh}^{(t-1)}-\varepsilon_{jh}^{(t)})\right).$$

Thus the q-dimension of $\mathcal{H}_0(C)$ is $\sum_{t=0}^{s-1}(s-t)k_t$. It follows that

$$\mathtt{dim}_q(C)=\sum_{\substack{i\,|\,n\\ i\in\mathcal{N}_q}}\mathtt{ord}_i(q)\cdot\left(\sum_{i=1}^{\gamma(i;q)}\triangle_{il}\right)+\sum_{\substack{j\,|\,n\\ i\notin\mathcal{N}_q}}\mathtt{ord}_j(q)\cdot\left(\sum_{h=1}^{\beta(j;q)}\blacktriangle_{jh}\right).$$

From Remark 3,

$$\triangle_{il}=\sum_{t=0}^{s-1}\triangle_{il}^{(t)}=\sum_{t=\lceil\frac{s}{2}\rceil}^{s-1}\triangle_{il}^{(t)}\le s-\left\lceil\frac{s}{2}\right\rceil,$$

and if $j\in\mathcal{N}_q$ then $\blacktriangle_j=0$. Otherwise,

$$\blacktriangle_{jh}=\sum_{t=0}^{s-1}\blacktriangle_{jh}^{(t)}=\sum_{t=0}^{\lceil\frac{s}{2}\rceil-1}\blacktriangle_{jh}^{(t)}+\sum_{t=\lceil\frac{s}{2}\rceil}^{s-1}\blacktriangle_{jh}^{(t)}$$

$$\leq \max_{0\leq b\leq s-\lceil \frac{s}{2}\rceil} \left\{\left(\left\lceil\frac{s}{2}\right\rceil+b\right)+2\left(s-\left\lceil\frac{s}{2}\right\rceil-b\right)\right\} = s. \quad \square$$

5. The average q-dimension

We will denote by $\mathcal{C}(n;R)$ the set of all cyclic serial codes over length n over R. The average q-dimension of the Euclidean hull of cyclic of length n over R is

$$\mathtt{E}_R(n) = \sum_{C\in\mathcal{C}(n;R)} \frac{\mathtt{dim}_q(\mathcal{H}_0(C))}{|\mathcal{C}(n;R)|}.$$

In this section, an explicit formula for $\mathtt{E}_R(n)$ and bounds are given in terms of $\mathtt{B}_{n,q}$ where

$$\mathtt{B}_{n,q} = \mathtt{deg}\prod_{\substack{i\,|\,n\\ i\in\mathcal{N}_q}}\left(\prod_{l=1}^{\gamma(i;q)}\Omega(G_{il})\right) = \sum_{\substack{i\,|\,n\\ i\in\mathcal{N}_q}}\phi(i),$$

where G_{il} are symmetric q-cyclotomic cosets modulo n of size $\mathtt{ord}_j(q)$, as defined in (4).

Consider the maps

$$\begin{array}{cccc} \triangle: & \mathcal{E}_s & \to & \mathbb{N} \\ & (x^{(0)},\cdots,x^{(s-1)}) & \mapsto & \sum\limits_{t=0}^{s-1}\min\left\{\sum\limits_{a=0}^{t}x^{(a)};1-\sum\limits_{a=0}^{s-t-1}x^{(a)}\right\}, \end{array} \tag{14}$$

and $\blacktriangle:\mathcal{E}_s\times\mathcal{E}_s\to\mathbb{N}$ defined as

$$\blacktriangle(\mathbf{y},\mathbf{z}) = \sum_{t=0}^{s-1}\left(\min\left\{\sum_{a=0}^{t}y^{(a)};1-\sum_{a=0}^{s-t-1}z^{(a)}\right\}+\min\left\{\sum_{a=0}^{t}z^{(a)};1-\sum_{a=0}^{s-t-1}y^{(a)}\right\}\right), \tag{15}$$

where $(\mathbf{y},\mathbf{z}) = ((y^{(0)},\cdots,y^{(s-1)}),(z^{(0)},\cdots,z^{(s-1)}))$.

Let $\tau\in\aleph(n,s,q)$ be an element in the set defined in Corollary 4. Then τ is the q-dimension of the Euclidean hull of a cyclic serial code of length n over R. The following result gives the number of cyclic serial codes of length n over R whose Euclidean hulls have q-dimension τ.

Proposition 8. *Let n be a positive integer such that $\mathtt{gcd}(n,p)=1$ and $\tau\in\aleph(n,s,q)$ where $\aleph(n,s,q)$ is described in Corollary 4. The number $\wp(n,\tau;R)$ of cyclic serial codes of length n over R whose Euclidean hulls have q-dimension τ is given by:*

$$\wp(n,\tau;R) = \sum_{(((\triangle_{il})^{\circ}),((\blacktriangle_{jh})^{\bullet}))\in\Upsilon(\tau)}\left(\prod_{\substack{i\,|\,n\\ i\in\mathcal{N}_q}}\prod_{l=1}^{\gamma(i;q)}\psi_s(\triangle_{il})\right)\left(\prod_{\substack{j\,|\,n\\ j\notin\mathcal{N}_q}}\prod_{h=1}^{\beta(j;q)}\rho_s(\blacktriangle_{jh})\right),$$

where

$$\psi_s(\triangle_{il}) = |\{\mathbf{x} \in \mathcal{E}_s \ : \triangle\ (\mathbf{x}) = \triangle_{il}\}|,\ \rho_s(\blacktriangle_{jh}) = |\{(\mathbf{y}, \mathbf{z}) \in \mathcal{E}_s \times \mathcal{E}_s\ :\ \blacktriangle(\mathbf{y}, \mathbf{z}) = \blacktriangle_{jh}\}|,$$

and

$$\Upsilon(\tau) = \left\{ (((\triangle_{il})^{\circ}), ((\blacktriangle_{jh})^{\bullet}))\ :\ \sum_{\substack{i\,|\,n \\ i\in N_q}} \mathit{ord}_i(q) \left(\sum_{l=1}^{\gamma(i;q)} \triangle_{il} \right) + \sum_{\substack{j\,|\,n \\ i\notin N_q}} \mathit{ord}_j(q) \left(\sum_{h=1}^{\beta(j;q)} \blacktriangle_{jh} \right) = \tau \right\}.$$

The above expression of $\mathtt{E}_R(n) = \sum_{\tau\in\aleph(n,s,q)} \frac{\tau\cdot\wp(n,\tau;R)}{|C\in C(n;R)|}$, might lead to a tedious and lengthy computation. The remainder of the section will show an alternative simpler expression for the expected value.

Lemma 5. *Consider the random variable $\triangle$ defined in (14) with uniform probability. The expected value $\mathtt{E}(\triangle)$ is given by:*

$$\mathtt{E}(\triangle) = \frac{\left\lceil \frac{s}{2} \right\rceil \left(s - \left\lceil \frac{s}{2} \right\rceil\right)}{s+1} = \begin{cases} \frac{s^2}{4(s+1)}, & \text{if } s \text{ even;} \\ \frac{s-1}{4}, & \text{if } s \text{ odd.} \end{cases}$$

Proof. Let $t \in \{0; 1; \cdots; s-1\}$ and $\mathbf{x} = (x^{(0)}, \cdots, x^{(s-1)}) \in \mathcal{E}_s$. Set

$$\triangle^{(t)}_{(\mathbf{x})} = \min \left\{ \sum_{a=0}^{t} x^{(a)}; 1 - \sum_{a=0}^{s-t-1} x^{(a)} \right\} \in \{0; 1\}.$$

Then $\triangle^{(t)}_{(\mathbf{x})} = 1$ if and only if $2t \geq s$ and , $\sum_{a=s-t}^{t} x^{(a)}_{il} = 1$. Thus for all $\eta \in \mathbb{N}$, we have

$$|\{\mathbf{x} \in \mathcal{E}_s\ : \triangle^{(t)}_{(\mathbf{x})} = \eta\}| = \begin{cases} 2t - s + 1, & \text{if } t \geq \left\lceil \frac{s}{2} \right\rceil \text{ and } \eta = 1; \\ 0, & \text{otherwise.} \end{cases}$$

Therefore,

$$\begin{aligned} |\{\mathbf{x} \in \mathcal{E}_s\ : \triangle\ (\mathbf{x}) = \eta\}| &= \begin{cases} \sum_{t=\left\lceil \frac{s}{2} \right\rceil}^{s-1} (2t - s + 1), & \text{if } \eta = s - \left\lceil \frac{s}{2} \right\rceil; \\ 0, & \text{otherwise.} \end{cases} \\ &= \begin{cases} \left\lceil \frac{s}{2} \right\rceil \left(s - \left\lceil \frac{s}{2} \right\rceil\right), & \text{if } \eta = s - \left\lceil \frac{s}{2} \right\rceil; \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Since $|\mathcal{E}_s| = s + 1$ and $\mathtt{P}(\{\mathbf{x} \in \mathcal{E}_s\ : \triangle\ (\mathbf{x}) = \eta\}) = \frac{|\{\triangle(\mathbf{x})=\eta\}|}{|\mathcal{E}_s|}$, it follows that,

$$\mathtt{E}(\triangle) = \sum_{\eta\in\mathbb{N}} \eta \mathtt{P}(\{\mathbf{x} \in \mathcal{E}_s\ : \triangle\ (\mathbf{x}) = \eta\}) = \frac{\left\lceil \frac{s}{2} \right\rceil \left(s - \left\lceil \frac{s}{2} \right\rceil\right)}{s+1}. \qquad \square$$

Lemma 6. *Consider the random variable $\blacktriangle : \mathcal{E}_s \times \mathcal{E}_s \to \mathbb{N}$ defined in (15) with uniform distribution. The expected value $E(\blacktriangle)$ is given by*

$$E(\blacktriangle) = \frac{s(2s+1)}{3(s+1)}.$$

Proof. From Corollary 4, for any $(\mathbf{y}, \mathbf{z}) \in \mathcal{E}_s \times \mathcal{E}_s$, $0 \leq \blacktriangle(\mathbf{y}, \mathbf{z}) \leq s$. Let

$$\mathcal{E}_s(\eta) = \{(\mathbf{y}, \mathbf{z}) \in \mathcal{E}_s \times \mathcal{E}_s \ : \ \blacktriangle(\mathbf{y}, \mathbf{z}) = \eta\},$$

for $0 \leq \eta \leq s$. Now,

$$|\mathcal{E}_s(\eta)| = \begin{cases} 2(\eta+1), & \text{if } 0 \leq \eta \leq s-1; \\ s+1, & \text{if } \eta = s. \end{cases}$$

Thus

$$\begin{aligned} \mathtt{E}(\blacktriangle) &= \frac{1}{(s+1)^2} \sum_{\eta=0}^{s} \eta |\mathcal{E}_s(\eta)|; \\ &= \frac{1}{(s+1)^2} \left(\sum_{\eta=1}^{s-1} 2\eta(\eta+1) + s(s+1) \right); \\ &= \frac{s(2s^2+3s+1)}{3(s+1)^2}. \quad \square \end{aligned}$$

Theorem 3. *The average q-dimension of the Euclidean hull of cyclic serial codes from $C(n; R)$ is*

$$E_R(n) = \begin{cases} \left(\frac{(2s+1)s}{6(s+1)}\right) n - \left(\frac{(s+2)s}{12(s+1)}\right) B_{n,q}, & \text{if } s \text{ even;} \\ \left(\frac{(2s+1)s}{6(s+1)}\right) n - \left(\frac{s^2+2s+3}{12(s+1)}\right) B_{n,q}, & \text{if } s \text{ odd,} \end{cases}$$

where $B_{n,q} = \sum_{\substack{i \mid n \\ i \in N_q}} \phi(i)$.

Proof. Let Y be the random variable that takes as value $\mathtt{dim}_q(\mathcal{H}_0(C))$ when we choose at random a cyclic serial code from $C(n; R)$ with uniform probability. Then $\mathtt{E}(Y) = \mathtt{E}_R(n)$. By Lemma 3, there exists an one-to-one correspondence between $C(n; R)$, and $\mathcal{E}_n(q, s)$. Therefore, choosing a cyclic serial code C from $C(n, R)$ their probabilities are identical. By Corollary 4, we obtain

$$Y = \sum_{\substack{i \mid n \\ i \in N_q}} \mathtt{ord}_i(q) \left(\sum_{l=1}^{\gamma(i;q)} \triangle_{il} \right) + \sum_{\substack{j \mid n \\ i \notin N_q}} \mathtt{ord}_j(q) \left(\sum_{h=1}^{\beta(j;q)} \blacktriangle_{jh} \right).$$

For all i and j dividing n such that $i \in \mathcal{N}_q$ and $j \notin \mathcal{N}_q$, from Lemmas 5 and 6, we note that $\mathtt{E}(\triangle_{il}) = \mathtt{E}(\triangle)$ and $\mathtt{E}(\blacktriangle_{jh}) = \mathtt{E}(\blacktriangle)$. So, we get

$$\begin{aligned}
\mathtt{E}(Y) &= \sum_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \mathtt{ord}_i(q) \left(\sum_{l=1}^{\gamma(i;q)} \mathtt{E}(\triangle) \right) + \sum_{\substack{j \mid n \\ i \notin \mathcal{N}_q}} \mathtt{ord}_j(q) \left(\sum_{h=1}^{\beta(j;q)} \mathtt{E}(\blacktriangle) \right); \\
&= \sum_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \phi(i) \mathtt{E}(\triangle_{il}) + \sum_{\substack{j \mid n \\ i \notin \mathcal{N}_q}} \frac{\phi(j)}{2} \mathtt{E}(\blacktriangle_{jh}); \\
&= \mathtt{B}_{n,q} \mathtt{E}(\triangle) + \left(\frac{n - \mathtt{B}_{n,q}}{2} \right) \mathtt{E}(\blacktriangle); \\
&= \frac{n}{2} \mathtt{E}(\blacktriangle) - \mathtt{B}_{n,q} \cdot \left(\frac{1}{2} \mathtt{E}(\blacktriangle) - \mathtt{E}(\triangle) \right).
\end{aligned}$$

From Lemmas 5 and 6, we have

$$\mathtt{E}_R(n) = \begin{cases} \left(\frac{(2s+1)s}{6(s+1)}\right) n - \left(\frac{(s+2)s}{12(s+1)}\right) \mathtt{B}_{n,q}, & \text{if } s \text{ even;} \\ \left(\frac{(2s+1)s}{6(s+1)}\right) n - \left(\frac{s^2+2s+3}{12(s+1)}\right) \mathtt{B}_{n,q}, & \text{if } s \text{ odd.} \end{cases} \qquad \square$$

From [19], we have $\mathtt{B}_{n,q} = n$ if $n \in \mathcal{N}_q$ and $1 \le \mathtt{B}_{n,q} \le \frac{2n}{3}$ if $n \notin \mathcal{N}_q$. Thus

- If $n \in \mathcal{N}_q$, then

$$\mathtt{E}_R(n) = \begin{cases} \frac{s^2 n}{4(s+1)}, & \text{if } s \text{ even;} \\ \frac{n(s-1)}{4}, & \text{if } s \text{ odd.} \end{cases}$$

- If $n \notin \mathcal{N}_q$, then

$$\begin{cases} \frac{(5s+1)sn}{18(s+1)} \le \mathtt{E}_R(n) \le \frac{2n(2s+1)s-(s+2)s}{12(s+1)}, & \text{if } s \text{ even;} \\ \frac{(5s^2+s-3)n}{18(s+1)} \le \mathtt{E}_R(n) \le \frac{2ns(2s+1)-(s^2+2s+3)}{12(s+1)}, & \text{if } s \text{ odd.} \end{cases}$$

Remark 4. $\mathtt{E}_R(n)$ grows at the same rate with ns as s and n is coprime with p and tend to infinity. Thus, the upper limit of the sequence $\left(\frac{\mathtt{E}_R(n)}{sn}\right)_{\substack{(s,n) \in (\mathbb{N} \setminus \{0\})^2 \\ \gcd(p,n)=1}}$ is at most $\frac{1}{3}$ and its lower limit is at least $\frac{5}{18}$.

6. Conclusion

The hulls of cyclic serial codes over an arbitrary finite chain ring have been investigated. Especially, the parameters and the average of the q-dimension of the Euclidean hull of cyclic codes are studied in terms of triple-sequences. The parameters and the average p^r-dimensions of the Euclidean hulls of cyclic serial codes of arbitrary length have been determined as well. Asymptotically, it has been shown that the average of p^r-dimension of the Euclidean hull of cyclic serial codes of length over R grows the same rate as the length of the codes. An extension of this paper to the case of the hulls of cyclic or constacyclic codes over finite chain rings is an interesting research problem as well. It would be interesting to study the properties of Euclidean hulls of negacyclic serial codes.

References

[1] E.F. Assmus, J.D. Key, Affine and projective planes, Discrete Math. 83 (1990) 161–187.
[2] A. Batoul, K. Guenda, T.A. Gulliver, On self-dual codes over finite chaing rings, Des. Codes Cryptogr. 70 (2014) 347–358.
[3] S. Bhowmick, A. Fotue-Tabue, E. Martínez-Moro, R. Bandi, S. Bagchi, Do non-free LCD codes over finite commutative Frobenius rings exist, Des. Codes Cryptogr. 88 (2020) 825–840.
[4] H.Q. Dinh, S.R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inf. Theory 50 (2004) 1728–1744.
[5] A. Fotue-Tabue, C. Mouaha, On the lattice of cyclic linear codes over finite chain rings, Algebra Discrete Math. 27 (2019) 252–268.
[6] A. Fotue Tabue, E. Martínez-Moro, C. Mouaha, Galois correspondence on linear codes over finite chain rings, Discrete Math. 343 (2020) 111653, https://doi.org/10.1016/j.disc.2019.111653.
[7] T. Honold, I. Landjev, Linear codes over finite chain rings, Electron. J. Comb. 7 (2000), #R11.
[8] H. Liu, X. Pan, Galois hulls of linear codes over finite fields, Des. Codes Cryptogr. 88 (2020) 241–255.
[9] S. Jitman, E. Sangwisut, The average hull dimension of negacyclic codes over finite fields, Math. Comput. Appl. 23 (3) (2018) 41, https://doi.org/10.3390/mca23030041.
[10] S. Jitman, E. Sangwisut, P. Udomkavanich, Hulls of cyclic codes over $\mathbb{Z}_4$, Discrete Math. 343 (2020) 111621, https://doi.org/10.1016/j.disc.2019.111621.
[11] J.S. Leon, Computing automorphism groups of error-correcting codes, IEEE Trans. Inf. Theory 28 (3) (1982) 496–511.
[12] B.R. McDonald, Finite Rings with Identity, Marcel Dekker Inc., New York, 1974.
[13] E. Martínez-Moro, I.F. Rúa, Multivariable codes over finite chain rings: serial codes, SIAM J. Discrete Math. 20 (2006) 947–959.
[14] G.H. Norton, A. Salagean, On the structure of linear and cyclic codes over a finite chain ring, Appl. Algebra Eng. Commun. Comput. 10 (2000) 489–506.
[15] E. Petrank, R.M. Roth, Is code equivalence easy to decide?, IEEE Trans. Inf. Theory 43 (1997) 1602–1604.
[16] N. Sendrier, Finding the permutation between equivalent codes: the support splitting algorithm, IEEE Trans. Inf. Theory 46 (2000) 1193–1203.
[17] N. Sendrier, On the dimension of the hull, SIAM J. Appl. Math. 10 (1997) 282–293.
[18] E. Sangwisut, S. Jitman, S. Ling, P. Udomkavanich, Hulls of cyclic and negacyclic codes over finite fields, Finite Fields Appl. 33 (2015) 232–257.
[19] G. Skersys, The average dimension of the hull of cyclic codes, Discrete Appl. Math. 128 (2003) 275–292.
[20] A.K. Singh, N. Kumar, K.P. Shum, Cyclic self-orthogonal codes over finite chain rings, Asian-Eur. J. Math. 11 (2018) 1850078.
[21] Robert B. Warfield Jr., Serial rings and finitely presented modules, J. Algebra 37 (1975) 187–222, https://doi.org/10.1016/0021-8693(75)90074-5.
[22] E.A. Whelan, A note on finite local rings, Rocky Mt. J. Math. 22 (1992) 757–759.