Discrete Mathematics 347 (2024) 113715

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On the structure of repeated-root polycyclic codes over local rings

Maryam Bajalan [a,1], Edgar Martínez-Moro [b,*,2], Reza Sobhani [c], Steve Szabo [d], Gülsüm Gözde Yılmazgüç [e,3]

[a] *Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Acad. G. Bonchev Str. Bl. 8, 1113, Sofia, Bulgaria*
[b] *Institute of Mathematics, University of Valladolid, Castilla, Spain*
[c] *Department of Applied Mathematics and Computer Science, Faculty of Mathematics and Statistics, University of Isfahan, Isfahan, Iran*
[d] *Department of Mathematics & Statistics, Eastern Kentucky University, Richmond, KY, USA*
[e] *Ipsala Vocational College, Trakya University, Edirne, Turkey*

ARTICLE INFO

Article history:
Received 29 January 2023
Received in revised form 6 July 2023
Accepted 20 September 2023
Available online 2 October 2023

Keywords:
Polycyclic code
Duality
Repeated-root code
Mattson-Solomon transform
Matrix-product code

ABSTRACT

This paper provides the Generalized Mattson Solomon polynomial for repeated-root polycyclic codes over local rings that gives an explicit decomposition of them in terms of idempotents. It also states some structural properties of repeated-root polycyclic codes over finite fields in terms of matrix product codes. Both approaches provide a description of the $\perp_0$-dual code for a given polycyclic code.

1. Introduction

Polycyclic codes over a finite local ring R were introduced in [20] and they are described as ideals on the quotient ring $R[x]/\langle f(x)\rangle$ with $f(x) \in R[x]$. These codes generalize the well-known classes of cyclic and constacyclic codes. Polycyclic codes over finite fields have been studied from several points of view, we will be especially interested in the so called $\perp_0$-duality (see [1,28] and the references therein). Polycyclic codes over chain rings have been studied in different directions, see for example [9,19,30,29]. In [2], the authors made a generalization where the ring is a finite commutative local ring and the polynomial defining the ambient space has simple roots. That paper proposed a transform approach that generalizes the classical Mattson-Solomon (Fourier) transform in finite fields.

* Corresponding author.
E-mail addresses: maryam.bajalan@math.bas.bg (M. Bajalan), edgar.martinez@uva.es (E. Martínez-Moro), r.sobhani@sci.ui.ac.ir (R. Sobhani), Steve.Szabo@eku.edu (S. Szabo), gozdeyilmazguc@trakya.edu.tr (G.G. Yılmazgüç).

[1] Maryam Bajalan is supported by the Bulgarian Ministry of Education and Science, Scientific Programme “Enhancing the Research Capacity in Mathematical Sciences (PIKOM)”, No. DO1-67/05.05.2022.

[2] Second author was supported in part by Grant TED2021-130358B-I00 funded by MCIN/AEI/10.13039/501100011033 and by the “European Union NextGenerationEU/PRTR”.

[3] Last author is supported by TÜBİTAK within the scope of 2219 International Post Doctoral Research Fellowship Program with application number 1059B192101164. Her work was completed while she visited the Institute of Mathematics of University of Valladolid (IMUVa). She thanks the IMUVa for their kind hospitality.

https://doi.org/10.1016/j.disc.2023.113715

On the other side, several papers have been devoted to explain the matrix product code structure of repeated-root cyclic and constacyclic codes over finite fields, see for example [31,4], and over some finite chain rings [5].

In this paper, we complete the study on the Mattson-Solomon transform approach in [2] for polycyclic codes over finite local rings in the case that the defining polynomial has repeated-roots. Some special cases for the cyclic case have been previously studied in [24], the so-called monomial like codes. We also give a matrix product code structure that describes repeated-root polycyclic codes over finite fields. In both cases, we provide expressions for the $\perp_0$-dual code of a given polycyclic code.

The structure of the paper is as follows. In Section 2, some preliminaries are given on finite commutative local rings, on the Hasse derivative of a polynomial over a finite local ring and on the Generalized Discrete Fourier Transform. Section 3 provides the Generalized Mattson Solomon polynomial (GMS) for polycyclic codes over local rings that gives an explicit decomposition of them in terms of idempotents. In Section 5, we state some structural properties of repeated-root polycyclic codes over finite fields in terms of matrix product codes. In both Section 3 and Section 5, we give a description of the $\perp_0$-dual code of a given polycyclic code.

2. Preliminaries

Throughout the paper, R will denote a finite local ring of characteristic $q = p^r$ for a prime p and a positive integer r, $\mathfrak{m}$ will denote the maximal ideal of R and $\mathbb{F}_q = R/\mathfrak{m}$ the finite residue field of R. It is well-known that R is trivially complete and thus Hensel, i.e., every element of R is nilpotent or a unit and $\mathfrak{m}$ is a nilpotent ideal. We denote by $\bar{\cdot}$ the natural polynomial ring morphism $\bar{\cdot} : R \to (R/\mathfrak{m})$ and, abusing notation, we will use it also for polynomial rings acting on the coefficients $\bar{\cdot} : R[x] \to (R/\mathfrak{m})[x] = \mathbb{F}_q[x]$. Let $\mathcal{J}$ denote the set of all polynomials f in $R[x]$ such that $\bar{f}$ has distinct zeros in the algebraic closure of $\mathbb{F}_q$, a polynomial in $\mathcal{J}$ has distinct zeros in local extensions of R, $\mathcal{R}_f = R[x]/\langle f \rangle$ (where f is monic) is a separable local extension ring if and only if f is an irreducible polynomial in $\mathcal{J}$, and the polynomials in $\mathcal{J}$ admit a unique factorization into irreducible polynomials and a polynomial in $\mathcal{J}$ has no multiple roots in any local extension of R. In the rest of the paper, unless other thing is stated, f will denote a polynomial in $\mathcal{J}$ and $F = f^m$ for a non-negative integer m (in some sections $m = p^k$ where p is the characteristic of R).

2.1. Hasse derivative and generalized discrete Fourier transform

The Generalized Discrete Fourier Transform (GDFT) for repeated-root cyclic codes over a finite field $\mathbb{F}_q$ of characteristic p (p a prime) of length $N = np^k$, where $(n, p) = 1$, was defined by Massey in [25]. After that, the definition is generalized for quasi-cyclic and quasi-twisted codes over finite fields in [15] and [13], respectively. In those references, the Hasse derivative of polynomials over finite fields plays an important role. For more information about the Hasse derivative of polynomials over fields we refer the reader to [25,12].

In this section, let R denote a commutative finite unitary ring and $p(x) = \sum_{i=0}^{n} p_i x^i \in R[x]$ be a polynomial. For $k \in \{0, 1, \ldots, n\}$, the k^{th} formal derivative of $p(x)$ is defined as $p^{(k)}(x) = k! \sum_{i=0}^{n} \binom{i}{k} p_i x^{i-k}$, and the k^{th} Hasse derivative of $p(x)$ is defined as $p^{[k]}(x) = \frac{1}{k!} p^{(k)}(x)$ [18, page 363], i.e.,

$$p^{[k]}(x) = \sum_{i=0}^{n} \binom{i}{k} p_i x^{i-k} = \sum_{i=0}^{n-k} \binom{i+k}{k} p_{i+k} x^i.$$

The following result holds directly from the definition and straightforward computations.

Lemma 2.1. *Let $p(x)$ and $q(x)$ be two polynomials in $R[x]$.*

1. *$(p+q)^{[k]}(x) = p^{[k]}(x) + q^{[k]}(x)$.*
2. *(Taylor expansion) If $p(x)$ is of degree n and λ is an arbitrary element in R, then $p(x+\lambda) = \sum_{k=0}^{n} p^{[k]}(\lambda) x^k$.*
3. *(Product rule) $(pq)^{[k]}(x) = \sum_{i=0}^{k} p^{[i]}(x) q^{[k-i]}(x)$.*

From now on, let $f(x)$ be a simple-root polynomial $f(x) = (x-\alpha_0)(x-\alpha_1)\ldots(x-\alpha_{n-1}) \in \mathcal{J}$ which has n distinct roots in a fixed ordering $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ in an extension ring R' of R. Recall that the Discrete Fourier Transform (DFT) of an n-tuple $(g_0, g_1, \ldots, g_{n-1})$ is $(g(\alpha_0), g(\alpha_1), \ldots, g(\alpha_{n-1}))$, where $g(x) = g_0 + g_1 x + \ldots + g_{n-1} x^{n-1} \in R[x]/\langle f(x) \rangle$, see [2] for further details.

Definition 2.1. Let $F(x) = ((x-\alpha_0)(x-\alpha_1)\ldots(x-\alpha_{n-1}))^m = (f(x))^m$ be a repeated-root monic polynomial in $R[x]$ of degree $N = nm$ and $g(x) = \sum_{i=0}^{N-1} g_i x^i \in R[x]/\langle F(x) \rangle$. We define the Generalized Discrete Fourier Transform (GDFT) of $g(x)$ as

$$\begin{bmatrix} g(\alpha_0) & g(\alpha_1) & \dots & g(\alpha_{n-1}) \\ g^{[1]}(\alpha_0) & g^{[1]}(\alpha_1) & \dots & g^{[1]}(\alpha_{n-1}) \\ \vdots & \vdots & \dots & \vdots \\ g^{[m-1]}(\alpha_0) & g^{[m-1]}(\alpha_1) & \dots & g^{[m-1]}(\alpha_{n-1}) \end{bmatrix},$$

where $g^{[i]}$ is the i^{th}-Hasse derivative for all $1 \leqslant i \leqslant m-1$.

Example 2.2. Suppose that $F(x) = x^6 - 3x^5 + 3x^4 - x^3 \in \mathbb{Z}_4[x]$, which is decomposed over $\mathbb{Z}_{16}$ as $F(x) = (x-1)^3(x-12)^3$. If $g(x) = 1 + 2x^3 + x^4 + 3x^5 \in \mathbb{Z}_4[x]/\langle F(x) \rangle$, then $g^{[1]} = 2x^2 + 3x^4$ and $g^{[2]} = 2x + 2x^2 + 2x^3$. Therefore, the GDFT of n-tuples related to $g(x)$ is

$$\mathrm{GDFT}(g) = \begin{bmatrix} g(1) & g(12) \\ g^{[1]}(1) & g^{[1]}(12) \\ g^{[2]}(1) & g^{[2]}(12) \end{bmatrix} = \begin{bmatrix} 7 & 1 \\ 5 & 0 \\ 6 & 8 \end{bmatrix}.$$

2.2. Generalized Vandermonde matrices

Let $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ be a fixed ordering of the roots of polynomial $f(x) = (x-\alpha_0)(x-\alpha_1)\dots(x-\alpha_{n-1}) \in R[x]$ in the extension ring R' of R.

For $0 \leqslant i \leqslant N-1$, take $p_i(x) = x^i$ and construct the $N \times m$ matrix

$$R(x) = \begin{bmatrix} p_0(x) & p_0^{[1]}(x) & \dots & p_0^{[m-1]}(x) \\ p_1(x) & p_1^{[1]}(x) & \dots & p_1^{[m-1]}(x) \\ \vdots & \vdots & \dots & \vdots \\ p_{N-1}(x) & p_{N-1}^{[1]}(x) & \dots & p_{N-1}^{[m-1]}(x) \end{bmatrix}.$$

In fact, ij-entry of $R(x)$ is $\binom{i-1}{i-j}x^{i-j}$ for $i \geqslant j$ and zero otherwise. The *generalized Vandermonde matrix* related to the roots $\alpha_0, \alpha_1, \dots, \alpha_n$ of the repeated-root polynomial $F(x) = (f(x))^m$ of degree $N = nm$ over a local ring R is defined by

$$V = V(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) = [R(\alpha_0)\ R(\alpha_1)\ \dots R(\alpha_{n-1})].$$

Example 2.3. If $F(x) = (x-\alpha_0)^3(x-\alpha_1)^3$ then

$$V = [R(\alpha_0)\ R(\alpha_1)] = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ \alpha_0 & 1 & 0 & \alpha_1 & 1 & 0 \\ \alpha_0^2 & 2\alpha_0 & 1 & \alpha_1^2 & 2\alpha_1 & 1 \\ \alpha_0^3 & 3\alpha_0^2 & 3\alpha_0 & \alpha_1^3 & 3\alpha_1^2 & 3\alpha_1 \\ \alpha_0^4 & 4\alpha_0^3 & 6\alpha_0^2 & \alpha_1^4 & 4\alpha_1^3 & 6\alpha_1^2 \\ \alpha_0^5 & 5\alpha_0^4 & 10\alpha_0^3 & \alpha_1^5 & 5\alpha_1^4 & 10\alpha_1^3 \end{bmatrix}.$$

Note that if $m = 1$, the generalized Vandermonde matrix is compatible with the usual Vandermonde matrix related to $F(x)$. The determinant of V is $\prod_{0 \leqslant i < j \leqslant n-1}(\alpha_i - \alpha_j)^{n_i n_j}$, see [14] for a proof. Thus V is an invertible matrix in the local ring R if and only if $\alpha_i - \alpha_j$ is a unit in R for each pair of indexes $i \neq j$, if and only if $\overline{\alpha_i} \neq \overline{\alpha_j}$; see Lemma 2.5 in [26]. Therefore V is an invertible matrix if and only if $\overline{\alpha_i} \neq \overline{\alpha_j}$ for all $i \neq j$. Note that throughout the paper, it is assumed that $f \in \mathcal{J}$, then $\bar{f}$ has distinct roots $\overline{\alpha_i}$ for $0 \leqslant i \leqslant n-1$. Thus V will always be an invertible matrix.

Let $F(x) = x^N - \sum_{i=0}^{N-1} F_i x^i$ and C_F be the companion matrix related to $F(x)$, i.e.,

$$C_F = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ F_0 & F_1 & F_2 & \dots & F_{N-1} \end{bmatrix}.$$

It is a well-known fact that $F(x)$ is the characteristic polynomial of C_F. Let us denote the Jordan form of the companion matrix C_F by J_F, i.e., a diagonal block matrix with $n \times n$ blocks so that each block has roots on the diagonal, 1 on the superdiagonal and other entries are zero. If V is invertible, then the companion matrix is reduced to $C_F = V J_F V^{-1}$.

3. Generalized Mattson Solomon polynomial

Let V be the usual Vandermonde matrix related to the distinct elements $\alpha_0, \dots, \alpha_{n-1}$ and $f(x) = \prod_{i=0}^{n-1}(x - \alpha_i)$. For a given $g(x) = \sum_{i=0}^{n-1} g_i x^i$ in $R[x]/\langle f(x)\rangle$, the Mattson Solomon polynomial of $g(x)$ is

$$\mathrm{MS}(g) = \sum_{i=0}^{n-1} g(\alpha_i)x^i = [g_0\, g_1\, \dots g_{n-1}]V[1\, x \dots x^{n-1}]^{\mathrm{tr}}, \tag{1}$$

where tr denotes the transpose matrix. Note that the map MS is well defined in the quotient space $R[x]/\langle f(x)\rangle$, see [2] for a complete account on it. Now, let $F(x) = f(x)^m$ be a repeated-root polynomial of degree $N = mn$ over the local ring R and fix an ordering on distinct roots $\alpha_0, \dots, \alpha_{n-1}$. Let us consider the quotient polynomial ring $\mathcal{R} = \left(\frac{R'[y]}{\langle y^m\rangle}, \cdot\right)$, where $\cdot$ is the ordinary polynomial multiplication modulo y^m.

Theorem 3.1. *The map*

$$\begin{array}{rcl} \mathrm{MS}: \left(\frac{R[x]}{\langle F(x)\rangle}, \bullet\right) & \longrightarrow & \left(\frac{\mathcal{R}[x]}{\langle f(x)\rangle}, \star\right) \\ g(x) & \mapsto & \sum_{j=0}^{n-1}\left(\sum_{i=0}^{m-1} g^{[i]}(\alpha_j)y^i\right)x^j \end{array}$$

is a ring injective homomorphism, where $\bullet$ denotes ordinary polynomial multiplication modulo $F(x)$ and $\star$ denotes the component-wise multiplication modulo $f(x)$.

Proof. First, we will show that the mapping is well-defined. Given two representatives $h(x), g(x)$ of an element in $\frac{R[x]}{\langle F(x)\rangle}$, that is $g(x) - h(x) = k(x)f(x)^m$, for $0 \le i \le m-1$. We have by applying the product rule that

$$g^{[i]}(x) - h^{[i]}(x) = \sum_{j=0}^{i} k^{[i]}(x)(f(x)^m)^{[i-j]}.$$

But $(f(x)^m)^{[i-j]} = (i-j)!(f(x)^m)^{(i-j)}$ (the usual derivative of $f(x)^m$) which is indeed 0 mod f for $0 \le i \le m-1$. Therefore for $0 \le i \le m-1$ one has that $g^{[i]}(x)$, $h^{[i]}(x)$ provide the same values when evaluated at α_j, $j = 0, \dots, n-1$.

Let $g(x) = \sum_{i=0}^{N-1} g_i x^i \in \frac{R[x]}{\langle F(x)\rangle}$ and V be the generalized Vandermonde matrix related to roots $\alpha_0, \dots, \alpha_{n-1}$. Consider the column vector

$$u = \left[1\, y \dots y^{m-1}\ x\ xy \dots xy^{m-1} \dots x^{n-1}\ x^{n-1}y \dots x^{n-1}y^{m-1}\right]^{\mathrm{tr}},$$

where tr denotes the transpose of the vector. Then we have that $\mathrm{MS}(g)$ is given by

$$\begin{aligned}&\left[g(\alpha_0)\ g^{[1]}(\alpha_0)\dots g^{[m-1]}(\alpha_0)\dots g(\alpha_{n-1})\ g^{[1]}(\alpha_{n-1})\ \dots g^{[m-1]}(\alpha_{n-1})\right]u \\ &= [g_0\, g_1\, \dots g_{N-1}]\, V u.\end{aligned}$$

Since the matrix V is invertible, then MS is injective. Now it is enough to show that $\mathrm{MS}(g \bullet h) = \mathrm{MS}(g) \star \mathrm{MS}(h)$ that follows applying the product rule of the Hasse derivative, we can easily check that $\mathrm{MS}(g) \star \mathrm{MS}(h)$ can be computed as

$$\sum_{i=0}^{n-1}\left(\left(\sum_{j=0}^{m-1} g^{[j]}(\alpha_i)y^j\right)\cdot\left(\sum_{j=0}^{m-1} h^{[j]}(\alpha_i)y^j\right)\right)x^i = \sum_{i=0}^{n-1}\left(\sum_{j=0}^{m-1}(gh)^{[j]}(\alpha_i)y^j\right)x^i. \quad \square$$

Note that the mapping in the above theorem gives the ordinary Mattson-Solomon transform when applied to a simple-root polynomial. Thus, by abusing the notation, we will denote both the same. We will call the map MS in the above theorem *the Generalized Mattson Solomon* map associated to F.

Example 3.2. (Example 2.2 Cont.) Let $m = 3$, $n = 2$, $f(x) = x^2 - x \in \mathbb{Z}_4[x]$ and $\mathcal{R} = \mathbb{Z}_{16}[y]/\langle y^3\rangle$. Then

$$\mathrm{MS}(g(x)) = (7 + 5y + 6y^2) + (1 + 8y^2)x \in \mathcal{R}[x]/\langle f(x)\rangle.$$

Remark 3.3. Theorem 3.1 states that every repeated-root polycyclic code is isomorphic to an ideal in a bivariable polynomial ring, since $\frac{\mathcal{R}[x]}{\langle f(x)\rangle} \simeq \frac{R'[x,y]}{\langle f(x), y^m\rangle}$.

Lemma 3.4. *The map* MS *in Theorem 3.1 is equivalent to each of the following mappings.*

$$\begin{array}{rccc} \mathrm{MS}: & \left(\frac{R[x]}{\langle F(x)\rangle}, \bullet\right) & \longrightarrow & \left(\frac{\mathcal{R}[x]}{\langle f(x)\rangle}, \star\right) \\ & g(x) & \mapsto & \sum_{i=0}^{n-1} g(\alpha_i + y)x^i \end{array} \tag{2}$$

and

$$\begin{array}{rccc} \mathrm{MS}: & \left(\frac{R[x]}{\langle F(x)\rangle}, \bullet\right) & \longrightarrow & \left(\frac{\frac{R'[u]}{\langle (u-1)^m\rangle}[x]}{\langle f(x)\rangle}, \star\right) \\ & g(x) & \mapsto & \sum_{i=0}^{n-1} g(u\alpha_i)x^i. \end{array} \tag{3}$$

Proof. Since $y^m = 0$, by the Taylor expansion for the Hasse derivative, we get $g(\alpha_i + y) = \sum_{j=0}^{m-1} g^{[j]}(\alpha_i)y^j$. Thus $\mathrm{MS}(g) = \sum_{i=0}^{n-1} g(\alpha_i + y)x^i$, which gives the mapping (2). The set $\{\alpha_0(y+1) - y, \ldots, \alpha_{n-1}(y+1) - y\}$ are roots of $F(x)$, since $y^m = 0$. Put $u = y + 1$ and use the mapping (2) to find $\mathrm{MS}(g(x))$. Now, $R'[u-1] \cong R'[u]$ provides the mapping (3). □

Remark 3.5. Note that in the case $F(x)$ is a simple-root polynomial (i.e., $m = 1$), we get $y = 0$ and $u = 1$. Hence, the two mappings presented in the previous lemma are compatible with the Mattson Solomon mapping given in [2].

Remark 3.6. In Definition 2.1, we define the GDFT for polycyclic codes of length $N = mn$ over rings as a generalization of the GDFT for repeated-root cyclic codes of length $N = np^k$ over fields presented by Massey in [25]. Now we are able to present other definitions of the GDFT associated with the mappings in Lemma 3.4:

$$\begin{array}{rccc} \mathrm{GDFT}: & R^N & \longrightarrow & \mathcal{R}^n \\ & (g_0, g_1, \ldots, g_N) & \mapsto & (g(\alpha_0 + y),\ g(\alpha_1 + y),\ \ldots,\ g(\alpha_{n-1} + y)) \end{array} \tag{4}$$

and

$$\begin{array}{rccc} \mathrm{GDFT}: & R^N & \longrightarrow & \mathcal{A}^n \\ & (g_0, g_1, \ldots, g_N) & \mapsto & (g(u\alpha_0),\ g(u\alpha_1),\ \ldots,\ g(u\alpha_{n-1})), \end{array} \tag{5}$$

where $\mathcal{A} = \frac{R'[u]}{\langle (u-1)^m\rangle}$. Note that (4) is compatible with the definition of the DFT given in [2], and Equation (5) is also compatible with the DFT in [16] in the quasi-cyclic case.

4. The decomposition of the ambient space

We will start by studying the ring $\mathcal{R}$ defined in the previous section.

Lemma 4.1 *(Corollary 3.8 in [10]). Let R be a local ring and $g \in R[x]$ be a monic irreducible polynomial. Then $R[x]/\langle g(x)^n\rangle$ is a local ring for any positive integer n.*

Lemma 4.2. *Let S be a Galois extension of the local ring R. Then*

1. *S is the unramified local ring, i.e., R and S has the same maximal ideal.*
2. *If $f \in R[x]$ is square-free, then f has distinct zeros in the local extension S.*
3. *S is an R-free module generated by roots of f.*

Proof. See Theorems 3.15, 3.18, 5.11 in [10] □

Corollary 4.3. *Let R' be the Galois extension of the local ring R containing n distinct roots of the polynomial $f(x) = \prod_{i=0}^{n-1}(x - \alpha_i)$. Then $\mathcal{R} = R'[y]/\langle y^m\rangle$ is a local ring.*

The proof of the corollary follows from the fact that R is local, R' is a Galois extension and applying Lemmas 4.1 and 4.2. Then, from the counting argument in [11], if we count the elements in $\mathcal{R}$ that are p^{ms}, and the number of zero divisors in $\mathcal{R}$ is given by $p^{c+(s-1)m}$ where p^c is the number of zero divisors of R, therefore from [11, Theorem 1], $\mathcal{R}$ is a local ring. Furthermore, note that $\mathcal{R}$ is also a chain ring if and only if R is a finite field. This follows from the fact that the maximal ideal of $\mathcal{R}$ is $\langle m, y\rangle$, where m is the generator of the maximal ideal of R and it is principal if p is the characteristic of R.

4.1. Decomposition of the codes

In this section, we are going to find a decomposition of the ambient space $\frac{R[x]}{\langle F(x)\rangle}$. Recall that the ring $\left(\frac{\mathcal{R}[x]}{\langle f(x)\rangle},\star\right)$ is equipped with the component-wise product and the ring $\left(\frac{R[x]}{\langle F(x)\rangle},\bullet\right)$ is equipped with the ordinary polynomial product. Let us denote $\frac{R[x]}{\langle F(x)\rangle}$ by R_F. Let $f = f_1f_2\dots f_r$, where $f_1, f_2\dots f_r$ are distinct monic irreducible polynomials. We will define a relation on the set of indices $I = \{0, 1, \dots, n-1\}$ as follows: $i \sim j$ if and only if α_i, α_j are roots of the same polynomial f_k, i.e., $f_k(\alpha_i) = f_k(\alpha_j) = 0$. Therefore I will be partitioned into the disjoint classes I_k related to f_k.

From now on in Subsection 4.1, we will consider the MS map in Theorem 3.1 extended to R'

$$\mathrm{MS}:\left(R'_F=\frac{R'[x]}{\langle F(x)\rangle},\bullet\right)\longrightarrow\left(\frac{\mathcal{R}[x]}{\langle f(x)\rangle},\star\right)$$

or, what is the same, consider a polynomial $f(x)$ which completely splits in linear factors in the ring we are working on.

It is easy to see that, again for cardinality reasons, it is now an isomorphism and we can define $E_i = \mathrm{MS}^{-1}\left(\sum_{j\in I_i} x^j\right)$. The pre-images $\{E_1, \dots, E_r\}$ will provide us the primitive idempotents, more precisely:

Proposition 4.4.

1. *Each E_i is a primitive idempotent.*
2. *$E_iE_j = 0$ for $i \neq j$, and $\sum_{i=1}^r E_i = 1$.*
3. *The only idempotents in R_F are in the form $\sum_{j\in S} E_j$ for some $S \subseteq \{1, 2, \dots, r\}$.*
4. *$R'_F \cong \oplus_{i=1}^r\langle E_i\rangle \cong \oplus_{i=1}^r \frac{R_F}{\langle 1-E_i\rangle}$.*

Proof. 1. Note that $x^j \star x^j = x^j$ for all $0 \le j \le n-1$. Thus $E_i^2 = \mathrm{MS}^{-1}\left(\sum_{j\in I_i} x^j\right) = E_i$. To check that E_i is primitive, let $E_i = A(x)+B(x)$, where $A(x)$ and $B(x)$ are orthogonal idempotents in R'_F. Let $\mathrm{MS}(A(x))$ be denoted by $\sum_{k=0}^{n-1} a_kx^k = a(x)$, and similarly let $\mathrm{MS}(B(x))$ be denoted by $\sum_{k=0}^{n-1} b_kx^k = b(x)$. We want to prove that $A(x) = 0$ or $B(x) = 0$, i.e. $a(x) = 0$ or $b(x) = 0$. By Contradiction, let $a(x) \neq 0$ and $b(x) \neq 0$. We know

$$\sum_{j\in I_i} x^j = \mathrm{MS}(E_i) = \mathrm{MS}(A(x)) + \mathrm{MS}(B(x)) = a(x) + b(x) = \sum_{i=0}^{n-1}(a_i + b_i)x^i,$$

and hence $a_k + b_k = 1$ for $k \in I_i$. Since $A(x)$ and $B(x)$ are idempotent, $a(x), b(x)$ are also idempotent elements in $\mathcal{R}[x]$. According to component-wise multiplication in $\mathcal{R}[x]$, we conclude that $a_i^2 = a_i$ and $b_i^2 = b_i$ for all i. Now since $\mathcal{R}$ is local, $a_i, b_i \in \{0, 1\}$ for all i. Moreover, the orthogonality of $A(x)$ and $B(x)$ implies that $0 = a(x)b(x) = \sum_{i=0}^{n-1} a_ib_ix^i$, and hence $a_ib_i = 0$ for all i. Now, considering that $a_k + b_k = 1$ and $a_k, b_k \in \{0, 1\}$ for $k \in I_i$, we must have $b_k = 0$ for that $k \in I_i$ with $a_k \neq 0$ and $a_k = 0$ for that $k \in I_i$ with $b_k \neq 0$. Define $M = \{j \in I_i : a_j \neq 0\}$ and $N = \{j \in I_i : b_j \neq 0\}$. Since $a(x) \neq 0$ and $b(x) \neq 0$, we have $M \neq \emptyset$ and $N \neq \emptyset$. Therefore, there are two non-empty subsets $M \subsetneq I_i$ and $N \subsetneq I_i$ such that $M \cap N = \emptyset$, $M \cup N = I_i$ and $a(x) = \sum_{j\in M} x^j$ and $b(x) = \sum_{j\in N} x^j$. According to the definition I_i, there is a polynomial f_k such that all roots of f_k are in I_i. Partitioning the set I_i into two disjoint subsets M and N separates the roots of f_k into two groups. Let's denote by $f_M(x)$ and $f_N(x)$ the polynomials whose roots are those corresponding to indices in M and N, respectively. Then $f_k(x) = f_M(x)f_N(x)$, which contradicts our initial assumption that $f_k(x)$ is irreducible.

2. For $i \neq j$, I_i and I_j are disjoint and hence $E_iE_j = 0$. Moreover, since $\sum_{i=0}^{n-1} x^i$ is the unit element of $\mathcal{R}[x]$ we get

$$1 = \mathrm{MS}^{-1}(\sum_{i=0}^{n-1} x^i).$$

3. Clearly, to obtain the idempotents in R'_F, it is necessary to study idempotents in $MS(R'_F) = \frac{\mathcal{R}[x]}{\langle f(x)\rangle}$. Let $a(x) = \sum_{k=0}^{n-1} a_kx^k$ be an idempotent element in $\frac{\mathcal{R}[x]}{\langle f(x)\rangle}$. We get $\sum_{k=0}^{n-1} a_kx^k = a(x) = a(x)^2 = \sum_{k=0}^{n-1} a_k^2x^k$. Thus $a_k = a_k^2$ for all $0 \leqslant k \leqslant n-1$ and since $\mathcal{R}$ is local, we have $a_k \in \{0, 1\}$ for all $0 \le k \le n-1$. If we let $S = \{i \mid a_i \neq 0\}$, then $a(x) = \sum_{i\in S} x^i$ and $A(x) = \mathrm{MS}^{-1}(a(x)) = \sum_{i\in S} E_i$.

4. The first isomorphism follows from the fact that $\{E_1, \dots, E_r\}$ is the set of pairwise primitive orthogonal idempotents. To prove the second isomorphism we define $\theta : R_F \to \langle E_i\rangle$ via $g \mapsto gE_i$. Let $gE_i = 0$. Then $g = g(1-E_i) + gE_i = g(1-E_i)$, and hence $\ker\theta = \langle 1-E_i\rangle$, which gives the result. □

This provides the following description of the codes in terms of the idempotents in the case of a ring of prime characteristic.

Proposition 4.5. *Let R' be a local ring with prime characteristic p and $N = np^k$. Then*

1. *If $f_i(x) = \prod_{j\in I_i}(x-\alpha_j)$ then $(f_i(x))^{p^k} = 1 - E_i$.*
2. *If the ideal C of R'_F has an idempotent generator, then C is generated by $\prod_{i\in S}(f_i(x))^{p^k}$ for some $S \subseteq \{1, 2, \ldots, r\}$.*

Proof.

1. $1 - E_i = \mathrm{MS}^{-1}(\sum_{i=0}^{n-1} x^i) - \mathrm{MS}^{-1}(\sum_{i=0}^{n-1} d_i x^i) = \mathrm{MS}^{-1}(\sum_{i=0}^{n-1} e_i x^i)$ such that $e_i \notin I_i$. On the other hand, recall that $\alpha_i - \alpha_j$ is a unit in R' if and only if $\overline{\alpha_i} \neq \overline{\alpha_j}$. Since $f \in \mathcal{J}$, $\bar{f}$ has distinct roots $\overline{\alpha_i}$ for $0 \leqslant i \leqslant n-1$, and we get
$$\begin{aligned}(f_i(\alpha_j + y))^{p^k} &= (\alpha_j + y - \alpha_{i_1})^{p^k} \ldots (\alpha_j + y - \alpha_{i_t})^{p^k}\\ &= ((\alpha_j - \alpha_{i_1})^{p^k} + y^{p^k}) \ldots ((\alpha_j - \alpha_{i_t})^{p^k} + y^{p^k})\\ &= (\alpha_j - \alpha_{i_1})^{p^k} \ldots (\alpha_j - \alpha_{i_t})^{p^k}\\ &= \begin{cases} 0 & j \in I_i,\\ \text{unit} & j \notin I_i.\end{cases}\end{aligned}$$
Thus $\mathrm{MS}((f_i(x))^{p^k}) = \sum_{j=0}^{n-1}(f_i(\alpha_0 + y))^{p^k} x^j \in \langle \sum_{j\notin I_i} x^j\rangle = \mathrm{MS}(1 - E_i)$. Now since MS is injective, the result holds.
2. The only idempotent elements in R'_F are in the form $\sum_{i\in K} E_i$ for some subset K of $\{1, 2, \ldots, r\}$. By the fact that E_i's are orthogonal we have
$$\sum_{i\in K} E_i = 1 - \sum_{i\notin K} E_i = \prod_{i\notin K}(1 - E_i) = \prod_{i\notin K}(f_i(x))^{p^k}.$$
Now it is enough to take $S = K^c$. □

Corollary 4.6. *Let R' be a local ring with prime characteristic p and $N = np^k$, where f completely splits. Then*

$$\frac{R'[x]}{\langle F(x)\rangle} = \frac{R'[x]}{\langle (f(x))^{p^k}\rangle} \cong \bigoplus_{i=1}^{r} \frac{R'[x]}{\langle (f_i(x))^{p^k}\rangle}.$$

Proof. Part (4) of Proposition 4.4, Part (1) of Proposition 4.5 and the Third Isomorphism Theorem give the proof. □

Remark 4.7. Note that in this section (Subsection 4.1) we have considered codes over the ring R'_F, if we want to restrict ourselves to R_F we must consider subring subcodes that behave as subfield subcodes in the field case, for a reference on them, their Galois closure and a Delsarte's like theorem in the chain ring case see [21].

4.2. $\perp_0$ duality

Consider the following inner product over the ring $R_F = \frac{R[x]}{\langle F(x)\rangle}$

$$\langle g_1(x), g_2(x)\rangle_{(0)} = g_1 g_2(0), \quad g_1(x), g_2(x) \in R_F. \tag{6}$$

We will denote the dual of the polycyclic code $C \subseteq R_F$ associated with this inner product by $C^{\perp_0}$ given by

$$C^{\perp_0} = \{g(x) \in R_F \mid \langle g(x), h(x)\rangle_{(0)} = 0, \text{for all } h(x) \in C\}.$$

Theorem 4.8. *Let C be a polycyclic code of length $N = np^k$ in R_F. If F_0 is an invertible element in R, then*

1. *The inner product $\langle\,,\rangle_{(0)}$ is non-degenerate.*
2. *$C^{\perp_0} = \mathrm{Ann}(C)$, where Ann stands for the annihilator ideal.*
3. *$C^{\perp_0}$ is a polycyclic code.*

Proof.

1. We must show that the orthogonal of R_F is zero. Let $g = g_0 + g_1 x + \ldots + g_{N-1}x^{N-1} \in R_F$ and $\langle g, x^i\rangle_{(0)} = 0$ for all $0 \leqslant i \leqslant N-1$. From $\langle g, 1\rangle_{(0)} = 0$ we conclude $g_0 = 0$. Also, by considering $0 = \langle g, x^i\rangle_{(0)} = g_{N-i}F_0$ for all $1 \leqslant i \leqslant N-1$ and invertibility F_0, we obtain $g_{N-i} = 0$, i.e., $g = 0$.
2. Let $h(x) \in \mathrm{Ann}(C)$, therefore $h(x)g(x) = 0$ for all $g(x) \in C$ and hence $hg(0) = 0$, i.e., $h(x) \in C^{\perp_0}$. Thus $\mathrm{Ann}(C) \subseteq C^{\perp_0}$. Conversely, let $h \in C^{\perp_0}$ and $g \in C$ be an arbitrary element. Hypothesis $0 = \langle g, h\rangle_{(0)} = hg(0)$ implies that $x^i hg(0) = 0$ for all $0 \leqslant i \leqslant N-1$. Now by part (1) we have $hg = 0$, which gives the result.
3. It is obvious by Part (2). □

Remark 4.9. In the literature of simple-root polycyclic codes over $R[x]/\langle f(x)\rangle$, it is always assumed that f_0 is a unit in the ring R, see [20,9]. Because this assumption is guaranteed that every left polycyclic code is right polycyclic and as a result we get ride of studying left and right at the same time. In this paper, we always assume that $F(0) = F_0$, the constant term of the polynomial F, is a unit in R. Because this assumption is guaranteed that the dual of every polycyclic code ($C^{\perp_0}$) is again polycyclic (also in our previous paper in the simple-root case [2] we have assumed that f_0 is a unit in order to have a polycyclic dual code).

We now define another inner product over R_F:

$$\langle g_1(x), g_2(x)\rangle_{\mathrm{MS}} = \mathrm{MS}(g_1) \star \mathrm{MS}(g_2), \quad g_1(x), g_2(x) \in R_F. \tag{7}$$

As usual, we will denote the dual of the polycyclic code $C \subseteq R_F$ associated with this inner product by $C^{\perp_{\mathrm{MS}}}$, which is naturally defined as

$$C^{\perp_{\mathrm{MS}}} = \{g \in R_F \mid \mathrm{MS}(g) \star \mathrm{MS}(c) = 0 \text{ for all } c \in C\}. \tag{8}$$

The following result shows how one can check the annihilator duality in terms of the Mattson Solomon transform.

Theorem 4.10. *For the polycyclic code C over R_F, we have* $\mathrm{Ann}(\mathcal{C}) = \mathcal{C}^{\perp_{\mathrm{MS}}}$.

Proof. Since the Mattson-Solomon mapping is an injective morphism we have

$$gc = 0 \iff \mathrm{MS}(gc) = 0 \iff \mathrm{MS}(g) \star \mathrm{MS}(c) = 0,$$

which implies $\mathrm{Ann}(\mathcal{C}) = \mathcal{C}^{\perp_{\mathrm{MS}}}$. □

Remark 4.11. Note that all the results in Subsection 4.2 are given in the ring R_F since only injectivity of the MS map is needed, so we do not need to consider the ring R'_F.

4.3. A note on multivariable codes

In [2], the Mattson Solomon map for several variable serial codes over chain rings is presented. That construction was based on the decomposition of the tensor product of the R-modules $R[x_1]/\langle f_1(x_1)\rangle$ and $R[x_2]/\langle f_2(x_2)\rangle$ in terms of the tensor product of powers of their related companion matrices E_f and E_g and their simultaneous diagonalization by the matrix $V_{f_1} \otimes V_{f_2}$ where V_{f_i} is Vandermonde matrix corresponding to f_i for $i = 1, 2$. In the case where we have a principal ring, at most one of the defining polynomials is a repeated-root one, say $f_1(x) = f(x_1)^m$, and the remaining ones should be non-repeated-root polynomials and R is a Galois ring, see [22]. In that later is the case, we can provide a Mattson Solomon transform in terms of the Generalized Vandermonde matrices in the same fashion as in [2].

Multivariable codes over the ring R are ideals of the quotient ring $\mathscr{R} = R[x_1, \dots x_w]/\langle t_1(x_1), \dots, t_w(x_w)\rangle$. If all polynomials $t_1(x_1), \dots t_w(x_w)$ are simple-roots, then these codes are called serial multivariate codes, and otherwise they are called modular multivariate codes. The transform approach to the serial case over local rings was studied in [2]. Note that serial multivariate codes are well-behaved because they can be regarded as principal ideals in $\mathscr{R}$. This property is not generally true in the modular case. In the case $r > 2$, $\mathscr{R}$ is principal ideal ring if and only if R is a Galois ring and the number of polynomials for which $\bar{t}_i(x_i)$ are not square-free is at most one, see [22, Theorem 1].

For the sake of simplicity, all results in this section will be proved for $w = 2$ and can be straightforward worked out for $w > 2$. Let R be a Galois ring, $f(x_1)$ a polynomial of degree n over R with distinct simple-roots $\alpha_0, \dots, \alpha_{n-1}$ in an extension ring R'_1, and $F(x_1) = (f(x_1))^m$ a polynomial of degree $N = nm$. Moreover, let $g(x_2)$ be a polynomial of degree M over R with distinct simple-roots $\beta_0, \dots, \beta_{M-1}$ in an extension ring R'_2. Let V be the generalized Vandermonde matrix related to $\alpha_0, \dots, \alpha_{n-1}$ and v be the usual Vandermonde matrix related to $\beta_0, \dots, \beta_{M-1}$. Consider the tensor product

$$v \otimes V = \begin{bmatrix} V & \dots & V \\ \beta_0 V & \dots & \beta_{M-1} V \\ \vdots & \dots & \vdots \\ \beta_0^{M-1} & \dots & \beta_{M-1}^{M-1} V \end{bmatrix}.$$

Since $det(v \otimes V) = det(v)^M det(V)^N$ and v, V are invertible, then $v \otimes V$ is invertible. A polynomial $p(x_1, x_2) \in R[x_1, x_2]/\langle F(x_1), g(x_2)\rangle$ can de written as $p(x_1, x_2) = \sum_{j=0}^{M-1} p_j(x_1) x_2^j$, where $p_j(x_1) = \sum_{i=0}^{N-1} p_{i,j} x_1^i$. Relate the vector

$$p = (p_{0,0},\ p_{1,0},\ \dots,\ p_{N-1,0},\ p_{0,1},\ p_{1,1},\ \dots,\ p_{N-1,1},\ \dots,\ p_{0,M-1},\ p_{1,M-1},\ \dots,\ p_{N-1,M-1})$$

to the polynomial $p(x_1, x_2)$. It can be easily seen that the product of the vector p and matrix $v \otimes V$ is as follows:

$$p(v\otimes V)=\big(p(\alpha_0+y,\beta_0),\ \dots,\ p(\alpha_{n-1}+y,\beta_0),\ p(\alpha_0+y,\beta_1),\ \dots,\ p(\alpha_{n-1}+y,\beta_1),\\ \dots,\ p(\alpha_0+y,\beta_{M-1}),\ \dots,\ p(\alpha_{n-1}+y,\beta_{M-1})\big).$$

Take $R''=R'_1+R'_2$. Clearly, $p(\alpha_i+y,\beta_j)\in R''$ for all $0\leqslant i\leqslant n-1$ and $0\leqslant j\leqslant M-1$. Define the multivariable Mattson-Solomon transform for modular multivariable codes as

$$\begin{aligned}\mathrm{MS}:\left(\tfrac{R[x_1,x_2]}{\langle F(x_1),g(x_2)\rangle},\bullet\right)&\longrightarrow\left(\tfrac{R''[x_1,x_2]}{\langle f(x_1),g(x_2)\rangle},\star\right)\\ p(x_1,x_2)\qquad&\mapsto\sum_{i=0}^{n-1}\sum_{j=0}^{M-1}p(\alpha_i+y,\beta_j)x_1^ix_2^j,\end{aligned}$$

where $\bullet$ denotes ordinary polynomial multiplication modulo $F(x_1)$, $g(x_2)$ and $\star$ denotes the component-wise multiplication modulo $f(x_1)$, $g(x_2)$. Obviously, the mapping MS is a ring homomorphism and since $v\otimes V$ is invertible, MS is also injective.

5. Matrix-product structure of certain polycyclic codes

We prove the structure of some repeated-root polycyclic codes with the help of matrix-product codes in the paper [31]. From now on, we will consider repeated-root polynomials just over the finite field $\mathbb{F}_q$, where $q=p^r$ where p is a prime number. Let $f(x)\in\mathbb{F}_{p^r}[x]$ be a simple-root polynomial of degree n and of order e, i.e., e is the smallest integer for which $f(x)|x^e-1$ and $\gcd(p,e)=1$. Let $f(x)=\prod_{i=1}^s f_i(x)$ be the unique factorization of $f(x)$ into distinct irreducible polynomials over $\mathbb{F}_{p^r}[x]$. Then, we have $f(x^{p^k})=\prod_{i=1}^s f_i(x^{p^k})$ and for each $1\le i\le s$, there exists an irreducible polynomial $g_i(x)$ in $\mathbb{F}_{p^r}[x]$ such that $f_i(x^{p^k})=g_i(x)^{p^k}$. From now on, we will assume that R is the ring

$$R=\mathbb{F}_{p^r}[x]/\langle f(x^{p^k})\rangle=\mathbb{F}_{p^r}[x]/\left\langle\left(\prod_{i=1}^s g_i(x)\right)^{p^k}\right\rangle \tag{9}$$

and we will have that $N=np^k$. One can write any element $a(x)\in R$ as $a_0(x)+a_1(x)x^{p^k}+\ldots+a_{n-1}(x)x^{(n-1)p^k}$, where $a_i(x)\in\mathbb{F}_{p^r}[x]$. Let S be the ring $\mathbb{F}_{p^r}[x,y]/\langle x^{p^k}-y,\ f(y)\rangle$. We have the following straightforward results.

Lemma 5.1. *Any ideal of the ring R is principally generated by a divisor of $f(x^{p^k})$. In fact, it is of the form $\langle G(x)\rangle$, where $G(x)=\prod_{j=1}^s g_i(x)^{i_j}$ and $0\le i_j\le p^k$.*

Lemma 5.2. *The map $\varphi:R\to S$ given by $\varphi\left(\sum_{i=0}^{n-1}a_i(x)x^{ip^k}\right)=a(x,y)=\sum_{i=0}^{n-1}a_i(x)y^i$ is a ring isomorphism.*

Now we will consider the ring

$$T=\mathbb{F}_{p^r}[x,y]/\langle x^{p^k}-1,\ f(y)\rangle=\left(\mathbb{F}_{p^r}[x]/\langle x^{p^k}-1\rangle\right)[y]/\langle f(y)\rangle, \tag{10}$$

and denote as W the ring $W=\mathbb{F}_{p^r}[x]/\langle x^{p^k}-1\rangle$. Note that W is a finite chain ring whose maximal ideal is $\langle(x-1)\rangle$.

Lemma 5.3. *The map $\psi:S\to T$ defined by $\psi(a(x,y))=a(y^{e'}x,y)$ is a ring isomorphism, where e' is the inverse of p^k in $\mathbb{Z}_e$.*

As an easy corollary, we have the following.

Corollary 5.4. *The code C is a polycyclic code in $\mathbb{F}_{p^r}[x]/\langle f(x^{p^k})\rangle$ if and only if $\mu(C)=\psi(\varphi(C))$ is a polycyclic code in $W[y]/\langle f(y)\rangle$.*

Therefore, since W is a chain ring we can apply [6, Theorem 3.5] and we get the following unique $(x-1)$-adic expansion of the code C (note that we have also a description of a system of generators of a polycyclic code over a chain ring in [27, Theorem 4.4] and its generalization in [23, Theorem 3.13]).

Proposition 5.5. *Any polycyclic code C in $W[y]/\langle f(y)\rangle$ is of the form*

$$C=\langle h_0(y),(x-1)h_1(y),\dots,(x-1)^{p^k-1}h_{p^k-1}(y)\rangle,$$

where $h_{p^k-1}(y)\mid h_{p^k-2}(y)\mid\cdots\mid h_0(y)\mid f(y)$ over $\mathbb{F}_{p^r}$. Moreover, we have

$$C=\bigoplus_{i=0}^{p^k-1}(x-1)^iC_i,$$

where for $0 \le i \le p^k - 1$, $C_i = \langle h_i(y)\rangle$ *is a polycyclic code in* $\mathbb{F}_{p^r}[y]/\langle f(y)\rangle$ *and* $C_0 \subseteq C_1 \subseteq \cdots \subseteq C_{p^k-1}$.

Note that the ideal defining C over the ring W is a single generated and the generator can be derived from the polynomials $h_i(x)$ in the above expression (see the proof of [23, Theorem 3.13]). The following theorem follows directly.

Theorem 5.6. Let $C = \langle g_1(x)^{i_1} g_2(x)^{i_2} \cdots g_r(x)^{i_r}\rangle$. Then we have

$$\mu(C) = \bigoplus_{i=0}^{p^k-1} (x-1)^i C_i,$$

where C_i is a simple-root polycyclic code with respect to $f(y)$ over $\mathbb{F}_{p^r}$. In fact we have $C_i = \langle k_i(y)\rangle$, where $k_i(y) = \prod_{j\in A_i} g_j(y)$ and $A_i = \{1 \le j \le r \mid i_j > i\}$.

The following definition introduces matrix product codes in this work. Matrix-product codes over some classes of rings have been studied in several works, see for example [8,7,5,17], but they did not consider the $\perp_0$-orthogonality.

Definition 5.1. Let $A = [a_{ij}]$ be an $\alpha \times \beta$ matrix with entries in $\mathbb{F}_{p^r}$ and let $C_1, \dots C_\alpha$ be codes of length n over $\mathbb{F}_{p^r}$. The matrix-product code $[C_1, \dots, C_\alpha] \cdot A$ is the set of all matrix products $[c_1, \dots, c_\alpha]A$, where $c_i \in C_i$, defined by

$$\begin{aligned}[c_1, \dots, c_\alpha] \cdot A = [c_1, \dots, c_\alpha] &\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1\beta} \\ a_{21} & a_{22} & \dots & a_{2\beta} \\ \vdots & \vdots & \dots & \vdots \\ a_{\alpha 1} & a_{\alpha 2} & \dots & a_{\alpha\beta} \end{bmatrix} \\ = [a_{11}c_1 + a_{21}c_2 + \dots + a_{\alpha 1}c_\alpha, a_{12}c_1 + a_{22}c_2 + \dots + a_{\alpha 2}c_\alpha,& \\ \dots, a_{1\beta}c_1 + a_{2\beta}c_2 + \dots + a_{\alpha\beta}c_\alpha].&\end{aligned} \tag{11}$$

Lemma 5.7 *(Proposition 2.9 [3]). If a matrix consisting of some* α *columns of* A *is non-singular and* $C = [C_1, \dots, C_\alpha] \cdot A$*, then* $\mid C \mid = \mid C_1 \mid \dots \mid C_\alpha \mid$.

Definition 5.2 *(Definitions 1 and 2 in [31]).*

- Let J be the $p^k \times p^k$ matrix whose $(i, p^k - i + 1)$-th entry $(1 \le i \le p^k)$ is equal to 1 and other entries are equal to zero, let P be the $p^k \times p^k$ matrix whose (i, j)-th entry $(1 \le i, j \le p^k)$ is equal to $\binom{i-1}{j-1}$ mod p, and let Q be the $p^k \times p^k$ matrix whose (i, j)-th entry is equal to $(-1)^{(i+j)}\binom{i-1}{j-1}$ mod p and $\mathrm{CYC}(p, k)$ to be JQJ.
- For $0 \le i \le N-1$ we will write $i = ap^k + j$ where $0 \le a \le n-1$, $0 \le j \le p^k - 1$. We define the permutation σ on $\{0, 1, \dots, N-1\}$ as $\sigma(i) = jn + a$.

Lemma 5.8. $A = \mathrm{CYC}(p, k)$ *is a non-singular matrix.*

Proof. The matrix $\mathrm{CYC}(p, 1)$ is upper triangular with exactly $p - i$ zeros in the column i and ones in the diagonal, and $A = \mathrm{CYC}(p, k) = \bigotimes_{i=1}^k \mathrm{CYC}(p, 1)$ by [31]. Since the tensor product of two upper triangular matrices is again upper triangular the result follows. □

Theorem 5.9. *Let* C *be a polycyclic code in* $\mathbb{F}_{p^r}[x]/\langle (f(x))^{p^k}\rangle$ *and* $\mu(C) = \bigoplus_{i=0}^{p^k-1}(x-1)^i C_i$*, then we have that*

$$\sigma(C) = [C_{p^k-1}, C_{p^k-2}, \dots, C_0] \cdot \mathrm{CYC}(p, k).$$

Proof. Assume $a(x) = \sum_{i=0}^{n-1} a_i(x)x^{i\cdot p^k} \in C$, then $\varphi(a(x)) = \sum_{i=0}^{n-1} a_i(x)y^i$ and hence $\psi(\varphi(a(x))) = \sum_{i=0}^{n-1} a_i(y^{e'}x)y^i$. If $\sigma(a(x)) = b(x) = \sum_{i=0}^{p^k-1} x^i b_i(x^{p^k})$ then we have $\psi(\varphi(a(x))) = \sum_{i=0}^{p^k-1}(y^{e'}x)^i b_i(y)$.

On the other hand, we can write

$$\begin{aligned} b_0(y) + (y^{e'})xb_1(y) + \dots + y^{(p^k-1)e'}x^{(p^k-1)}b_{p^k-1}(y) = \\ b_0(y) + (y^{e'})(x-1+1)b_1(y) + \dots + y^{(p^k-1)e'}(x-1+1)^{(p^k-1)}b_{p^k-1}(y) = \\ \sum_{i=0}^{p^k-1}\left(\sum_{j=0}^{i}\binom{i}{j}(x-1)^j\right) y^{je'}b_i(y) = \end{aligned}$$

$$\sum_{j=0}^{p^k-1} y^{je'} \left(\sum_{i=j}^{p^k-1} \binom{i}{j} b_i(y) \right) (x-1)^j.$$

For $0 \le j \le p^k - 1$, let us denote by $c'_j(y) = y^{je'} \sum_{i=j}^{p^k-1} \binom{i}{j} b_i(y)$, and $c_j(y) := \sum_{i=j}^{p^k-1} \binom{i}{j} b_i(y)$. Hence $\sum_{j=0}^{p^k-1} c'_j(y)(x-1)^j \in \psi(\varphi(C))$ and since $\psi(\varphi(C)) = \bigoplus_{i=0}^{p^k-1} (x-1)^i C_i$, we have $c'_j(y) \in C_j$. But C_j is a polycyclic code and y is a unit element because we assume that f_0 is a unit (see Remark 4.9). Hence $c_j(y) \in C_j$ as well. Now we have

$$[c_0(y), c_1(y), \ldots, c_{p^k-1}(y)] = [b_0(y), b_1(y), \ldots, b_{p^k-1}(y)] \cdot P,$$

where P is an invertible matrix whose inverse is the matrix Q. Therefore we have

$$[c_0(y), c_1(y), \ldots, c_{p^k-1}(y)] \cdot Q = [b_0(y), b_1(y), \ldots, b_{p^k-1}(y)],$$

and it follows $\sigma(C) \subseteq [C_0, C_1, \ldots, C_{p^k-1}] \cdot Q$ and since both of the sets have the same size, we have $\sigma(C) = [C_0, C_1, \ldots, C_{p^k-1}] \cdot Q$. Using similar arguments as those used in [31], we get $\sigma(C) = [C_{p^k-1}, C_{p^k-2}, \ldots, C_0] \cdot \mathrm{CYC}(p,k)$, and the proof is now completed. □

Remark 5.10. Note that if we consider C as a cyclic code of length np^k over the field $\mathbb{F}_{p^m}$ in [31], a permutation π is provided such that

$$\pi(C) = [C_{p^k-1}, C_{p^k-2}, \ldots, C_0] \cdot \mathrm{CYC}(p,k).$$

It can be easily checked that, in general, $\pi \neq \sigma$, where σ is the permutation defined above, while the codes C_i, $0 \le i \le p^k - 1$, are the same. Therefore we have two permutations for which $\pi(C) = \sigma(C)$ or equivalently $\pi^{-1} \circ \sigma \in \mathrm{Aut}(C)$, the group of automorphism of the code C. The reason for getting different permutation in this case is related to the different kinds of isomorphisms we have considered. In fact, in [31] the mapping considered was

$$\frac{\mathbb{F}_{p^m}[x]}{\langle x^{np^k} - 1 \rangle} \xrightarrow{\sim} \frac{F_{p^m}[x, y]}{\langle x^n - y, y^{p^k} - 1 \rangle},$$

while in this paper we have considered the isomorphism

$$\frac{\mathbb{F}_{p^m}[x]}{\langle x^{np^k} - 1 \rangle} \xrightarrow{\sim} \frac{F_{p^m}[x, y]}{\langle x^{p^k} - y, y^n - 1 \rangle}.$$

Since the matrix $\mathrm{CYC}(p,1)$ is a Non-Singular by Columns matrix (NSC matrix) (see [31] for a definition), Proposition 2 in [32] implies the following corollary involving the minimum Hamming distance d_i of each of the component codes C_i and the distance of the code $d(C)$.

Corollary 5.11. *Let C be a polycyclic code in $\mathbb{F}_{p^r}[x]/\langle (f(x))^{p^k} \rangle$ such that $\mu(C) = \bigoplus_{i=0}^{p^k-1} (x-1)^i C_i$, then we have*

$$d(C) = \min\{p^k d_{p^k-1}, (p^k - 1) d_{p^k-2}, \ldots, d_0\},$$

where $d_t = d(C_t)$ and $t = 0, 1, \ldots, p^k - 1$.

5.1. $\perp_0$ duality of codes in $\mathbb{F}_{p^r}[x]/\langle f(x^{p^k}) \rangle$

The annihilator dual of a matrix-product code can be also explicitly described in terms of matrix-product codes. First we will introduce the following auxiliary result.

Lemma 5.12. *The isomorphism μ introduced in Corollary 5.4 is a $\perp_0$-duality preserving map, i.e., $\mu(C^{\perp_0}) = (\mu(C))^{\perp_0}$.*

Proof. For all $p(x)$ and $q(x)$ in $\mathbb{F}_{p^r}[x]/\langle f(x^{p^k}) \rangle$, it is easy to see that

$$\langle p(x), q(x) \rangle_0 = 0 \iff \langle \mu(p(x)), \mu(q(x)) \rangle_{(0)} = 0. \tag{12}$$

Let $p(x) \in C^{\perp_0}$. By Equation (12), we have $\langle \mu(p(x)), \mu(q(x)) \rangle_0 = 0$ for all $q(x) \in C$, i.e., $\mu(p(x)) \in (\mu(C))^{\perp_0}$, which gives $\mu(C^{\perp_0}) \subseteq (\mu(C))^{\perp_0}$. Conversely, let $z \in (\mu(C))^{\perp_0}$. Then $\langle z, \mu(p(x)) \rangle_0 = 0$ for all $p(x) \in C$. Using Equation (12), we get $\langle \mu^{-1}(z), p(x) \rangle_0 = 0$ for all $p(x) \in C$, which implies $\mu^{-1}(z) \in C^{\perp_0}$, i.e., $z \in \mu(C^{\perp_0})$. □

We will need the following Theorem to prove some results relating the $\perp_0$-dual of the matrix product code in terms of the $\perp_0$-duals of their constituent codes. For a matrix A we will denote its transpose as A^{tr}.

Theorem 5.13. *Let $D_0, \dots, D_{p^k-1}$ be polycyclic codes over $\mathbb{F}_{p^r}[x]/\langle f(x^{p^k})\rangle$. Then*

$$\big([D_{p^k-1}, \dots, D_1, D_0]\cdot \mathrm{CYC}(p,k)\big)^{\perp_0} = [D_{p^k-1}^{\perp_0}, \dots, D_1^{\perp_0}, D_0^{\perp_0}]\cdot (\mathrm{CYC}(p,k)^{-1})^{\mathrm{tr}}.$$

Proof. We claim that

$$[\mathrm{Ann}(D_{p^k-1}), \dots, \mathrm{Ann}(D_0)]\cdot (\mathrm{CYC}(p,k)^{-1})^{\mathrm{tr}} \subseteq \mathrm{Ann}\big([D_{p^k-1}, \dots, D_0]\cdot \mathrm{CYC}(p,k)\big). \tag{13}$$

Indeed, let $z = [z_{p^k-1}, \dots, z_0]\cdot (\mathrm{CYC}(p,k)^{-1})^{\mathrm{tr}} \in [\mathrm{Ann}(D_{p^k-1}), \dots, \mathrm{Ann}(D_0)]\cdot (\mathrm{CYC}(p,k)^{-1})^{\mathrm{tr}}$. Note that z is a row vector. If we consider the product of two row vector v, w as $v.w = vw^{\mathrm{tr}}$, then for an arbitrary element $x = [x_{p^k-1}, \dots, x_0]\cdot \mathrm{CYC}(p,k) \in [D_{p^k-1}, \dots, D_0]\cdot \mathrm{CYC}(p,k)$ we have

$$\begin{aligned} z.x &= \big([z_{p^k-1}, \dots, z_0]\cdot (\mathrm{CYC}(p,k)^{-1})^{\mathrm{tr}}\big)\cdot \big(\mathrm{CYC}(p,k)^{\mathrm{tr}}\cdot [x_{p^k-1}, \dots, x_0]^{\mathrm{tr}}\big) \\ &= [z_{p^k-1}, \dots, z_0]\cdot [x_{p^k-1}, \dots, x_0]^{\mathrm{tr}} = 0. \end{aligned}$$

Using the above claim, we get

$$[(D_{p^k-1})^{\perp_0}, \dots, (D_0)^{\perp_0}]\cdot (\mathrm{CYC}(p,k)^{-1})^{\mathrm{tr}} \subseteq \big([D_{p^k-1}, \dots, D_0]\cdot \mathrm{CYC}(p,k)\big)^{\perp_0}.$$

By Lemmas 5.7, 5.8 it follows

$$\begin{aligned} \mid [(D_{p^k-1})^{\perp_0}, \dots, (D_0)^{\perp_0}]\cdot (\mathrm{CYC}(p,k)^{-1})^{\mathrm{tr}} \mid &= \mid (D_{p^k-1})^{\perp_0} \mid \dots \mid (D_0)^{\perp_0} \mid \\ &= \frac{\mid \mathbb{F}_{p^r} \mid^n}{\mid D_{p^k-1} \mid} \cdots \frac{\mid \mathbb{F}_{p^r} \mid^n}{\mid D_0 \mid} \\ &= \frac{\mid \mathbb{F}_{p^r} \mid^{p^k n}}{\mid D_{p^k-1} \mid \dots \mid D_0 \mid} \\ &= \frac{\mid \mathbb{F}_{p^r} \mid^{p^k n}}{\mid [D_{p^k-1}, \dots, D_0]\cdot \mathrm{CYC}(p,k) \mid} \\ &= \mid \big([D_{p^k-1}, \dots, D_0]\cdot \mathrm{CYC}(p,k)\big)^{\perp_0} \mid, \end{aligned}$$

which gives the proof. □

Corollary 5.14.

$$\big([D_{p^k-1}, \dots, D_1, D_0]\cdot \mathrm{CYC}(p,k)\big)^{\perp_0} = [D_0^{\perp_0}, \dots, D_{p^k-2}^{\perp_0}, D_{p^k-1}^{\perp_0}]\cdot \mathrm{CYC}(p,k).$$

Proof.

$$\begin{aligned} \big([D_{p^k-1}, \dots, D_1, D_0]\cdot \mathrm{CYC}(p,k)\big)^{\perp_0} &= [D_{p^k-1}^{\perp_0}, \dots, D_1^{\perp_0}, D_0^{\perp_0}]\cdot ((\mathrm{CYC}(p,k))^{-1})^{\mathrm{tr}} \\ &= [D_{p^k-1}^{\perp_0}, \dots, D_1^{\perp_0}, D_0^{\perp_0}]\cdot Q \\ &= [D_0^{\perp_0}, \dots, D_{p^k-2}^{\perp_0}, D_{p^k-1}^{\perp_0}]\cdot JQ \\ &= [D_0^{\perp_0}, \dots, D_{p^k-2}^{\perp_0}, D_{p^k-1}^{\perp_0}]\cdot \mathrm{CYC}(p,k). \quad \square \end{aligned}$$

Now, combining Theorem 5.13 and Corollary 5.14 we get the following result.

Corollary 5.15. *Let C be a polycyclic code in $\mathbb{F}_{p^r}[x]/\langle f(x^{p^k})\rangle$ of such that $\sigma(C) = [C_{p^k-1}, C_{p^k-2}, \dots, C_0]\cdot \mathrm{CYC}(p,k)$ as in Theorem 5.6. Then*

$$\sigma(C^{\perp_0}) = [C_0^{\perp_0}, \dots, C_{p^k-2}^{\perp_0}, C_{p^k-1}^{\perp_0}]\cdot \mathrm{CYC}(p,k).$$

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] Adel Alahmadi, Steven Dougherty, André Leroy, Patrick Solé, On the duality and the direction of polycyclic codes, Adv. Math. Commun. 10 (4) (2016) 921–929.

[2] Maryam Bajalan, Edgar Martínez-Moro, Steve Szabo, A transform approach to polycyclic and serial codes over rings, Finite Fields Appl. 80 (jun 2022) 102014.

[3] Tim Blackmore, Graham H. Norton, Matrix-product codes over $\mathbb{F}_q$, Appl. Algebra Eng. Commun. Comput. 12 (6) (2001) 477–500.

[4] Yonglin Cao, Yuan Cao, Hai Q. Dinh, Fang-Wei Fu, Paravee Maneejuk, On matrix-product structure of repeated-root constacyclic codes over finite fields, Discrete Math. 343 (4) (2020) 111768.

[5] Yuan Cao, Yonglin Cao, Fang-Wei Fu, Matrix-product structure of constacyclic codes over finite chain rings $\mathbb{F}_{p^m}[u]/\langle u^e\rangle$, Appl. Algebra Eng. Commun. Comput. 29 (6) (2018) 455–478.

[6] Hai Quang Dinh, Sergio R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inf. Theory 50 (8) (2004) 1728–1744.

[7] Yun Fan, San Ling, Hongwei Liu, Homogeneous weights of matrix product codes over finite principal ideal rings, Finite Fields Appl. 29 (2014) 247–267.

[8] Yun Fan, San Ling, Hongwei Liu, Matrix product codes over finite commutative Frobenius rings, Des. Codes Cryptogr. 71 (2) (2014) 201–227.

[9] Alexandre Fotue-Tabue, Edgar Martínez-Moro, J. Thomas Blackford, On polycyclic codes over a finite chain ring, Adv. Math. Commun. 14 (3) (2020) 455–466.

[10] G. Ganske, B.R. McDonald, Finite local rings, Rocky Mt. J. Math. 3 (4) (dec 1973).

[11] Marcos J. González, On distinguishing local finite rings from finite rings only by counting elements and zero divisors, Eur. J. Pure Appl. Math. 7 (1) (2014) 109–113.

[12] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton University Press, 2008, stu - student edition.

[13] Jia Yan, On quasi-twisted codes over finite fields, Finite Fields Appl. 18 (2) (2012) 237–257.

[14] Dan Kalman, The generalized Vandermonde matrix, Math. Mag. 57 (1) (1984) 15–21.

[15] San Ling, Harald Niederreiter, Patrick Solé, On the algebraic structure of quasi-cyclic codes. IV. Repeated roots, Des. Codes Cryptogr. 38 (3) (2006) 337–361.

[16] San Ling, Patrick Solé, On the algebraic structure of quasi-cyclic codes. I. Finite fields, IEEE Trans. Inf. Theory 47 (7) (2001) 2751–2760.

[17] Hongwei Liu, Jingge Liu, Homogeneous metric and matrix product codes over finite commutative principal ideal rings, Finite Fields Appl. 64 (2020) 101666.

[18] Henri Lombardi, Claude Quitté, Commutative Algebra: Constructive Methods. Finite Projective Modules, 2015, 20:xlix+996, Translated from the French by Tania K. Roblot.

[19] Sergio R. López-Permouth, Hakan Özadam, Ferruh Özbudak, Steve Szabo, Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes, Finite Fields Appl. 19 (2013) 16–38.

[20] Sergio R. López-Permouth, Benigno R. Parra-Avila, Steve Szabo, Dual generalizations of the concept of cyclicity of codes, Adv. Math. Commun. 3 (3) (2009) 227–234.

[21] E. Martínez-Moro, A.P. Nicolás, I.F. Rua, On trace codes and Galois invariance over finite commutative chain rings, Finite Fields Appl. 22 (2013) 114–121.

[22] E. Martínez-Moro, A. Piñera Nicolás, I.F. Rúa, Multivariable codes in principal ideal polynomial quotient rings with applications to additive modular bivariate codes over $\mathbb{F}_4$, J. Pure Appl. Algebra 222 (2) (2018) 359–367.

[23] E. Martínez-Moro, I.F. Rúa, Multivariable codes over finite chain rings: serial codes, SIAM J. Discrete Math. 20 (4) (2006) 947–959.

[24] Edgar Martínez-Moro, Hakan Özadam, Ferruh Özbudak, Steve Szabo, On a class of repeated-root monomial-like abelian codes, J. Algebra Comb. Discrete Struct. Appl. 2 (2) (2015) 75–84.

[25] James L. Massey, Shirlei Serconek, Linear complexity of periodic sequences: a general theory, in: Advances in Cryptology—CRYPTO '96, Santa Barbara, CA, in: Lecture Notes in Comput. Sci., vol. 1109, Springer, Berlin, 1996, pp. 358–371.

[26] Graham H. Norton, Ana Sălăgean, On the key equation over a commutative ring, Des. Codes Cryptogr. 20 (2) (2000) 125–141.

[27] Graham H. Norton, Ana Sălăgean, On the structure of linear and cyclic codes over a finite chain ring, Appl. Algebra Eng. Commun. Comput. 10 (6) (2000) 489–506.

[28] Minjia Shi, Xiaoxiao Li, Zahra Sepasdar, Patrick Solé, Polycyclic codes as invariant subspaces, Finite Fields Appl. 68 (14) (2020) 101760.

[29] Minjia Shi, Rongsheng Wu, Yan Liu, Patrick Solé, Two and three weight codes over $\mathbb{F}_p + u\mathbb{F}_p$, Cryptogr. Commun. 9 (5) (2017) 637–646.

[30] Minjia Shi, Shixin Zhu, Shanlin Yang, A class of optimal p-ary codes from one-weight codes over $\mathbb{F}_p[u]/\langle u^m\rangle$, J. Franklin Inst. 350 (5) (2013) 929–937.

[31] R. Sobhani, Matrix-product structure of repeated-root cyclic codes over finite fields, Finite Fields Appl. 39 (2016) 216–232.

[32] Bram van Asch, Matrix-product codes over finite chain rings, Appl. Algebra Eng. Commun. Comput. 19 (1) (2008) 39–49.